Council of the European Union

Brussels, 25 September 2023
(OR. en)

13344/23

HYBRID 59	**ENER 508**
DISINFO 74	**EUMC 404**
COPS 458	**CIVCOM 233**
PROCIV 66	**TRANS 368**
CSDP/PSDC 666	**COEST 522**
CYBER 220	**ESPACE 60**
CFSP/PESC 1298	**COTER 169**
JAI 1197	**CSC 457**
ECOFIN 919	**IPCR 58**
POLMIL 248	**COSI 154**

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2023) 315 final
Subject:	JOINT STAFF WORKING DOCUMENT Seventh 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

Delegations will find attached document SWD(2023) 315 final.

Encl.: SWD(2023) 315 final

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 14.9.2023
SWD(2023) 315 final

JOINT STAFF WORKING DOCUMENT

Seventh 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

Seventh 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 number of state and non-state actors are using an expanding array of hybrid tactics against democracies, targeting their core values and aiming to fracture society and undermine political decision-making. In Europe, this trend was exacerbated in 2022 and 2023 by Russia's ongoing war of aggression against Ukraine. This has been accompanied by hybrid campaigns against the EU and its partners with the primary goal to erode their unity and solidarity with Ukraine.

Foreign information manipulation and interference (FIMI) and cyberattacks have been among the most common forms of hybrid influencing. However, the weaponisation of energy and the acts of sabotage against the Nord Stream gas pipelines have led to a heightened need to ensure the resilience of the EU's critical infrastructure. The EU stepped up its efforts in this area as set out in the **Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure** of 8 December 2022[1] and the **Directive on the resilience of critical entities** (CER Directive)[2], as well as the revised Directive on the security of network and information systems (NIS2 Directive)[3].

In a context of hybrid threats that are growing in complexity and sophistication, implementing the **EU Strategic Compass for Security and Defence**[4] (Strategic Compass) and the **EU Security Union Strategy**[5] is of crucial importance. The Commission services and the European External Action Service (EEAS) have contributed to creating the **EU Hybrid Toolbox**. This toolbox provides a framework for a coordinated and well-informed response to hybrid campaigns, bringing together all relevant internal and external tools and measures. The EEAS and the Commission services are also working together with Member States on setting up **EU hybrid rapid response teams** to provide short-term tailored assistance in countering hybrid threats to Member States, partner countries and common security and defence policy (CSDP) missions and operations. To support Moldova's efforts in countering hybrid threats, the EU deployed a civilian **CSDP mission**. The revised **EU Protocol for countering hybrid threats**[6] describes EU's processes and tools applicable for hybrid threats and campaigns.

The Commission services and the EEAS are also testing response options and running exercises, based on different scenarios, including the multilayer crisis management exercise **EU Integrated Resolve 2022** (19 September to 18 November 2022).

The conceptual approach to resilience and hybrid threats was further developed by the Joint Research Centre (JRC) and the European Centre of Excellence for Countering Hybrid Threats

[1] OJ C 20, 20.1.2023, p. 1.
[2] OJ L 333, 27.12.2022, p. 164.
[3] OJ L 333, 27.12.2022, p. 80–152.
[4] Council document 7371/22.
[5] COM 2020 (605).
[6] SWD(2023) 116 final.

(Hybrid CoE) publishing a flagship report ***Hybrid Threats: A Comprehensive Resilient Ecosystem*** (CORE)[7] in April 2023.

This seventh progress report summarises the main developments in countering hybrid threats since July 2022. The report should be read in conjunction with the fifth progress report on the implementation of the EU Security Union strategy[8] and the eighth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils[9].

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 inform policy preparation and decision-making at all levels by providing all-source (open-source and intelligence-based) strategic analysis on hybrid threats. The HFC has also given verbal briefings in various Council bodies. To support the EU decision-making process, the HFC has regularly analysed hybrid threats to the EU, its neighbourhood and interests, including in the context of Russia's war of aggression against Ukraine.

Through regular interaction with its different networks and partners, the HFC has continued its efforts with regard to creating a better common understanding of hybrid threats at EU level. In cooperation with the rotating Presidency of the Council of the EU, the HFC held meetings of the **national points of contact for countering hybrid threats** (National POCs) twice a year. In addition, while respecting existing restrictions on sharing classified information, it maintained its close cooperation with the NATO Joint Intelligence and Security Division Hybrid Analysis Branch (NATO HAB).

In line with the National POCs' interests, the HFC initiated the process of an overarching intelligence **assessment on threats to the EU institutions.** Based on Member States' contributions and the results of interinstitutional workshops, an intelligence assessment was issued in July 2022. A second iteration is planned in 2023.

The HFC-led annual **Hybrid Trends Analysis** covering 2022 was issued in **April 2023**, with more contributions from Member States and EU institutions.

In 2023, the HFC began to develop and produce **cyberthreat landscape reports** on the main threat actors targeting Member States. These reports will be updated once a year to track changes in these threat actors' cyber operations. The HFC actively contributed to the **Cyber Diplomacy Toolbox**, which was activated several times in 2022. In addition, a significant part of HFC reporting and briefings was focused on different adversaries' malicious cyber activities against private and public bodies in Member States as well as thematic topics on the development of cyber technologies.

The HFC was actively involved in exercises, such as **EU Integrated Resolve 2022 (PACE)**, a cyber-crisis management exercise conducted by the Czech Presidency and the Space Threat Response Architecture (STRA-23). As part of these exercises, the HFC carried out open-

[7] 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.
[8] COM(2022) 252 final.
[9] Council Document 10254/23

source and intelligence-based assessments (including a parallel and coordinated intelligence assessment in cooperation with NATO HAB).

Strengthening institutional resilience

The Commission remains committed to strengthening the EU administration's resilience and improving its security culture against the ever-increasing cyber and hybrid threats. To this end, it has made significant progress in deploying new IT systems for handling classified information.

On the basis of the Commission proposal for a **Regulation establishing measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union**[10], the co-legislators reached a provisional agreement on 26 June 2023. Once the text is finalised, the European Parliament and the Council will have to formally adopt the new Regulation before it can enter into force. Union entities will then be required to comply with the obligations and meet the deadlines specified in the text. This will contribute to ensuring higher levels of cybersecurity in the EU administration and be better prepared to face future challenges.

The Commission proposed in March 2022 the **Regulation on information security in the institutions, bodies, offices and agencies of the Union[11].** The regulation will create a minimum set of information security rules and standards for all EU institutions, bodies, offices and agencies to ensure an enhanced and consistent protection against the evolving threats to their information, both EU classified and non-classified. These new rules will provide a stable ground for a secure exchange of information across EU institutions, bodies, offices and agencies, and with the Member States, based on standardised practices and measures to protect information flows.

The **Joint Communication on the EU policy on cyber defence**[12], adopted on 10 November 2022, announced the development of military cyber bodies and/or mechanisms in the civilian and military cyber ecosystem. These bodies, such as the Military Computer Emergency Response Teams Operational Network and the EU Cyber Defence Coordination Centre, will complement the cyber situational awareness and include threats to CSDP missions and operations. The European Cybersecurity Shield proposed under the EU Cyber Solidarity Act[13] will also strengthen common EU detection, situational awareness and response capabilities.

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

Strategic communication, FIMI and disinformation

The EU stepped up its efforts to counter FIMI, especially in the context of Russia's war of aggression against Ukraine. During the reporting period, the EEAS focused its strategic communication efforts on exposing Russia's increased use of FIMI. The Commission is also looking very closely at disinformation narratives concerning Russia's war of aggression against Ukraine. To limit the spread of FIMI the EU has adopted several unprecedented

[10] COM(2022) 122 final.
[11] COM(2022) 119
[12] JOIN(2022)49 final.
[13] COM(2023) 209 final

measures, such as **sanctioning a number of Russia's war propaganda instruments** (for example, Russia Today and Sputnik).

Against this background, to prevent, deter and respond to FIMI, the EEAS has worked closely with other EU institutions, Member States, like-minded international partners (in particular the G7 and NATO), civil society and private industry. The EEAS published its **first report on FIMI threats**[14], which builds on a solid understanding of the tactics, techniques and procedures used by Russia and China to engage in FIMI, including suppressing and controlling critical opinions and voices. In addition, on 8 February 2023, the EEAS launched a new EU initiative to bring information exchange to the next level through a dedicated **FIMI Information Sharing and Analysis Centre**.

At policy level, the EEAS and the Commission have developed an **EU toolbox to address and counter FIMI** in cooperation with Member States. The toolbox will strengthen the EU's existing tools to prevent, deter and respond to FIMI, including by imposing costs on the perpetrators of such activities.

On 7 February 2023, the EEAS published the 2022 report on its activities to counter FIMI[15]. This report describes EEAS efforts to tackle FIMI across the eastern and southern neighbourhoods and the Western Balkans, support CSDP missions and operations to build their capacity, strengthen cooperation with international partners and highlight work on developing comprehensive situational awareness of China's manipulation efforts.

To counter the spread of online disinformation, on 16 June 2022, the signatories of the **EU Code of Practice on Disinformation**[16] published a major overhaul of the Code, based on the Commission's 2021 guidance[17]. The new Code has a detailed set of commitments to tackle online disinformation in different areas. Many different signatories, 44 to date, have signed the Code. In addition to major online platforms and players from the online advertising industry, new signatories include smaller or specialised platforms, research and civil society organisations and fact-checkers.

The new Code includes a strengthened monitoring system that incorporates reporting measurable at Member State level. The signatories submitted their first monitoring reports under the new Code in January 2023. A permanent task force under the Code is charged with developing the monitoring systems in view of technological, social market and legislative developments and exchanging disinformation threats observed in the context of the COVID-19 pandemic and Russia's war of aggression against Ukraine.

The Commission continues to support the work of the **European Digital Media Observatory** (EDMO), which is creating a cross-border and multidisciplinary community of independent fact-checkers and academic researchers in the EU. In addition to its central digital platform, EDMO is composed of national and regional hubs, which now cover the entire EU population. As a result of Russia's war of aggression against Ukraine, EDMO set up a dedicated task force that has produced thousands of war-related fact-checks and several analyses of disinformation campaigns. EDMO has also established a dedicated task force focusing on the 2024 European elections.

Incitement to racist and xenophobic violence and hatred has also been perceived as a growing problem since the start of Russia's war of aggression against Ukraine with increased

[14] https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en
[15] https://www.eeas.europa.eu/eeas/2022-report-eeas-activities-counter-fimi_en
[16] https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation
[17] COM(2021) 262 final.

antisemitic, anti-Muslim and anti-refugee narratives being circulated, often in combination with dissemination of disinformation and conspiracy theories. The Commission has continued to work with IT companies and civil society under the **Code of conduct on countering illegal hate speech**[18] to tackle this problem; discussions are currently ongoing with the signatory IT companies on further strengthening the code to help the effective enforcement of the Digital Services Act[19].

Lastly, to strengthen young people's ability to detect, respond and build resilience to FIMI, in October 2022 the Commission published **Guidelines for teachers and educators on tackling disinformation and promoting digital literacy** through education and training[20]. The guidelines are part of the EU's Digital Education Action Plan (2021-2027)[21] and give advice on how to use digital technologies critically and responsibly.

Securing free and fair elections and protecting democratic processes

Securing free and fair elections and protecting democratic processes have been priorities for the Commission since the adoption of its 2018 electoral package[22]. These priorities were included in the initiatives announced in the 2020 European democracy action plan[23]. The proposals for a **regulation on the transparency and targeting of political advertising**[24] and for a **regulation on the statute and funding of European political parties and European political foundations**[25] are at an advanced stage of negotiation among the European co-legislators. They are part of a package of measures to strengthen democracy and protect the integrity of elections.

Other measures have been taken forward, including as part of the regular meetings of the **European cooperation network on elections**[26]. This includes a 'joint mechanism for electoral resilience' organised and coordinated by the EU Network on Elections in close cooperation with the Network and Information Systems (NIS) Cooperation Group and the EU's Rapid Alert System. It has supported several Member States since it started operations in 2022.

As announced in its 2021 Communication on protecting election integrity and promoting democratic participation[27], the Commission will continue using the EU Network on Elections to deliver on its commitments. It will support, among others, the cooperation between EU networks and international organisations to build capacity and exchange best practices in countering electoral threats and promote high international standards in the use of new technologies, including through its planned compendium of e-voting practices.

[18] https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en
[19] OJ L 277, 27.10.2022, p. 1–102.
[20] European Commission, Directorate-General for Education, Youth, Sport and Culture, *Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training*, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2766/28248.
[21] COM(2020) 624 final.
[22] COM(2018) 637 final.
[23] COM(2020) 790 final
[24] COM(2021)731 final.
[25] COM(2021)734 final.
[26] https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/eu-citizenship/democracy-and-electoral-rights_en#european-cooperation-network-on-elections
[27] COM(2021)730 final

The European Centre of Excellence for Countering Hybrid Threats

The EU institutions, bodies and agencies have intensified work with the Hybrid CoE through research, training, exercises and exchanges at different levels. In 2022, the Hybrid CoE provided **tailor-made training on hybrid threats** to EU institutions staff. In addition, the Centre organised several **events and seminars,** including the third EU-NATO High-Level Retreat for high-ranking civil servants, a foresight-themed workshop for policy-planning staff from both organisations, and a briefing to Commission staff on disinformation and how the EU should respond.

The Hybrid CoE cooperates with the rotating presidencies of the Council of the EU based on their requests. In 2022-2023, the Hybrid CoE provided several briefings to the Council Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats and facilitated an exercise for the group during discussions on the EU Hybrid Toolbox implementing guidelines.

Hybrid CoE cooperated with the Commission on the resilience of critical infrastructure and the **design of stress tests of critical infrastructure in the energy sector**.

The Hybrid CoE and the JRC continued to cooperate on many initiatives, including the CORE report, contributing to the conceptualisation of hybrid threats. Hybrid CoE is one of the key partners of the project **Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET)**, funded under the EU's Horizon 2020 research and innovation programme. This project brings together security practitioners, academics, industry players and small and medium-sized companies to develop a pan-European network to detect, prepare for and counter hybrid threats. The network has steadily grown to represent over 100 members organisations across Europe. EU-HYBNET also conducts research, identifies innovation initiatives and organises training and exercises, which lead to recommendations on different Commission initiatives.

Protection of critical infrastructure

As established in the Security Union Strategy, the protection of critical infrastructure should be addressed both from the physical and digital perspectives. An update on the measures related to the latter is included in the cybersecurity section of this report.

On 8 December 2022, the **Council adopted a Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure**[28] to step up the EU's capacity to protect itself. This Recommendation sets out a series of targeted actions at Union and national level to support and enhance the resilience of critical infrastructure, with a focus on critical infrastructure with significant cross-border relevance and in identified key sectors, such as energy, digital infrastructure, transport and space. Those targeted actions consist of enhanced preparedness, response and international cooperation. One of the key actions is to enhance preparedness against sabotage with the help of stress tests of critical infrastructure in the energy sector. In December 2022 Commission, Member States, EU Intelligence and Situation Centre (Intcen) and the Hybrid CoE developed common principles and scenarios for the relevant stress tests. Member States will now support the conduct of these stress tests by critical infrastructure operators in the energy sector to identify and remedy vulnerabilities and strengthen their resilience. The stress tests should be finalised by the end of 2023 at the latest and could be expanded to other sectors. The Recommendation also invites the Commission to draw up a draft **blueprint on a coordinated response to**

[28] OJ C 20, 20.1.2023, p. 1–11.

disruptions to critical infrastructure of significant cross-border importance. Preparation of the proposal for a blueprint is ongoing.

In January 2023, the **CER Directive** entered into force. It covers 11 sectors, including energy, digital, space, health, transport and water. It puts forward a clear set of obligations for Member States and critical entities, as well as mechanisms for cooperation and support at EU level.

On 8 February 2023, the Commission adopted a recommendation[29] and a communication[30] to set out **common goals to boost disaster resilience** in civil protection. Given the rapidly changing risk landscape, including hybrid threats, the aim is to improve the capacity of the EU, its Member States and Participating States in the Union Civil Protection Mechanism to anticipate and withstand the effects of major disasters and emergencies in the future. The Commission developed in cooperation with the Member States five union disaster resilience goals setting a new European resilience agenda, covering key civil protection prevention and preparedness actions.

At the request of Member State authorities, the Commission also deployed EU **protective security advisory missions** to several critical infrastructure operators and high threat events in Member States to conduct security vulnerability assessments and help them improve their preparedness against a range of threats, including sabotage and other malicious activities.

Based on an opportunity for cooperation identified during the last cycle of the **coordinated annual review of defence**, the EDA hosted a symposium on critical maritime infrastructure protection on 27 April 2023.

As part of the **Consultation Forum for Sustainable Energy in the Defence and Security Sector** and in coordination with the Commission, the EDA conducted a study to explore options for increasing the resilience of defence-related critical energy infrastructure against hybrid threats.

Energy security of supply and energy infrastructure

The EU has adopted a number of new legislative rules to combat the energy crisis, strengthen preparedness and secure energy supplies. The **Gas Storage Regulation**[31], adopted on 29 June 2022, was instrumental in getting Member States to refill storage and achieve a 95% filling rate by 1 November 2022. On 5 August 2022, the EU adopted a Regulation setting a voluntary reduction target of 15% of gas demand by Member States[32]. Between August and November 2022, a 20.2% reduction in gas demand was achieved. The **REPowerEU plan**[33], proposed in May 2022, will help EU gain independence from Russian energy, namely by saving energy, accelerating the clean energy transition and diversifying supplies. Before the start of Russia's war of aggression in Ukraine in February 2022, around 40% of pipeline gas imports came from Russia. Now, imports are down to below 10%. Similarly, the **EU Energy Platform** has supported diversifying through reliable suppliers and sources. Renewed arrangements have been set up, for example with the United States, Norway, Azerbaijan, Egypt, Israel and Algeria. The Platform also ensures that existing infrastructure is used as efficiently as possible.

On 14 March 2023 the Commission adopted a proposal for a new **Electricity Market Design**[34]. This aims to make the EU energy market more resilient and the energy bills of EU

[29] OJ C 56, 15.2.2023, p. 1.
[30] COM(2023)61 final.
[31] OJ L 173, 30.6.2022, p. 1.
[32] OJ L 206, 8.8.2022, p. 1–10.
[33] COM(2022) 230 final.
[34] COM(2023) 148 final.

consumers and companies more independent from short-term electricity market prices. In the context of the proposal, the Commission adopted a Recommendation on energy storage[35]. This focuses on the most important issues contributing to the wider deployment of energy storage in the energy system and making the most of its benefits. This is particularly important to ensure a highly secure and stable energy supply as the EU strives to integrate new renewable sources into the grid.

Another major goal of REPowerEU is to boost the development of renewables to replace gas in power generation and heating. The **Net-Zero Industry Act**[36] proposed by the Commission on 16 March 2023 supports the industrial manufacturing of key clean technologies in the EU. The Act sets out a simplified regulatory framework for producing clean technology and the supply chain components required. It also proposes accelerated permitting procedures, including for clean tech manufacturing projects. To ensure the supply of critical raw materials needed for the green and digital transitions, defence and aerospace, on 16 March 2023 the Commission proposed the **Critical Raw Materials Act**[37]. This aims to support the EU in building up the energy sector in terms of renewables and clean energy technologies, with a focus on diversifying supply chains to ensure resilience and preparedness in a crisis.

Securing strategic domains

In the **aviation sector**, the Commission continued to regularly monitor emerging threats, including hybrid threats, to adapt the aviation security baseline. The Commission, in cooperation with Intcen and Member States, conducted a **comprehensive mapping of aviation security risks** to take stock of existing and evolving threats and vulnerabilities and to identify areas where further mitigation may be necessary. In February 2023, the Commission proposed a **new approach towards an enhanced and more resilient aviation security policy**[38]. One of the key issues addressed is to consider a new EU baseline for aviation security in light of evolving threats and available technologies. The risk mapping will support the decision-making process for a new EU future-proof baseline.

The Commission, in cooperation with Intcen, European Union Aviation Safety Authority (EASA) and Member States, continued to regularly monitor and assess the **security risk to civil aviation from conflict zones**. Russia's war of aggression against Ukraine has intensified global navigation satellite systems jamming and/or possible spoofing in areas surrounding Ukraine and other areas that the Commission is closely monitoring.

Unmanned aircraft systems (drones) can be used by malicious actors, including those involved in hybrid actions. The threat is likely to grow as drones become more ubiquitous and capable. As set out in the **Drone Strategy 2.0**[39], adopted on 29 November 2022, the Commission is considering a possible amendment to aviation security rules to ensure that aviation authorities and airports are more resilient to the risks posed by drones.

On **maritime security**, the Commission and the EEAS continued monitoring conflict events or situations that could impact maritime security. In 2022, the European Maritime Safety Authority (EMSA) and the Commission issued the first update to the **Interim Guidance on Maritime Security for Member States' Competent Authorities**[40]. The update reflects the

[35] COM(2023/C 103/01).
[36] COM(2023) 161.
[37] COM(2023) 160.
[38] SWD(2023) 37 final.
[39] COM(2022) 652 final.
[40] European Commission MARSEC Doc. 8708 annex.

experience gained from the Commission's maritime security inspections and shares best practices among Member States. There is a particular emphasis on cybersecurity.

The Commission also carried out an **EU-level risk assessment on passenger ship security** with Member State authorities in October 2022 to better identify threats and vulnerabilities in this sector.

On 10 March 2023, the Commission and the High Representative adopted a Joint Communication **"An enhanced EU Maritime Security Strategy for evolving maritime threats"**[41] to ensure a peaceful use of the sea and safeguard the maritime sector from new threats. The new action plan contains, in particular, measures on the resilience and protection of critical maritime infrastructure. These measures include: (i) conducting regular, full-scale live exercises at EU level focused on harbour protection and countering cyber and hybrid threats; (ii) developing specialised ways to patrol and protect maritime infrastructure; and (iii) increasing cooperation to develop regional cooperation plans at EU level to ensure the surveillance of underwater and offshore infrastructure.

Related to the update of the EU Maritime Security Strategy, the EDA has made progress in the **Maritime Surveillance Networking Project (MARSUR)**, which will greatly improve Member States' awareness in the maritime domain, including of hybrid threats. The EDA took active steps in supporting Member States in launching a new programme on a comprehensive approach to situational awareness for the maritime spaces of Europe. The programme was approved in April 2023 and aims to provide a forum for aligning the work of various initiatives and develop cooperation in the full spectrum of capability development of maritime situational awareness for defence.

The EDA also continued to support projects on harbour and maritime surveillance and protection. These projects aim to strengthen the EU's capability to counter threats, including hybrid ones.

On **rail security**, in December 2022 the Expert Group on Land Transport Security[42] adopted guidelines on security culture in rail bodies and among staff and passengers.

In September 2022, the Commission proposed a **Single Market Emergency Instrument**[43] providing for a general framework for anticipating, preparing for, 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.

Border and supply chain security and export control

The European Council, in its conclusions of the extraordinary meeting on migration of 9 February 2023[44], addressed the role of transport operators in facilitating irregular migration to the EU. As announced in the action plan on the Western Balkans[45], the Commission on 6 June 2023 presented a **toolbox of new measures to address the increasing misuse of commercial transport by criminal networks facilitating irregular migration to the EU**[46].

[41] JOIN (2023) 8 final.
[42] The Expert Group on Land Transport Security was established by Commission Decision 2012/286/EU of 31 May 2012 for a permanent duration.
[43] COM(2022) 459 final.
[44] EUCO 1/23.
[45] https://home-affairs.ec.europa.eu/eu-action-plan-western-balkans_en
[46] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3057

Considering the importance and the attractiveness of the EU transport market, the EU has significant leverage with third-country transport authorities and operators and can play a key role in setting high transport standards globally, including in terms of developing measures to counter the misuse of commercial transport by criminal networks that facilitate irregular migration. Alongside the adoption of new rules to reinforce the EU's legal framework in this area and stepped-up situational awareness, the EU will enhance its engagement with transport operators and authorities in third countries, especially in the aviation sector.

On 14 March 2023, the Commission adopted a **Communication establishing the multiannual strategic policy for European integrated border management**[47], providing policy priorities and strategic guidelines in this area.

On export control and sanctions, the Commission has adopted **eleven sanction packages**, including restrictions on exports of dual-use and advanced technologies to Russia and Belarus. The lists of restricted items, technologies and bodies have been regularly updated in light of intelligence gathered on Ukrainian battlefields and information provided by partners. The Commission has also been working with EU partner countries to ensure that these restrictions remain effective and tackle the risk of circumvention and backfilling.

Space

The **EU Space Strategy for Security and Defence**[48] was adopted on 10 March 2023 and proposes concrete actions to strengthen the resilience and protection of space systems and services, including against hybrid threats. It proposes to set up an EU security framework for information sharing, cooperation and the protection of space systems. In developing EU space systems and services that support security and defence, the Commission will take into account all necessary security requirements and measures to ensure their resilience (a 'security by design' approach). The strategy also includes action to strengthen space domain awareness at EU level, which is crucial to protect space assets from different kinds of threats.

Copernicus, the Earth observation component of the EU space programme, continued supporting the EU and its Member States in countering hybrid threats through its **security service**[49] and its **emergency management service**[50]. Sentinel satellites and the Copernicus Atmosphere Monitoring Service were used to identify the gas leaks in the Nord Stream 1 and 2 pipelines after they were sabotaged.

Regulation establishing the **Union secure connectivity programme for the period 2023-2027** entered into force in March 2023[51]. The programme aims at deploying an EU satellite constellation called IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite). The programme aims to provide and maintain secure, autonomous, high-quality, reliable and cost-effective satellite governmental communication services for government-authorised users in the EU and the world. The system will support the protection of critical infrastructure, situational awareness, external action, crisis management and applications that are critical for the economy, the environment, security and defence.

Defence capabilities

[47] COM(2023)146 final.
[48] JOIN(2023) 9 final.
[49] Including border surveillance, maritime surveillance and support to EU external action.
[50] For civil protection in disasters caused by natural or human factors.
[51] OJ L 79, 17.3.2023, p. 1.

The Commission continued to support the research and development of defence capabilities by strengthening the autonomy and resilience of the European defence technological and industrial base. Following the first-ever calls for proposals under the **European Defence Fund** (EDF) 2021 work programme, 60 projects have been awarded and, after 3 years of implementation, the EU has dedicated around EUR 3.5 billion to support collaborative defence R&D. Another batch of 41 projects with a total EU support of EUR 0.8 billion were selected for funding in June 2023.

The EDA continued its work supporting the Permanent Structured Cooperation (PESCO), both as part of the PESCO secretariat and by facilitating project management at Member States' requests. For example, the EDA continues to support projects, such as the Cyber Rapid Response Teams and the Cyber and Information Domain Coordination Centre.

Protecting public health and food security

The work on **raising awareness of hybrid threats within the Technical Working Group on Preparedness of the Health Security Committee** includes discussions on the possible impact of hybrid threats on public health and how to address them to improve health preparedness and resilience. This includes an all-hazard approach in health preparedness planning for Member States that are revising their plans or developing new ones. Discussions are ongoing under Article 7 (reporting on preparedness) and Article 5 (the EU preparedness plan) of the Serious Cross-Border Health Threats Regulation[52], and the inclusion of hybrid threats in the first health preparedness training programme under Article 11 of the Regulation is also being considered, particularly taking into account the use of disinformation in the health domain.

A study on mapping risks and vulnerabilities of the EU food supply chain and its critical infrastructure is currently being carried out.

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 was finalised in May 2021. It paved the way for a robust **impact assessment study on regulating the marketing and use of high-risk chemicals that can be used for terrorist attacks**. This work was finalised in April 2023.

The Commission continues to implement actions on **CBRN defence capabilities and research** under the EDF and its predecessor programmes, such as the European defence and industrial development programme project "Chemical, Biological, Radiological and Nuclear Reconnaissance and Surveillance System". The EDF medical response category and CBRN actions received EU funding support of close to EUR 60 million in the 2021 EDF awards.

The EDA continues work on **CBRN surveillance** as a service. It supports the PESCO project with the same name and has recently successfully completed the prototyping phase. Field testing will be the next step in rapidly deploying an around-the-clock CBRN surveillance capability.

Under the Union Civil Preparedness Mechanism (UCPM), European Civil Protection Pool capabilities have been pre-committed by a number of Member States. At this stage, seven **CBRN detection and sampling capabilities** are available with four more in the pipeline, including capabilities for search and rescue in CBRN conditions and decontamination.

[52] OJ L 314, 6.12.2022, p. 26.

To further strengthen the Union CBRN preparedness, three additional streams of CBRN capabilities are under development under rescEU comprising decontamination, detection and CBRN medical countermeasures; the latter capacity being co-developed with the European Health Emergency Preparedness and Response Authority (HERA). While individual countries are responsible for the development of each rescEU CBRN capability, the Commission regularly brings together CBRN experts from across the Union to ensure the interoperability of the capabilities and maximise the operational learnings across the Union.

In addition, the Emergency Response Coordination Centre of the European Commission has carried out a **short-term assessment of Union-level CBRN readiness** and supported the organisation of an **informal ministerial-level coordination meeting on CBRN preparedness** on 30 May 2023 in Brussels. The outcomes of these efforts fed into the development of the Council Conclusions on strengthening whole-of-society resilience in the context of civil protection, including preparedness for CBRN threats[53], adopted in June 2023.

One of the recommendations of these Council Conclusions is for the Commission to explore how to increase market access to different kinds of CBRN-relevant equipment, supplies and material. To that end, HERA has identified, in its medical countermeasures catalogue, relevant threat-specific as well as horizontal medical countermeasures, including for preparedness and response to CBRN threats. This allows HERA to **monitor the supply chain resilience** of these items. In July 2023, HERA launched "HERA Invest", which is **HERA's new investment tool** with a budget of EUR 100 m to fund the development of novel (CBRN) medical countermeasures[54].

Cybersecurity

On 16 January 2023, the **NIS2 Directive** came into force. To respond to the growing threats due to digitalisation and interconnectedness, particularly intensified by the coronavirus crisis, the revised Directive will cover medium and large-sized entities from more sectors, based on their criticality for the economy and society. 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.

Furthermore, in September 2022, the Commission adopted a proposal for **a Cyber Resilience Act**[55], aiming to establish common mandatory cybersecurity requirements for products with digital elements, hardware and software, as a condition for accessing the internal market, thus also strengthening the security of supply chain.

On 18 April 2023, the Commission adopted a **cybersecurity package**, consisting of three different initiatives. A proposal for the **Cyber Solidarity Act**[56] (with the objective to strengthen cybersecurity capacities in the EU), a **Cybersecurity Skills Academy**[57] (presented as part of the 2023 European Year of Skills to ensure a more coordinated approach towards closing the cybersecurity talent gap) and a **proposal for a targeted amendment to the Cybersecurity Act**[58] (to enable the future adoption of European certification schemes for 'managed security services').

[53] Council document 10048/23.
[54] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3775
[55] COM(2022) 454 final.
[56] COM(2023) 209 final
[57] COM(2023) 207 final
[58] OJ L 151, 7.6.2019, p. 15–69

Also, on 15 June 2023, EU Member States, in cooperation with the Commission and European Union Agency for Cybersecurity (ENISA), published a **Second progress report on the implementation of the EU Toolbox on 5G cybersecurity**. It highlights the progress made, but also underlines the shortcomings in the implementation of its measures. Complementary to this, the Commission adopted a **Communication on 5G cybersecurity**[59] to take note of and welcome the adoption of the report and support its findings.

The European Cybersecurity Competence Centre started its activities in May 2023 with the aim to increase Europe's cybersecurity capacities and competitiveness, working together with a Network of National Coordination Centres (NCCs) to build a strong cybersecurity Community.

On 15 February 2023, ENISA and the EU's Computer Emergency Response Team (CERT-EU) jointly published the **report *Sustained activity by specific threat actors***[60]. It highlighted that malicious cyber activities of the threat actors presented in the report pose a significant and ongoing threat to the EU. The two organisations made recommendations and encouraged all public and private sector organisations to apply them systematically. On the basis of the joint publication, CERT-EU made available **specific implementation recommendations**. The recommended measures would allow them to improve their cybersecurity posture to fend off a wide range of attacks and limit the number of incidents and will help them detect and react to cyber operations that may be carried off by sophisticated threat actors.[61]

CERT-EU has been monitoring the **cyber aspects of Russia's war of aggression on Ukraine** since January 2022. The aim was to observe the global cyber landscape and anticipate if and how cyber operations would target EU institutions, bodies and agencies, and other organisations. This work resulted in a dedicated report published on 24 February 2023[62].

On 11 March 2023, CERT-EU published a security guidance, with the contribution of the Commission, on the **potential impact and risks of generative AI in EU institutions, bodies and agencies**[63]. The document takes account of the rapid advancement of AI and while it embraces this transformative innovation, it flags the potential risks. Overall, the guidance aims at defining the position of CERT-EU towards generative AI technology and provide an initial overview of this complex topic.

Cybersecurity in the energy sector

Smart meters are an essential part of energy distribution networks. To help protect the overall infrastructure, the Commission has fostered the development of harmonised standards in support of Commission Delegated Regulation 2022/30[64]. Those specifications aim to determine the appropriate levels of cybersecurity and protection of user privacy.

The Commission continued working closely with ENISA and the NIS Cooperation Group's dedicated sectoral workstream on energy to ensure awareness and cooperation on sector-specific topics. Furthermore, the Commission continued working on a Network Code for sector-specific rules on the cybersecurity of cross-border electricity flows.

[59] COM (2023) 4049.
[60] TLP:CLEAR, 15.02.2023, JP-23-01.
[61] Security Guidance 22-001 - Cybersecurity mitigation measures against critical threats
[62] Russia's war on Ukraine: one year of cyber operations
[63] Security Guidance 23-002 - Potential impact and risks of Generative AI in EUIBAs
[64] OJ L 7, 12.1.2022, p. 6.

Cybersecurity in the financial services sector

Further progress was made on the legislative framework for digital operational resilience in the financial sector. On 27 December 2022, the **Digital Operational Resilience Act** was published[65]. It entered into force in January 2023 and will become applicable from 17 January 2025. The agreed new rules aim to create a regulatory framework on digital operational resilience whereby all financial bodies need to ensure they can withstand, respond to and recover from all types of ICT disruptions and threats. The Act also places critical ICT third-party service providers under a supervisory framework.

Cybersecurity in the transport sector

At the start of 2023, the EU regulatory framework for cybersecurity in **civil aviation** was completed. The scope of the NIS2 Directive was extended to cover a broader range of air, rail, water and road transport bodies. In the area of aviation safety, the Commission adopted Delegated Regulation (EU) 2022/1645[66] and Implementing Regulation (EU) 2023/203[67] both on requirements for managing information security risks with a potential impact on aviation safety. Work on aligning aviation cybersecurity requirements has continued in the Aviation Cybersecurity Working Group. EASA is leading the European Centre for Cyber Security in Aviation for information exchange, the Network of Cybersecurity Analysts for occurrence analysis, and the European Strategic Cybersecurity Platform for discussing and coordinating initiatives at strategic level. International activities have allowed for regular exchanges on aviation cybersecurity with key partner states, such as the United States and international organisations (International Civil Aviation Organization, European Civil Aviation Conference and Eurocontrol).

The European Aviation Crisis Coordination Cell continues to give training on, monitor and coordinate responses to any future aviation network crisis, including cyberattacks on aviation critical infrastructure.

In terms of developing aviation security capacity in non-EU countries, the Civil Aviation Security in Africa, the Middle East and Asia project (CASE II) aims to improve aviation security in partner countries. It includes a component on cybersecurity capacity building, based on the standards set by the International Civil Aviation Organization.

In the rail sector, cybersecurity is one of the priority areas in the work programme of the Working Party on Rail Security under the Commission Expert Group on Land Transport Security. The rail sector also falls under the scope of the **Cyber Resilience Act**.

The Commission organised a workshop on cybersecurity in the **maritime sector** with Member State authorities in November 2022. Afterwards, a **guidance document on how to treat cybersecurity in ports and port facilities**[68] was finalised. This guidance clarifies the legislative cybersecurity requirements set out in EU maritime security legislation and makes further recommendations on applying them. The scope of the NIS2 Directive was extended to include a broader range of maritime transport bodies. The Commission is also following developments at the International Maritime Organization on maritime cybersecurity and discussing the topic with international partners.

[65] OJ L 333, 27.12.2022, p. 1.
[66] OJ L 248, 26.9.2022, p. 18.
[67] OJ L 31, 2.2.2023, p. 1.
[68] European Commission MARSEC Doc. 8910.

In 2022, in cooperation with the Commission, EMSA's maritime security team initiated a series of **maritime cybersecurity measures**. Furthermore, EMSA took further action to improve maritime cybersecurity awareness and sharing information. The Agency hosted and participated in the second ENISA Maritime Cybersecurity Conference on 14 October 2022.

EMSA also organised its first **maritime cybersecurity workshop** on 8 December 2022. The event brought together 50 participants from Member States and speakers from the Commission, ENISA and the private maritime sector. The objective of this workshop was to raise awareness on maritime cybersecurity for shipping. Following the workshop, EMSA started supporting the Commission in developing specific guidance on how to address cybersecurity on board ships during audits, controls, verifications and inspections. At the request of Member States and the Commission, EMSA also started developing training on maritime cybersecurity to strengthen and support the capabilities of EU maritime administrations.

Cyber defence

The Joint Communication on the **EU Policy on Cyber Defence**[69] was published on 10 November 2022. It gives strategic guidance for developing new EU and national cyber defence capabilities and will bridge the gap between civilian and military bodies and public and private entities. It also heavily underlines the importance of EU-NATO cooperation. The policy will allow building cyber defence capabilities, enhancing EU-wide situational awareness and coordination of the whole range of defensive options available to strengthen EU resilience, respond to cyber-attacks and ensure solidarity and mutual assistance. As set out in the Joint Communication, military Computer Emergency Response Teams (MilCERTs) will be connected at EU level and an EU Cyber Defence Coordination Centre will be established to allow for exchange of situational awareness and coordinate appropriate responses, including by Cyber Rapid Response Teams.

The Commission services and the EEAS continued to support and implement action to support the development of cyber defence capabilities and cyber defence research through the EDF and its precursor programmes. For example, the results of the EDF 2021 calls for proposals show that the EDF supported cyber defence projects with a budget close to EUR 40 million. These projects covered capability development and research.

In September 2022, the EDA, together with the European Security and Defence College and Hybrid CoE, organised the pilot course "The contribution of cyber in hybrid conflicts". Work on transforming this pilot into a regular course is ongoing, based on the evaluation report published in November 2022.

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

As agreed in the Strategic Compass, the **implementing guidelines of the Cyber Diplomacy Toolbox** were revised in June 2023[70]. The revision enables the development of sustained, tailored, coherent and coordinated strategies towards persistent cyber threat actors. It allows the EU to address better the challenges of continued lower level grey-zone threats and activities stemming from persistent cyber threat actors.

[69] JOIN (2022) 49 final.
[70] Council document ST 10289/23 COR1.

With the EEAS support the Council will formulate tailored strategies to counter particular cyber threat actors and monitor the implementation. The revision also strengthens exchanges on situational awareness among relevant stakeholders, and better position the Cyber Diplomacy Toolbox within the EU's cyber crisis management framework. Furthermore, other additional measures have been identified, including building global partnerships, raising awareness, as well as suspension or cancellation of engagements or dialogues.

International cooperation on cybersecurity

The EU holds regular cyber dialogues with many partner countries. In addition, cybersecurity and cyber defence have been a topic of several international security and defence dialogues.

In September 2022, the second round of the **EU-Ukraine Cybersecurity Dialogue** took place, where both sides emphasised the importance of further strengthening cyber resilience efforts and cooperation.

Since 2014, a comprehensive **EU-US Cyber Dialogue** has been taking place regularly. It is a whole-of-government dialogue and tackles all cyber issues, including cybersecurity, cybercrime, cyber diplomacy, cyber capacity building and internet governance. The eighth cyber dialogue took place in December 2022.

The EU has also organised specific **cyber dialogues with Japan, Brazil, India and South Korea,** as well as consultations with the ASEAN. An **EU-China Task Force** was also set up to deepen mutual trust and understanding, discuss the economic aspects of ICT security, work constructively in developing norms for state behaviour and promote the application of existing international law in cyberspace. A cyber dialogue with the UK is in development, as agreed under the Trade and Cooperation Agreement.

The EU also continued its **cyber capacity building projects** in the EU's neighbourhood, including the Western Balkans, Ukraine, Georgia and Moldova, as well as other partner countries experiencing a rapid digital development.

The EEAS has also been highly involved in the elaboration, dissemination and implementation of **confidence building measures (CBMs)** through several regional organisations, such as the Organization for Security and Co-operation in Europe (OSCE) and the ASEAN Regional Forum, to develop and maintain communication between states to defuse conflicts and prevent escalation.

The EU continues to promote a global, open, stable and secure cyberspace, respecting the **United Nations framework of responsible state behaviour in cyberspace**, notably within the UN First and Third Committees. The EU actively supports the establishment of a programme of action to advance responsible state behaviour in cyberspace.

Screening of foreign direct investment

Regulation (EU) 2019/452 establishing the EU framework for the screening of foreign direct investment into the EU[71] has been fully applicable since 11 October 2020. It **allows the Commission and Member States to review foreign direct investments** on the sole grounds of security or public order, and Member States to prohibit or condition the investment if specific risks are identified.

[71] OJ L 79I, 21.3.2019, p. 1.

The Regulation does not oblige Member States to maintain a screening mechanism. However, the Commission has repeatedly called to adopt and maintain fully fledged screening mechanisms. Currently 19 Member States have a mechanism in force, and many others are in the process of adopting one[72]. On average, the cooperation mechanism assesses more than 400 transactions annually.

On 20 June 2023, the **Joint Communication on a European economic security strategy**[73] was adopted. The strategy focuses on minimising risks arising from certain economic flows in the context of increased geopolitical tensions and accelerated technological shifts, while preserving maximum levels of economic openness and dynamism. Four categories of risks for the security of the Union have been identified: (1) resilience of supply chains; (2) physical and cyber security of critical infrastructure; (3) technology security and technology leakage; and (4) weaponisation of economic dependencies or economic coercion.

Building resilience against radicalisation and violent extremism

The **Terrorist content online regulation**[74] is applicable since 7 June 2022. Ensuring its full implementation is fundamental to prevent terrorists from misusing the internet to spread their ideology, intimidate, radicalise and recruit citizens online.

As mentioned in the 5th progress report on the implementation of the Security Union Strategy, the EU is also working to prevent foreign influence and funding supporting radical/extremists views in the Member States. Since the end of 2021, projects managed by the Commission are published as soon as the grant agreement is signed. The Commission's proposed revision of the Financial Regulation includes adding the issue of a 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 2022 and 2023**[75] 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 is making tools available to tech companies. These include the knowledge package of violent right-wing extremist groups, symbols and manifestos, detecting financing activities of violent extremists, and handbooks on borderline content and video gaming. The EUIF also revised the **EU Crisis Protocol**[76] to respond better to terrorist attacks with a cross-border online dimension. Work is ongoing to develop partnerships between governments and traditional media to report on terrorist attacks responsibly and strengthen resilience against misinformation.

[72] Member States that have no screening mechanism but where a legislative process is ongoing: Belgium, Croatia, Cyprus, Greece, Ireland, Luxembourg and Sweden.
[73] JOIN(2023) 20 final.
[74] OJ L 172, 17.5.2021, p. 79–109
[75] https://home-affairs.ec.europa.eu/system/files/2022-03/2022-2023%20Strategic%20orientations%20on%20a%20coordinated%20EU%20approach%20to%20prevention%20of%20radicalisation_en.pdf
[76] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2372

The EUIF is expanding its outreach to internet infrastructure providers and financial technology companies to address terrorist-operated websites and new technological developments. It has also funded a study on the effects of algorithmic amplification on people's journeys to radicalisation. The EUIF continues to provide alternative narratives to radicalised viewpoints and terrorist propaganda and supports fundamental rights and values through civil society empowerment programmes. The EUIF also published 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 to understand, detect, moderate and respond to borderline content better.

Increasing cooperation with partner countries

As part of the implementation of Action 18 of the Joint Framework on countering hybrid threats, **hybrid risk surveys** (HRS) have been launched with six partners: four in the Western Balkans (Albania, Kosovo*, North Macedonia and Montenegro) and two in the eastern neighbourhood (Moldova and Georgia). Also, one HRS has been offered in the southern neighbourhood (Jordan). In 2022, the EU started revisiting a few of the surveys. In this context, the EU relaunched the **HRS process with Moldova**, which provided its replies in February 2023. On this basis, a set of recommendations were prepared on gaps and vulnerabilities that can be addressed jointly, drawing on appropriate funding mechanisms. The EEAS and the Commission services also visited **Albania** in November 2022 to follow up on the HRS implementation.

Projects and other activities, in particular under the Commission's Technical Assistance and Information Exchange Instrument (TAIEX) Twinning and the Rapid Response Pillar of the Neighbourhood, Development and International Cooperation Instrument (NDICI), are ongoing in partner countries. Where relevant, they address recommendations from the HRS. From July 2022 to July 2023, around **20 TAIEX workshops and events on hybrid threats** took place.

In the **eastern neighbourhood**, the EU-funded regional CyberEast programme adapted a few of its activities resulting from Russia's war of aggression against Ukraine. A 2-day TAIEX multi-country workshop on Strategies to Counter Disinformation was organised in February 2023 to support Ukraine, Moldova and Georgia in detecting, analysing and devising suitable responses to disinformation.

In **Ukraine**, the Commission continued to support the country amid the ongoing war. In addition to the EUR 10.7 million for emergency cyber support, the Commission gave EUR 19 million for resilient digital transformation to strengthen the digital state and cybersecurity. Similarly, the Commission provided EUR 120 million in budget support, in which cyber resilience was one of the benchmarks.

The EU has financed and delivered equipment for a cyber lab, security software and hardware to the Ukrainian Armed Forces, as part of its ongoing support to Ukraine under the European Peace Facility. The cyber lab was unveiled in Kyiv in December 2022. With this support, Ukraine can build and further develop the cyber defence capacities of its armed forces. The Moldovan Armed Forces also received cyber defence support through the European Peace Facility (EPF). Through the Rapid Response Pillar of the NDICI, **Moldova** received EU support to address disinformation by increasing government cybersecurity capabilities as well

* This designation is without prejudice to positions on status and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

as to manage the crisis resulting from the influx of people fleeing war in Ukraine. Under bilateral programs, Moldova has received support to strengthen media outlets. A TAIEX workshop was organised in June 2022 with the State Protection and Guard Service and the Ministry of Internal Affairs on strengthening capacity on investigative techniques and intelligence gathering.

On 23 April 2023, the Council established a civilian mission to strengthen the areas of crisis management and hybrid threats, including cybersecurity and countering FIMI, in Moldova (EU Partnership Mission in the Republic of Moldova). It was formally launched by the Council on 22 May[77].

In **Georgia**, a Twinning project "Strengthening Cybersecurity Capacities" has been supporting those involved in cybersecurity. The EU has procured network protection equipment. In addition, under the EPF, negotiations have been successfully completed to support the Georgian Military Defence Cybersecurity Bureau.

For the **Western Balkans,** the Commission launched a comprehensive regional cybersecurity programme in March 2023 based on the regional identification and formulation study conducted in 2022 by the e-Governance Academy. A new regional action to improve protection of public spaces and critical infrastructure was also launched in March 2023. Similarly, CFSP-aligned countries (Albania, Montenegro and North Macedonia) were supported by the Rapid Response Pillar under the Neighbourhood, Development and International Cooperation Instrument (NDICI) to increase their resilience to hybrid threats resulting from Russia's war of aggression against Ukraine, in particular disinformation and cyber threats. A number of TAIEX missions took place across the region mainly to strengthen cyber-incident preparedness of the relevant authorities.

In its efforts to support the democratic resilience of its partners, the Commission approved a new multi-country action plan in November 2022. The plan creates an **EU-Council of Europe Horizontal Facility for the Western Balkans and Türkiye** – Phase III, focusing on strengthening the capacity of the Western Balkans and Türkiye to uphold the rule of law and ensure that fundamental rights and freedom of expression are protected.

In the **southern neighbourhood,** new programmes on maritime security and safety, in particular search and rescue and border management, were launched in Tunisia, Egypt and Libya. As part of the EU-funded regional CyberSouth programme, training and courses on tackling cybercrime were given to magistrates and law enforcement agencies.

EU-NATO cooperation

EU and NATO staff-to-staff interactions on countering hybrid threats continued within the well-established channels, as highlighted in the eighth annual progress report on EU-NATO cooperation. Staff-to-staff interactions and **cooperation on resilience** increased considerably during the reporting period. This was the result of the higher level of ambition in this area in both organisations, which was also reflected in the third Joint Declaration on EU-NATO cooperation[78], and the closer EU-NATO cooperation in response to Russia's war of aggression against Ukraine.

Under the Structured Dialogue on Resilience, a new EU-NATO **Task Force on the Resilience of Critical Infrastructure** was announced by Commission President Ursula von der Leyen and NATO Secretary General Jens Stoltenberg in January 2023. The Task Force

[77] Council Decision (CFSP) 2023/855.
[78] Joint Declaration on EU-NATO cooperation, signed in Brussels on 10 January 2023.

presented its final assessment report on 29 June 2023, in which it maps out challenges to critical infrastructure in the energy, transport, digital infrastructure and space sectors. The report presents recommendations to strengthen critical infrastructure resilience. As a contribution to the work of the task force, the HFC and NATO HAB conducted a parallel and coordinated assessment (PACA) of the threat landscape related to critical infrastructure, in line with the established practice of NATO-EU cooperation.

EU-NATO cooperation in the **cyber** domain has grown with an increase in cross-briefings and cross-invitations to cyber exercises and more regular exchanges. The EU policy on cyber defence also specifically highlights the need to strengthen EU-NATO cooperation in cyber training, education, situational awareness and exercises.

Staff exchanges at technical level continue to take place between CERT-EU and NATO Cyber Security Centre on the basis of the technical arrangement of 2016 between the two entities.

Cooperation on **FIMI** between the EU and NATO has a long tradition. EU and NATO staff frequently exchange in-depth analyses, real-time insights and work hand-in-hand to maintain shared situational awareness of hostile activities in the information environment, including through the EU Rapid Alert System. The EU and NATO regularly engage in mutual efforts to strengthen partner countries' strategic communication capabilities.

The EU and NATO continued to cooperate on **CBRN** defence and resilience issues. Dedicated staff talks took place in September 2022. These focused on: (i) capacity-building activities for partners; (ii) implementation of NATO's new CBRN defence policy; and (iii) CBRN implications of Russia's war of aggression in Ukraine. CBRN, including radiological safety and efforts to counter Russia's CBRN-related disinformation, has also regularly featured in the discussions of the EU-NATO staff coordination on Ukraine. NATO's Joint CBRN Defence Centre of Excellence (JCBRN Defence COE) cooperates with the EU on training and capacity-building activities for CBRN defence, including training on CBRN consequence management and other aspects of emergency response. The JCBRN Defence COE also supports the activities of the EU's CBRN Risk Mitigation Centre of Excellence Initiative, which works to build the resilience of a worldwide network of partners.

EU Protocol for countering hybrid threats and exercises

As announced in the EU Security Union Strategy, the **EU Protocol for countering hybrid threats**[79] was published in April 2023. The Protocol represents a revision of the 2016 'EU Hybrid Playbook', which outlines the various tools the EU can deploy to counter hybrid threats and campaigns, taking into account experience and institutional changes from the past years.

In 2020, the EU and NATO agreed to extend the **Parallel and Coordinated Exercise** (PACE) for 2 years (2022 and 2023)[80]. Under this new agreement, the EU, as the lead organisation, conducted the EU Integrated Resolve 2022 PACE exercise from 19 September to 18 November 2022. NATO led the Crisis Management Exercise 2023 (CMX23), conducted from 9 to 14 March 2023. As part of the exercises, the EU response to hybrid threats was tested, as was the staff-to-staff cooperation between EU and NATO.

[79] SWD(2023) 116 final.
[80] Plan for the Implementation of Parallel and Coordinated Exercises (PACE) between the European Union and NATO for 2022-2023, Doc. 13382/20, 26 November 2020.

Article 42(7) of the Treaty on European Union (TEU) and Article 222 of the Treaty on the Functioning of the European Union (TFEU)

The Strategic Compass includes a commitment to continue regular exercises, including cyber exercises, to further strengthen the EU's mutual assistance in case of an armed aggression, in line with Article 42(7) TEU. In November 2022, the EEAS and the European Union Institute for Security Studies, together with the Czech Presidency of the Council, organised **HybridTTX'22** – the first-ever table top exercise in the Council Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats. HybridTTX'22 was the second in a three-part sequence of exercises that began with a Cyber Diplomacy Toolbox exercise (CyDipTTX'22) on 16 November and concluded with a scenario-based policy discussion on implementing Article 42(7) TEU in the Council's Political and Security Committee (PSC). The exercise aimed to test the relationship between the Cyber Diplomacy Toolbox and the new EU Hybrid Toolbox. It enabled further discussions on the application of international law to state conduct in cyberspace, informed the development of the Implementing guidelines for the framework for a coordinated EU response to hybrid campaigns and provided a basis for an escalation in the scenario for the exercise in the PSC.

CSDP operations and missions

As EU military rapid response operations may be confronted with hybrid threats and must be able to operate in a hybrid threats environment, the updated **European Union military rapid response concept**[81] of 13 March 2023 includes an instruction to give due consideration to countering hybrid threats during the planning and preparation process, in line with the EU Guidance on countering hybrid threats during the planning phase of EU-led CSDP military operations and missions.

The Joint Communication on the EU Policy on Cyber Defence has highlighted the need for better cyber protection of CSDP operations and missions and has proposed setting up an EU Cyber Defence Coordination Centre. Currently work is in progress on a PESCO project for a Cyber Information Domain Coordination Centre.

CONCLUSION

During the reporting period, the evolving security landscape was marked by an increased use of hybrid threats and campaigns against the EU, its Member States and partners, especially in critical infrastructure and energy sectors. Concrete cases, such as the sabotage of the Nord Stream pipelines, prompted a rapid response at EU level, proving that the approach and tools set out in the 2016 Joint Framework, the 2018 Joint Communication, the EU Security Union Strategy and the Strategic Compass allow us to increase our resilience against hybrid threats and to respond to hybrid campaigns quickly. The entering into force of important initiatives, such as the CER Directive and the NIS2 Directive, the adoption of the Council recommendation on resilience of critical infrastructure have also confirmed the need to go even further, enhancing our efforts to strengthen our resilience and counter hybrid threats.

Implementation of the Strategic Compass initiatives and the EU Security Union Strategy played a key role in countering hybrid threats during the reporting period. The EU Hybrid Toolbox was put in place, the new EU Protocol for countering hybrid threats was published, the concept of the FIMI Toolbox was discussed in the Council, the Cyber Diplomacy Toolbox

[81] ST 7366/23.

was revised and the cyber defence policy was developed within the deadlines set by the Strategic Compass.

The number of initiatives included in this report show the importance of acting in different domains for countering hybrid threats effectively. Among other initiatives, the Joint communication on the update of the EU Maritime Security Strategy and its Action Plan was published, taking into account the increased hybrid threats in the maritime domain, including to maritime infrastructure. In March 2023, the EU released its Space Strategy for Security and Defence, which promotes the preservation of a safe, secure and sustainable space environment and the peaceful use of outer space.

Cooperation with the EU's partners gained momentum with the third Joint Declaration on EU-NATO Cooperation and the hybrid risk survey for Moldova. On 24 April 2023, the Council also decided to set up the EU Partnership Mission in the Republic of Moldova, which opens a new chapter for the CSDP's contribution to strengthening partner resilience to hybrid threats.

The increasing geopolitical challenges, in particular those related to the continued war of aggression by Russia in Ukraine, confirm the need to spear no efforts to protect the EU and its Member States against hybrid attacks in all sectors.