EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 23.6.2021
SWD(2021) 729 final

JOINT STAFF WORKING DOCUMENT

Fifth 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

Fifth 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

Countering hybrid threats is one of the most complex challenges the European Union (EU) and its Member States are facing. The EU response aims to enhance situational awareness, boost resilience in all critical sectors, provide for adequate response and recovery in case of crisis and cooperate with like-minded countries and organisations.

While Member States remain predominantly responsible for building resilience, detecting, preventing and responding to these threats, **actions at EU level** support and complement national efforts. Given the cross-border nature of hybrid threats and their EU-wide targeting, EU level coordination, integrating the external and internal dimension in a seamless flow and together with the whole-of-government and whole-of-society approaches at national levels, are vital to adequately counter them.

Since 2016, the EU has set up a broad array of measures aiming to create a holistic response across relevant instruments and actors involved to counter hybrid threats in a growing number of policy areas and has consistently adapted them to respond to ever evolving hybrid threat activities. The progress made on the implementation of measures announced in the *2016 Joint Framework on countering hybrid threats – a European Union response*[1] and further developed in the *2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats*[2], carried forward in close interaction with Member States, EU institutions and entities, as well as with international partners, notably the North Atlantic Treaty Organization, was described in four annual progress reports presented to the Council[3] which should be read in conjunction with the present report.

In its EU Security Union Strategy 2020-2025[4] of July 2020, the Commission set out a renewed EU approach to hybrid threats underscoring the growing role they have in the rapidly evolving security environment. The Strategy proposes a comprehensive focus to better counter ever more sophisticated hybrid attacks by state and non-state actors through mainstreaming hybrid considerations into policy making, streamlining information flows from different sources and systematically track and objectively measure progress in resilience building. It calls for a full spectrum of actions to ensure early detection, comprehensive analysis and awareness, enhanced resilience and prevention.

On 18 June 2020, the **European Parliament decided to set up a Special Committee on foreign interference in all democratic processes in the European Union**, including disinformation (INGE committee). The INGE committee will assess the level of hybrid threats in different spheres: major national and European elections across the EU, disinformation campaigns on traditional and social media to shape public opinion, cyber-attacks targeting critical infrastructure, direct and indirect financial support and economic coercion of political actors and civil society subversion. It will also identify solutions and

[1] JOIN (2016) 18 final
[2] JOIN (2018) 16 final
[3] JOIN (2017) 30 final; JOIN (2018) 14 final; SWD (2019) 200 final; SWD(2020) 153 final
[4] COM (2020) 605

propose tools to counter attempts to sabotage the European Parliament's core work. It will share its findings and conclusions in the format of a report at the end of its mandate.

The **December 2020 Council Conclusions**[5] called, in the context of the COVID-19 pandemic, for further enhanced responses at EU level to counter hybrid threats, including by strengthening resilience to counter hybrid threats, and highlighted, among others, the intensified spread of disinformation and manipulative interference.

This fifth progress report **takes stock of developments made since July 2020** on the full spectrum of actions of the *2016 Joint Framework on countering hybrid threats* and the *2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*. The report should be read in conjunction with the EU Security Union Strategy progress report[6] and the sixth progress report *on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*[7].

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

Recognising the hybrid nature of a threat at the national level

Member States continued to coordinate and exchange views and best practices on national measures to enhancing resilience and countering hybrid threats through the dedicated Horizontal Council Working Party.

In response to the December 2019 Council Conclusions *on Complementary Efforts to Enhance Resilience and Counter Hybrid Threats*[8] calling for a possible revision of the **Hybrid Risk Survey** in order to better address vulnerabilities to hybrid threats, Member States with the support of the Commission services and the European External Action Service (EEAS) launched a second hybrid risk survey in December 2020, focusing on domains identified by Member States as of particular importance. The responses of the Member States and contributions by EU institutions will be analysed by the Commission's Joint Research Centre (JRC) and findings will guide future actions of the Council in the framework of the Horizontal Working Party.

During the subsequent **German and Portuguese Presidencies** in the second half of 2020 and first half of 2021 respectively, the Council's Horizontal Working Party held regular meetings. Ambitious Council Conclusions[9] were adopted in December 2020 under German Presidency, reflecting on developments related, among others, to lessons learnt during the COVID-19 pandemic. During the Portuguese Presidency meetings focused on disinformation, foreign information manipulation and interference in Europe and the Southern Neighbourhood, on civilian and military Common Security and Defence Policy (CSDP) missions and operations, as well as on maritime aspects of hybrid threats, among others. Moreover, the Horizontal Working Party actively examined and contributed to follow-up actions with regards to the

[5] 14064/20
[6] COM (2021) 440
[7] https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf
[8] EUCO 9/19
[9] 14064/20

Security Union Strategy and further development of the hybrid toolbox as well as the European Democracy Action Plan[10] and the strengthening of the code of practice on disinformation.

EU Hybrid Fusion Cell

The EU Hybrid Fusion Cell (HFC) within the EU Intelligence and Situation Centre (EU INTCEN) has continued to provide **strategic analysis reporting on hybrid and cyber threats** to the decision-makers in the EU institutions and Member States. The HFC provided regular briefings in a written and verbal form to various Council working groups, notably the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats and the Horizontal Working Party on Cyber Issues. The HFC reporting has covered hostile activities and strategic objectives of various state and non-state actors which conduct hybrid activities as well as key events that might trigger an increase of hybrid attacks.

In order to achieve a common, inter-institutional, **EU-wide approach on hybrid threats and a comprehensive situational picture**, the HFC has engaged with multiple networks, integrating relevant bodies of the EU, Member States' intelligence community and governmental structures, academia, partner countries and organisations. Within existing limitations of classified information sharing, the HFC has maintained its **close cooperation with the North Atlantic Treaty Organization Hybrid Analysis Branch and the Centre of Excellence for Countering Hybrid Threats,** with the aim of strengthening situational awareness, mutual understanding of respective activities, and exploring further potential cooperation avenues.

The HFC has continued to develop the **Hybrid Trends Analysis** (HTA), which is used for monitoring hybrid threats and informing EU and Member States' decision-makers about the scale and intensity of hybrid threats targeting different domains in Member States and the EU Institutions. The Hybrid Trend Analysis also offers a brief insight into potential future developments.

Enhancing institutional resilience

Hybrid threats, including disinformation, are a critical issue for the EU institutions, bodies and agencies as well, and the EU was confronted to serious corporate incidents during 2020. The EU's ambitious policies in the domain of climate change, external relations and health are clearly targets for attackers who rely heavily on hybrid approaches. Progress has been made to increase institutional resilience through **pro-active monitoring of the cyber threats landscape.**

In 2020 and 2021, the **Computer Emergency Response Team for the EU Institutions**, bodies and agencies (CERT-EU) has continued to proactively monitor the cyber threat landscape in order to alert EU institutions, bodies and agencies of direct threats or inform them of significant new techniques, tactics and procedures (TTPs). In 2020/21, CERT-EU released 84 threat alerts with actionable information to help detection and mitigation of cyber threats. In 2020, CERT-EU released 175 threat memos and in 2021, as of 31 May, already 70 threat memos have been released. Topics of special interest for the hybrid threat landscape include: politically motivated hack and leak operations, tainted leaks, use of social media

[10] COM2020 (790) final

platforms and encrypted messaging apps for disinformation or influence operations, use of deep fakes by state-sponsored actors for disinformation and use of fake news websites.

Under the **Cybersecurity in the EU institutions, bodies and agencies pillar** of the *EU's Cybersecurity Strategy*[11], stakeholders' consultation and benchmarking of current policies are ongoing with a view to making proposals before the end of 2021, particularly, the Commission's proposal for common binding rules on cybersecurity for all EU institutions, bodies and agencies. The new cybersecurity rules will increase the capability to respond to rising threat levels and the overall level of cyber maturity of all EU institutions, bodies and agencies.

Securing free and fair elections and protecting democratic processes

The Commission continued to pursue a comprehensive approach to address democratic and electoral resilience and **adopted the *European Democracy Action Plan***[12] in December 2020. It sets out a broad framework to promote free and fair elections and strong democratic participation, support free and independent media, and counter disinformation. It proposes measures to ensure greater transparency in the area of political advertising[13] as well as against the abusive use of strategic lawsuits against public participation (SLAPPs). The Action Plan also sets out measures to counter disinformation as well as foreign information manipulation and interference. This includes measures to further refine definitions used to capture illegitimate behaviour in the information space, develop a common methodology and framework to collect systematic evidence of disinformation, and improve the existing EU toolbox for countering foreign interference. It also envisages a new joint operational mechanism to promote resilient electoral processes, which will build upon the work of the European Cooperation Network on Elections (ECNE).

The ECNE continued to support enhanced collaboration among Member States. In 2020, the discussions specifically took into account the efforts made for ensuring free and fair elections and a fair democratic debate in the context of the COVID-19 crisis. As one of the priority topics, the ECNE also addressed the effective and inclusive democratic participation for all EU citizens, as well as transparency of online political advertising and the fight against disinformation. A Presidency-led technical dialogue between the EU and the United States on resilient electoral processes within the framework of the European Cooperation Network on Elections is being resumed. Interlinkages between the ENCE and the EEAS-managed Rapid Alert System on Disinformation continued and further increased, including by cross-briefings between the networks.

Further, the Commission is preparing **guidelines on dealing with foreign interference targeting EU Research and Innovation Institutions**. The guidelines will have a twofold aim: protecting fundamental values by safeguarding academic freedom, integrity and institutional autonomy, and shielding students, researchers and innovators; and protect key research findings, from coercive, covert, deceptive or corrupting foreign actors. The guidelines will contribute to secure democratic processes.

[11] JOIN(2020) 18 final

[12] COM(2020) 790 final

[13] The Commission started preparations for a legislative initiative on transparency of political advertising. For details see: Political advertising – improving transparency (europa.eu)

Strategic communications

In the area of strategic communication, **EU efforts to tackle disinformation have continued in close cooperation with stakeholders**, including major online platforms active in the EU and major trade associations representing the European advertising sector. The *Code of Practice on Disinformation*[14], in force since October 2018 and co-signed by key stakeholders, has been instrumental. It has provided an innovative tool for ensuring greater transparency and accountability of online platforms as well as a structured framework for monitoring and improving the platforms' policies on disinformation.

To further strengthen the *Code of Practice on Disinformation*, the Commission on 26 May 2021 issued a guidance[15] as part of wider comprehensive actions to address disinformation and accompanied by complementary legislation for greater transparency of political advertising, as announced in the European Democracy Action Plan. The guidance sets out the Commission's views on how to address gaps and shortcomings of the Code[16], and how to create a more transparent, safe and trustworthy online environment. The guidance aims at evolving the existing Code of Practice towards a co-regulatory instrument, i.e. a "Code of Conduct", in line with the Commission's proposal for the *Digital Services Act*[17] for addressing systemic risks linked to disinformation.

In addition, a monitoring programme has been set up where platform signatories report monthly on actions taken to combat COVID-19 disinformation in the EU. It has provided an in-depth overview and transparency of the actions taken by platforms to counter disinformation around COVID-19 based on the Code of Practice on Disinformation's commitments, thereby putting the Code of Practice through a stress test.

On 10 June 2020, the Commission and the High Representative presented a **Joint Communication on Tackling COVID-19 Disinformation**[18]. It addressed the challenges brought about by the "infodemic", analysed gaps in the EU's approach to tackle disinformation related to the pandemic and called for more coordinated action, in line with the EU's democratic values, to address the risk COVID-19 disinformation poses to open societies. Furthermore, the **Commission put in place an internal network against disinformation**, which serves to facilitate knowledge sharing and training of Commission's communications officers. Within this network, a dedicated COVID-19 vaccine disinformation working group was created to coordinate communication responses of relevant services.

Significant progress has been made on **strengthening the work of the EEAS Strategic Communications Division and its Task Forces.** The division has recruited two experts specifically on China. To maintain the operations and further enhance the work of the three Strategic Communications Task Forces (East, South and Western Balkans) and reinforce work on other emerging priorities and geographical areas, the EEAS Strategic Communications Divisions' sustainable funding has been secured under the 2021-2027

[14] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
[15] COM(2021) 262 final
[16] identified in the *assessment of the Code of Practice on Disinformation* SWD(2020)180
[17] COM(2020) 825 final
[18] JOIN(2020) 8 final

Multiannual Financial Framework[19], including for EU Delegations for their communication and outreach efforts. This is further bolstered with the recruitment of staff across 27 EU Delegations in the EU Neighbourhood, Russia, Turkey and the Western Balkans. Working in close coordination with headquarters, this new network of delegation-based communications officers strengthens EU capacities for coordinated action. On the Commission's side the work in this area is complemented by the **internal network against disinformation**. The network and the EEAS launched joint disinformation attack simulations and collaborated to produce strategic reports.

To improve the Union's capabilities to detect, analyse and expose disinformation, the EEAS Strategic Communications and Information Analysis Division has built up **in-house data expertise and tools**. A dedicated data team supports and expands the division's activities and oversees the implementation of data analytics resources. Following the call of the European Democracy Action Plan to establish a common framework and methodology to collect systematic evidence of disinformation incidents, the EEAS Strategic Communications Division has started conceptual work on such a framework and methodology.

Throughout the pandemic, the EEAS Strategic Communications Division has released public reports on COVID-19 related disinformation, covering activities by Russia, China and other relevant actors. **The East Stratcom Task Force** continued to raise awareness about pro-Kremlin disinformation campaigns, notably with regard to the COVID-19 pandemic and Western vaccines, pushing back the attack on the EU, its Member States and the European Medicines Agency. Direct response to disinformation campaigns has been coupled with increased efforts to ensure support for the independent media in the Eastern neighbourhood and proactive communication with help of the EU Delegations on the ground. The activities and actions carried out by the **Western Balkans Task Force** continued in the form of public campaigns and strategic engagements with partners and stakeholders in the region. By practicing public and cultural diplomacy, the Western Balkans Task Force sought to go beyond traditional information channels and translate its actions in effective and varied communication products, adapted to the local context. Particular attention has been given to the monitoring of disinformation in the region, especially during COVID-19 pandemic, with a view to expanding and consolidating the analytical capabilities of the Task Force as well as the understanding of the regional information environment. **The Task Force South** continued to effectively address disinformation in the Middle East-North Africa region through the expansion of its analytical capability to detect and monitor disinformation in the region. It also engaged in designing pro-active and positive communications strategies and narratives, while also promoting the support to independent media as well as to the resilience of civil society actors and local partners in the region. In particular, the Task Force South designed and implemented tailored systemic and tactical responses, most notably in Libya and Syria, using all means available in the StratCom toolbox. In this sense, the pilot @EUinArabic account and Regional Media Officer position have also widened the EU proactive communications reach in Arabic. The Task Force South is also expanding its monitoring capabilities by establishing an early warning system and a crisis communications protocol, working to strengthen civil society actors and independent media operating in the region. In the wake of the COVID-19 pandemic, the Commission also launched several actions under

[19] This includes EUR 11.1 million in 2021 for the EEAS's work on addressing the threat that disinformation, information manipulation and foreign interference pose to the EU's social cohesion and security and EUR 12.88 million for EU Delegations for their communication and outreach efforts.

the Instrument contributing to Stability and Peace aimed at **addressing the rising disinformation in conflict-affected contexts** in Africa, Latin America, the Middle East, North Africa and Asia. This has strengthened the capacities of journalists and media actors, civil society organisations, and other fact-checkers to detect and respond to rumours and disinformation. Activities have also included the establishment of regional and global online resources, awareness raising campaigns on COVID-19, promotion of media literacy, and the production and broadcasting of radio programmes to inform and engage the broader public and hard-to-reach communities.

Other disinformation-related engagements carried out under the Instrument contributing to Stability and Peace have focused on Libya and Ukraine. In Libya, analysis of disinformation trends or "coordinated inauthentic content" on social media have been undertaken in the framework of the EU Libya Expertise, Analysis and Deployment project (EULEAD). In Ukraine, the Countering disinformation in southern and eastern Ukraine project aims to engage the population and strengthen their resilience to disinformation attacks by supporting journalists and youth in the east and south of the country, and implementing activities aimed at increasing media literacy and critical thinking.

The EEAS teamed up with the North Atlantic Treaty Organisation (NATO) Stratcom Centre of Excellence to develop a **training programme to contribute to the long-term resilience of EU staff against disinformation**. The interactive exercise that focused on the response to a coordinated disinformation attack was delivered to more than 100 EU staff members working at the European Union Representations in the EU Member States, European Parliament Liaison Offices in the EU Members States and the EU Delegations in the Eastern Partnership countries.

The EEAS Strategic Communications Division has strengthened its tools and analytical capacity to **address emerging risks, and areas of growing importance like providing additional support to Common Security and Defence Policy (CSDP) Missions and Operations**.

The EEAS-managed **Rapid Alert System on Disinformation** (RAS), launched on 18 March 2019, has been active for over two years and proven to be a useful, long-term platform to connect all EU Member States and relevant EU Institutions on a daily basis. The EEAS, in close cooperation with the European Commission services and EU Member States, has continued to strengthen the RAS to further increase cooperation inside the EU on situational awareness and policy development in the field of tackling disinformation, including foreign efforts to manipulate the EU's information space.

In line with its mandate, the RAS has increased cooperation with the G7 Rapid Response Mechanism (RRM) and with NATO, as set out in the 2018 Action Plan against Disinformation. A setting up of a dedicated "International Cooperation Space" that facilitates direct exchanges between the EU Institutions and services, Member States and these international partners was finalised in spring 2021.

To ensure a close cooperation with key partners, effective information sharing and a thorough understanding of deliberate manipulation of the information environment, the EEAS is in close contact with like-minded partners inside and outside the EU including through bilateral dialogues. The EEAS Strategic Communications team is in close contact with other international groups working on this issue. Additionally, contacts and cooperation with stakeholders from the civil society and private industry have been built up further.

EU funding has been provided, through the Connecting Europe Facility Programme, to a European Digital Media Observatory (EDMO). EDMO aims to scale up cooperation between independent fact-checkers and academic researchers and improve knowledge and scrutiny around disinformation in the EU. It will operate through national hubs, which will become operational in summer 2021. A central platform for the exchange between fact-checkers, academics and other relevant stakeholders is already operational. These stakeholders' inputs can support work carried out by the Strategic Communications Division and its Task Forces by providing additional evidence about possible disinformation campaigns conducted by hostile actors. The Commission has started to explore potential cooperation between RAS and EDMO.

Further, as noted in the European Democracy Action Plan, **strengthening the role of education** and training in view of tackling disinformation through equipping citizens **with digital literacy skills** is vital if citizens are to feel informed, empowered and safe when navigating the online world. Likewise, low levels of digital skills pose risks to the democratic functioning of societies and act as a barrier to social inclusion. Against this background, the Commission adopted the **new Digital Education Action Plan**[20] (2021-2027) in September 2020, which provides the way forward in accelerating the rollout of accessible, high quality and inclusive digital education for all learners across Europe. The Action Plan includes a dedicated action focusing on the **development of guidelines for teachers and educational staff** to foster digital literacy and tackle disinformation which will be informed by a Commission Expert Group. The guidelines will aim to provide teachers and educational staff with better awareness and knowledge on disinformation, promote a broad understanding of digital literacy through education and training and enhance the responsible and safe use of digital technologies. The guidelines will be launched in 2022 as part of a "back-to-school" campaign across Europe.

Additionally, the Commission will continue to support media literacy through the **Erasmus+ programme and the European Solidarity Corps** which funds projects contributing to the bottom-up mobilisation of education, training and youth actors against disinformation. Lastly, the **annual theme for eTwinning in 2021 is "Media Literacy and Disinformation"**[21] and includes the organisation of activities both at European and national levels including professional development opportunities for teachers, online cross-border projects by teachers and their students, the annual eTwinning conference in October 2021, articles and resources for teachers[22], and dedicated communication campaigns[23].

Centre of Excellence for Countering Hybrid Threats

The Helsinki based European Centre of Excellence for Countering Hybrid Threats (the Hybrid CoE) has continued to make progress with a **growing participation, a broad-ranging work programme** and a steady budget. As of April 2021, it has 28 members from both the EU Member States and the NATO allies. Further countries are expected to join. The Hybrid CoE continues to provide pro-active support through dedicated educational events,

[20] COM(2020) 624 final
[21] https://www.etwinning.net/en/pub/newsroom/highlights/etwinning-annual-theme-2021-m.htm
[22] https://www.etwinning.net/en/pub/newsroom/highlights/simple-ways-to-address-disinfo.htm
[23] https://www.etwinning.net/en/pub/newsroom/highlights/how-to-be-smart-online---etwi.htm; https://twitter.com/GabrielMariya/status/1366717458502008835

including seminars, workshops and conferences. In the course of the year, the Hybrid CoE has also ramped up its capability to offer different exercises on hybrid threats.

Cooperation with key stakeholders has raised awareness and contributed to shared assessment on hybrid threats. Close cooperation with the rotating Council Presidencies has contributed to shaping the agenda of Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats.

The Hybrid CoE has also contributed to a number of **hybrid scenario-based discussions and exercises**. In January 2021, it facilitated a scenario-based discussion on Article 42.7 of the Treaty on European Union for the Political and Security Committee. Additionally, the Hybrid CoE facilitated a workshop focusing on hybrid deterrence in the context of the Strategic Compass. It has also continued to facilitate further EU-NATO cooperation, including workshops and other staff-to-staff interactions.

In November 2020, **the Hybrid CoE together with the Commission's Joint Research Centre launched a conceptual model as the basis for the conceptualisation and characterisation of hybrid threats at EU and national levels**: *"Landscape of Hybrid Threats: A conceptual model*"[24]. A follow-up joint report from the Joint Research Centre and the Hybrid CoE focusing on resilience against hybrid threats is under preparation and will be presented at the beginning of 2022.

The Hybrid CoE and the Joint Research Centre are also partners in a network, funded under Horizon 2020, which brings together security practitioners, stakeholders, academics, industry players and small and medium enterprises across the EU. In April 2020, the network **EU-HYBNET** started its activities, focusing on monitoring relevant developments in research and innovation with respect to countering hybrid threats, including recommendations for uptake and industrialisation and definition of common European requirements. The network will run until 2025 and will then be integrated into the Hybrid CoE.

Cooperation between the Hybrid CoE and the European Defence Agency (EDA) has been pursued, with a view to contributing to the implementation of the EU's Capability Development Priorities derived from the 2018 Capability Development Plan (CDP). Since 2019, the EDA has been contributing to the workshops organised under the HyFUTec (Hybrid Warfare: Future and Technologies) project led by the Hybrid CoE, with both capability planning and Research and Technology specialists. The project aims at the assessment and improved understanding of the disruptive potential of new and future technological trends, as catalysts of hybrid warfare and conflict.

Protection and resilience of critical infrastructure

Progress was made to ensure that **Member States and entities providing essential services within Europe are better equipped to deal with hybrid risks.** On 16 December 2020, the Commission adopted the proposals for a *Critical Entities Resilience (CER) Directive*[25] and for the revised *Network and Information Systems (NIS2) Directive*[26], which are currently under discussion by the co-legislators. The CER-Directive aims to enhance the resilience of entities

[24] Giannopoulos, G., Smith, H., Theocharidou, M., *The Landscape of Hybrid Threats: A conceptual model*, European Commission, Ispra, 2020, PUBSY No. 117280

[25] COM(2020) 829 final

[26] COM(2020) 823 final

that provide essential services on which European citizens and the functioning of the internal market depend. The proposal includes the expansion of the sectoral scope of EU-rules two to all together ten sectors. It obliges critical entities to perform risk assessments and implement resilience enhancing measures and puts forward a comprehensive set of rules for improved cooperation between Member States, a long-term and strategic approach as well as dedicated support for critical entities. In order to ensure coherence between the CER and the NIS2 Directives, all critical entities identified under the CER Directive would be subject to cyber resilience obligations under NIS2, therefore allowing for a future-proof cyber-physical resilience framework.

Projects for resilience against hybrid threats in sectors such as energy, space, water, health, transport, communication and finance are funded with EU budget. Ten Horizon 2020 projects from the Secure Societies strand are supporting resilience with a combined EU contribution of around EUR 77 million, including the project STOP-IT that deals with the cyber-physical resilience of water suppliers. Furthermore, two additional projects have been preselected for funding in 2021 and resilience of critical infrastructures will be a priority in the first work programme of Horizon Europe, with a dedicated call for proposals worth EUR 10 million to counter hybrid threats[27].

Energy security of supply and energy infrastructure

Progress has been made in the area **of security of gas supply,** where under *Regulation (EU) 2017/1938 concerning measures to safeguard the security of gas*[28] now all Member States have adopted their national preventive action plans and emergency plans. These plans take into account the risk assessments made at regional and national levels, considering political, technological, commercial, social and natural risks, including cyberattacks, sabotage, and terrorism. Member States updated some regional risk assessments of 2018 to take account of new gas infrastructures which had recently entered into operation. Work continued to implement the solidarity provisions of the regulation as regards technical, legal and financial arrangements.

Ad hoc meetings were held with experts from Member States and industry associations, within the different Coordination Groups on electricity, gas and oil security of supply, with a view to monitor and analyse the impact of the pandemic on the security of gas supply and business continuity. As a result of this work, the Commission **issued a *Staff Working Document, on Energy Security: Good Practices to address Pandemic Risks***[29].

Progress has also been made in the area of **security of electricity supply**. Member States are obliged to prepare, by January 2022 (and to update every four years), Risk Preparedness Plans for electricity containing measures to prevent and mitigate identified risks. The obligations follow from the *Regulation 2019/941 on risk-preparedness in the electricity sector and repealing the Directive 2005/89/EC26*[30]. The plans are based on risks identified at national level by Member States, but also on regional risks, which are relevant for several Member States and include hybrid threats. The European Network of Transmission System Operators

[27] Work programme to be published in June: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/horizon
[28] OJ L 280, 28.10.2017
[29] SWD(2020) 104 final
[30] OJ L 158, 14.6.2019

(ENTSO-E) identified such regional risks for the first time in September 2020 and will carry out further updates at least every four years. Additional mandatory elements include a mechanism for the exchange of information during a crisis and to issue an early warning to the Commission and Member States when a crisis may occur.

At the end of May 2021, the Commission completed a **study to identify the critical supply chains for energy security and clean energy transition.** The study proposes measures for improving their resilience against pandemics and other threat scenarios. Its findings and recommendations will feed into the relevant Commission work streams, such as those addressing issues related to the availability of critical raw materials for renewable energy technologies, potential bottlenecks in manufacturing certain components for producing renewable energy, and addressing cyber threats stemming from suppliers of products and services.

Following its re-launch in June 2020, the **Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)** has met several times. The network has brought together more than 60 operators from 21 Member States to discuss topics such as risk assessments, mechanism to exchange information and the financing of security.

For addressing energy security challenges, including the protection of defence-related critical energy infrastructure, the **Consultation Forum for Sustainable Energy in the Defence and Security Sector** (CF SEDSS) - an EU funded initiative managed by the EDA - aims to assist the Ministries of Defence of Member States and related stakeholders in reducing energy costs and ecological footprint while increasing operational efficiency and resilience. In this context, the CF SEDSS explores the benefits that could be achieved in the defence and security sectors from implementing the Commission's related energy policy framework while contributing to implementing the European Green Deal[31].

To support the Ministries of Defence' efforts to enhance the resilience of defence-related critical energy infrastructure against hybrid threats and address relevant vulnerabilities, a **specific research study and a table-top exercise are to be developed** as part of the CF SEDSS phase III. The study entitled "Increasing the resilience of defence-related critical energy infrastructure against hybrid threats" will provide Ministries of Defence with a conceptual basis to develop appropriate measures in the domain of preparedness and response for ensuring the resilience of those critical energy infrastructures (CEI) that the defence sector depends on for their sustainability and effectiveness. To ensure coherence in the European landscape, the study's methodological approach will rely on the conceptual model developed by the Hybrid CoE and the Commission's Joint Research Centre. In collaboration with the Commission, the EDA will also organise, in the context of the CF SEDSS III, a table-top exercise to explore the effects of hybrid threats on defence-related CEI. The exercise will test the defence prevention and response planning and capabilities with the objective to produce lessons learned and recommendations for improving processes and procedures and identifying how the EU can complement national efforts. The findings and key recommendations of the two respective activities will also contribute to implementing the EU's Climate Change and Defence Roadmap[32], the first-ever EU action plan to address the links between defence and climate change, as part of the wider climate-security nexus.

[31] https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en
[32] 12741/20

The **EDA has also launched research projects** such as the Smart Camps Technical Demonstrator, Smart Blue Water Camps, the Total Energy and Environment Military Capability Assessment Framework, and the sustainable defence concept along with the toolkit which has been released to the Member States' authorities and is currently being tested and evaluated by them. In addition, the EDA has initiated a project (ARTENET) with the primary objective to explore the role of artificial intelligence and its potential applications to the military energy domain.

In the **area of nuclear infrastructure**, the Commission is monitoring the effective transposition and implementation by the Member States of the *EURATOM nuclear safety legal framework*[33]. This includes monitoring - through the European Nuclear Safety Regulators Group (ENSREG) - the implementation of the outstanding safety improvements identified in the EU's post-Fukushima stress tests. The Commission and ENSREG have started preparations for the second EU topical peer review. They will also continue to follow up on the implementation by the participating countries of the recommendations of the topical peer review conducted in 2017-2018 on the ageing of nuclear power plants and research reactors.

In the context of the **European Reference Network for Critical Infrastructure Protection** (ERNCIP), the Thematic Group on Radiological and Nuclear Threats to Critical Infrastructure is currently working on the following topic: "Requirements and capabilities needed for testing of robotic equipment carrying measurement devices for the detection of Chemical, Biological, Radiological, Nuclear, and Explosives threats in an authentic environment". The report is expected in the last quarter of 2021.

In the context of the **Generation IV International Forum** (GIF), which carries out Research and Development on the new generation of nuclear reactors, six technologies are currently under investigation. The Proliferation resistance and Physical Protection (PR&PP) working group with the participation of the Commission is updating its white papers on the PR&PP features of the six GIF reactor technologies. The papers will address the resistance of the systems against threats posed by State actors, e.g. diversion of nuclear material, misuse of technology, physical protection robustness against threats posed by non-state actors such as theft of nuclear material and sabotage. The six white papers are expected to be completed in 2021.

Transport security

For all areas of transport, namely civil aviation, maritime and land transports, the Commission, together with the relevant agencies, maintains a continuous dialogue on emerging security threats, including those of a hybrid nature, with Member States and contracting parties to the Agreement on the European Economic Area, industry and other stakeholders. This is in order to build up the knowledge and capacity to react to those threats and effectively managing related risks. Security is a necessary precondition to ensure the resilience of infrastructures and critical entities that provide essential services in transport.

[33] Directive 2009/71/Euratom, OJ L 172, 2.7.2009, p. 18 and its amendment, Directive 2014/87/Euratom, OJ L 219, 25.7.2014), Directive 2011/70/Euratom on the Spent Fuel and Radioactive Waste Directive, OJ L 199, 2.8.2011, p. 48 and Directive 2013/59/Euratom laying down basic safety standards for protection against the dangers arising from exposure to ionising radiation, OJ L 13, 17.1.2014, p. 1

In the area of **land transport security,** the Commission has continued to support the exchange of relevant experience, policies and best practices[34]. The Expert Group on Land Transport Security (Landsec) meets four times a year and assists the Commission to foster exchanges of relevant experience, policies and practices between the Member States and the various parties involved. Critical transport entities are also within the scope of the mentioned Commission's proposal for a *Directive on the resilience of critical entities*.

In the **area of rail security,** the Commission reached almost full implementation of the 2018 action plan to improve the security of rail passengers and staff[35], with the support of the EU Rail Passenger Security Platform. This Platform, which is composed of Member States' authorities competent in the field of rail security and of interested stakeholders, adopted a number of good practices documents regarding, for instance, risk assessments, insider threat mitigation and detection technologies. The Platform also serves as a forum to exchange good security practices and foster greater cooperation among Member States in the area of rail security.

In the area of **maritime and aviation security**, the Commission has established common rules and standards aimed at protecting aviation and maritime infrastructures from unlawful interference.

In the aviation sector, the Commission continued to carry out its regular monitoring of emerging threats, including hybrid threats, to adapt the Aviation Security (AVSEC) baseline. The Commission also continued to ensure a high level of protection of civil aviation against acts of unlawful interference, supported by the Commission's aviation security inspections system, in accordance with the applicable EU legislation. In 2020, the Commission continued inspections regarding the implementation of the EU's civil aviation security rules in Member States in accordance with its inspection strategy using remote methods[36]. Further, the EU has incorporated the information sharing elements of the Standards and Recommended Practices of the International Civil Aviation Organization into the EU AVSEC legislative acquis.

Under the Conflict Zone Alerting System, common risk assessments take place on a regular basis under the lead of the integrated EU aviation security risk assessment group. The aim is to share information on the assessment of risks arising from conflict zones in a timely manner. The outcomes of the integrated EU aviation security risk assessment group support the decision making process on possible mitigation measures, including the issuance of a Conflict Zone Information Bulletin (CZIB) or information notes by European Union Aviation Safety Agency.

In addition to risks arising from conflict zones, including unconventional conflicts of hybrid nature, the safety of international civil aviation may be put at risk by actions conducted by states abusing existing international rules regulating civil aviation including unplanned escorts of civilian flights by military aircrafts. As a result, the European Council strongly condemned

[34] LANDSEC, the Expert Group on Land Transport Security, assists the Commission in formulating and implementing the European Union's activities aimed at developing policy on security relating to land transport, and to foster ongoing exchanges of relevant experience, policies and practices between the Member States and the various parties involved

[35] https://ec.europa.eu/transport/modes/rail/news/2018-06-12-action-plan-security-rail-passengers_en

[36] In 2020, the Commission carried out 11 comprehensive inspections covering airports, air carriers and entities in 7 countries

the forced landing of a Ryanair flight in Minsk, Belarus[37], on 23 May 2021, endangering aviation safety[38].

In March 2021, the European Union Aviation Safety Agency – with the support of the Commission – issued guidance to help aviation operators and national authorities to manage drone incidents at and around airports[39]. In April 2021, the Commission adopted a regulatory framework for the European **unmanned traffic management** concept[40] (the U-Space), which should make it easier for authorities to distinguish between cooperative and non-cooperative, potentially malicious drones overhead. The EDA has organised a series of workshops with participating Member States and industry to exchange information on national projects, to share lessons learned and to harmonise requirements.

Within the framework of EDA's Key Strategic Activities (KSA) work-strand, Counter Unmanned Aerial System is one of the 10 topics selected for in-depth industrial assessment within the 2021 annual cycle, according to the Steering Board Decision of January 2021.

On maritime security, the Commission, the EEAS and the EDA continued to support, in line with the revised EU *Maritime Security Strategy Action Plan* (EUMSS AP)[41], a coordinated response to challenges affecting people, activities, and infrastructure in the maritime domain, including to hybrid threats. A new *implementation report on the EUMSS AP*[42] was adopted on 23 October 2020, based on the inputs from Member States, EU institutions and agencies. Progress has already been made in enhancing the overall resilience of EU critical maritime infrastructure.

Through the *European Union Maritime Security Strategy* (EUMSS), the Commission assesses and improves the resilience of critical maritime transport infrastructure, such as port security, sea lines of communication, energy infrastructure, offshore installations and telecommunications networks and sensors (e.g. cables), including under water. In particular, the Commission ensures, mainly through the Commission's maritime-security inspections system that ships, ports and port facilities are properly secured and protected according to international and EU legislation on maritime security[43].

Further, the Commission continued to engage with stakeholders and Member States to improve passenger ship security, focusing on the protection of passengers and staff. To this end, the Commission initiated cooperation with Member States that will lead to risk assessment at EU level.

---

[37] On 23 May 2021, Ryanair flight FR4978 from Athens to Vilnius was diverted to Minsk airport and escorted there by a Belarus Mig-29 fighter jet. Belarusian flight controllers notified the crew of a potential security threat on board as it was flying through Belarus's airspace and instructed it to divert to the Minsk airport. Upon landing, authorities detained journalist Roman Protasevich and Sofia Sapega. Belarus authorities confirmed that no bomb was found on board. The aircraft was diverted before it was due to cross into Lithuanian airspace. After seven hours on the ground, the plane took off and landed in Vilnius.

[38] https://www.consilium.europa.eu/en/press/press-releases/2021/05/24/european-council-conclusions-on-belarus-24-may-2021/

[39] https://www.easa.europa.eu/sites/default/files/dfu/drone_incident_management_at_aerodromes_part1_website_suitable.pdf

[40] C(2021) 2671 final, C(2021) 2672 final, C(2021) 2673 final

[41] 10494/18

[42] SWD(2020) 252 final

[43] The Commission carried out inspections of 7 national entities, 3 ports, 6 port facilities and 2 ships

Regarding maritime surveillance, the transitional phase put in place in May 2019, with the aim to facilitate the transition of the Common Information Sharing Environment for the maritime domain (CISE) from the pre-operational validation status to a fully operational network, has been extended until the fourth quarter of 2023. In the context of hybrid threats, CISE can provide a comprehensive understanding of the pattern of life in the maritime domain, enabling the definition of thresholds and therefore supporting European and National authorities to properly act against this kind of threats.

The EDA has continued to further develop the Maritime Surveillance (MARSUR) project, to improve exchange of maritime surveillance data in the defence sector and contribute to cooperation in the CISE framework. The MARSUR network was chosen to support the Coordinated Maritime Presences pilot case in the Gulf of Guinea, upon which further contributions towards a maritime surveillance network could be developed.

In addition, the Commission continued to monitor conflictive events or situations that could impact maritime security, including piracy and maritime disputes that could disrupt shipping and trade routes of EU interest. In view of the fact that the EU and European Economic Area Members control over 40 % of the world's merchant fleet and that the EU is a major trading block, hybrid activities, incidents or attacks on existing and future maritime trans-oceanic trade routes could have significant disruptive effects on value and supply chains in Europe[44].

The Hybrid CoE also organised events and educated institutions' and Member States' maritime operators to enhance their preparedness.

Border and supply chain security

The inter-agency cooperation **in support of coastguard function activities** between the European Fisheries Control Agency (EFCA), the European Maritime Safety Agency (EMSA) and the European Border and Coast Guard Agency (FRONTEX) has been further developed. On 18 March 2021, a new tripartite working arrangement was signed among the agencies EFCA, EMSA and FRONTEX enabling them to assist the Member States' national authorities more effectively, contributing also to countering hybrid threats in the maritime domain.

In the area of **border security**, in September 2020, the Commission adopted a *proposal for a Screening Regulation*[45]. The objective of screening is to better manage mixed migration flows by ensuring that the identity of migrants but also any potential security risks are quickly discovered. The screening will consist among other aspects of an identity check against information in European databases, registration of biometric data in the appropriate databases, and a security check through a query of relevant national and Union databases, in particular the Schengen Information System (SIS), to verify that the person does not constitute a threat to internal security.

[44] The Commission closely monitored UNCLOS/international law compliance, maritime disputes and maritime incidents, with a possible effect on EU interests or risk of potential disruption, mainly regarding the freedom of navigation in the current (or future) international shipping routes; including developments in the South China Sea, Taiwan Strait, the gradually opening Northern Sea Route and the trans-Arctic routes, or the lasting sabotage attacks and maritime incidents in the HoA/Gulf of Aden, around the strategic Bab-el-Mandeb Strait.
[45] COM(2020)612

The Commission also adopted an *implementing regulation on the situational pictures of the European Border Surveillance System*[46] (EUROSUR) regarding information exchange and cooperation as well as situational awareness, risk analysis and supporting to the planning and conduct of border control operations.

To increase the structured approach to **customs risk management** with a view to making controls more effective and to reduce financial and non-financial risks to the EU and its citizens whilst ensuring competitiveness of legitimate EU business, the Commission is currently preparing a new Customs Risk Management Strategy. As part of the implementation of the EU Strategy and Action Plan for strengthening customs risk management[47], the Commission is also developing a new customs advance cargo risk management system (ICS2), enabling collaborative safety and security risk analysis before goods arrive in the EU or are loaded for transport to the EU. ICS2 for air express and postal was launched in March 2021. A feasibility study of interoperability of security and border management systems with customs systems will be launched soon.

In the area of **supply chain security**, in November 2020 the Council and the European Parliament reached a political agreement on a proposal for a new Export Control Regulation[48] that significantly enhances the EU's capacity to address security risks in strategic supply chains and counter aggressive technology acquisition actions by foreign entities of concern engaged in the destabilising acquisition of dual-use items, including civilian goods and technology that may be misused to undermine international security.

The update of the new Industrial Strategy[49] of May 2021 initiated further steps to strengthen the EU's strategic autonomy. It includes a first analysis of the EU's strategic dependencies across sensitive industrial ecosystems. The Commission will carry out a second stage of reviews of key areas and establish a periodic monitoring system. The updated strategy proposes further steps to engage with partners in third countries to diversify the EU's imports and strengthen existing supply chains. The update also calls for building the EU's domestic capacity in strategic areas. For example, it announces setting up new industrial alliances for microelectronics as well as cloud and edge services. Further actions to facilitate EU capacity building include the preparation a standardisation strategy to support a more assertive stance on European interests in standardisation. Also, a structured dialogue process is ongoing to detect vulnerabilities and dependencies in EU supply chains as regards medicines as announced in the EU Pharmaceutical Strategy of November 2020.

The Commission has been working to **safeguard the Union's strategic assets, interests, autonomy, or security in the research and innovation** domains through the implementation of article 22(5) of the *Horizon Europe Regulation*[50], allowing to limit the participation of certain entities controlled or established outside the Union to specific research actions.

[46] Commission Implementing Regulation (EU) 2021/581 of 9 April 2021 on the situational pictures of the European Border Surveillance System (EUROSUR) OJ L of 12.4.2021. p. 3.
[47] COM(2014) 527 final.
[48] 2016/0295(COD)
[49] COM(2020) 102 final
[50] COM/2018/435 final

Limitations will be inserted exceptionally, where duly justified and strictly necessary, without compromising the extensive openness of the framework programme[51].

Space

For security actors (police, border management, civil protection, defence, etc.), the possibility to access the EU autonomous space enabled services, in particular for the communication, navigation and timing and earth observation, is essential. The EU Satellite Centre (SatCen) provided to the EU Intelligence and Situation Centre satellite imagery services that allow faster, better and more accurate identification of facts and interpretation of matters while identifying deep fake geospatial information which other non-specialised centres and agencies cannot detect.

In 2020, Copernicus contributed to support the security needs of the EU and to counter hybrid threats with the **provision of situational awareness through the Copernicus security service**, including border surveillance, maritime surveillance and support to EU external action. In 2020, the updated Copernicus risk and threat analysis identified the main potential threats and risks, in particular as to cybersecurity, for the system. This analysis will be the basis for further enhancement of the security and resilience of the programme's infrastructure. Initial work on the evolution of the Copernicus Security Service has started in close cooperation with the relevant EU services and agencies.

In order to **increase the overall Galileo Open Service robustness**, it has been decided to include an authentication feature in the Galileo Open Service signals, the so called Open Service Navigation Message Authentication (OS NMA) intended to facilitate the protection of Galileo users equipped with OS NMA compatible receivers. The Galileo OS NMA system end-to-end tests have started in 2021 and the start of Galileo OS NMA service provision is currently planned in 2023. Galileo Public Regulated Service authorised governmental users are able to access a more robust and resilient Galileo positioning and timing services based on encrypted signals.

In the area of **satellite navigation**, the Commission is currently undertaking a new initiative to foster the use of Galileo in critical infrastructure for timing and synchronisation based on space based services including in energy, telecommunications as well as bank and finance transactions networks. This aims at increasing the resilience of the infrastructures in Europe that are critical for security and the economy by making them gradually less dependent on foreign satellite navigation systems (e.g. Global Positioning System (GPS), Globalnaja Nawigacionnaja Sputnikowaja Sistiema (GLONASS) or the Chinese BeiDou). This initiative considers awareness actions on Galileo's and European Geostationary Navigation Overlay

[51] Article 22(5) contained in the Horizon Europe Regulation reads as follows – "*For actions related to Union strategic assets, interests, autonomy or security, the work programme may provide that the participation can be limited to legal entities established only in Member States or to legal entities established in specified associated or other third countries in addition to Member States. Any limitation of the participation of legal entities established in associated countries which are EEA members shall be in accordance with the terms and conditions of the Agreement on the European Economic Area. For duly justified and exceptional reasons, in order to guarantee the protection of the strategic interests of the Union and its Member States, the work programme may also exclude the participation of legal entities established in the Union or in associated countries directly or indirectly controlled by non-associated third countries or by legal entities of non-associated third countries from individual calls for proposals, or make their participation subject to conditions set out in the work programme*."

Service's (EGNOS) ability to bring improved resilience to timing and synchronisations operations, specific industrial or research and development support or the preparation of specific legislation. In June 2020, the final report for the "Impact assessment study on the Use of Galileo for Critical Infrastructures that depend on Satellite Navigation for Timing and Synchronisation" was published[52] and an open public consultation was concluded.

The Government **Satellite Communication (GOVSATCOM)** initiative aims to provide the EU and Member State authorities with an infrastructure capable to support security critical missions, with the ability to exchange sensitive information worldwide. The EU Agency for the Space Programme (EUSPA)[53] has already launched the procurement of GOVSATCOM ground infrastructure. In 2021 the Commission will also prepare implementing acts to define the service portfolio and the operational requirements of GOVSTACOM, as well as its security requirement. In the meanwhile, the EUSPA is also continuing the institutional dialogue with governmental users and Member States representatives through the ENTRUSTED initiative, with funds from Horizon 2020.

In addition, a project funded under Horizon 2020 and coordinated by the EUSPA started in September 2020 that establishes a **Network of Users for governmental Satellite Communications** in Member States and the relevant EU agencies[54], aiming at achieving a reliable collaboration and coordination between them.

Furthermore, 17 Member States participating in the EDA and the European Peace Facility are contributing to the **Project Arrangement for the EDA's GOVSATCOM Pooling and Sharing Demonstration Project**, which has been in execution phase since in January 2019 and has been already providing the first governmental SATCOM services.

In addition, a first **study on the secure space-based connectivity system** to be carried out by a consortium of space primes, system and telecom operators, was launched in December 2020. The main system characteristics (type of constellations, frequency bands, use cases, inclusion of quantum technology) were already addressed. The study will also cover a preliminary architecture design of the system and define specification for the full deployment phase, the exploitation models and the associated costs.

With the new **Space Programme Regulation,** space situational awareness is becoming one of the space components of the EU Space Programme. The objective of space situational awareness is to enhance space surveillance and tracking capabilities to monitor, track and identify space objects and space debris with the aim to further increase the performance and autonomy of space surveillance and tracking capabilities at Union level. The Space Programme Regulation also foresees the alignment of the security governance of EU-Space Surveillance and Tracking (EU-SST) with the one of Galileo (including accreditation) and the inclusion of EU-Space Surveillance and Tracking in the remit of the Council Decision (CFSP)

[52] This impact assessment aims to explore a proposed European initiative to further protect and improve the resilience of critical infrastructure that rely on the timing and synchronisation elements of satellite navigation (GNSS). This initiative also offers a way to decrease dependency on foreign GNSS technologies.

[53] The EU Agency for the Space Programme (EUSPA) has replaced the European Agency for Global Navigation Satellite Systems (GSA), with the entry into force of the Regulation (EU) 2021/696 of the EP and the Council.

[54] European Border and Coast Guard Agency (Frontex), European Maritime Safety Agency (EMSA), European Union Agency for Network and Information Security (ENISA), European Union Agency for Law Enforcement Cooperation (Europol), European Defence Agency (EDA), European Union Satellite Centre (SatCen), European Fisheries Control Agency (EFCA) and the Commission's Joint Research Centre (JRC).

2021/698[55]. The general security requirements to be complied with by the future EU-SST partnership are under preparation.

Concerning the **security of EU space assets**, the Council and the High Representative have been given specific responsibilities by Council Decision (CFSP) 2021/698 to avert a threat to the security of the Union or of one or more of its Member States or to mitigate serious harm to the essential interests of the Union or of one or more of its Member States arising from the deployment, operation or use of the systems set up and services provided under the components of the Union Space Programme, or in the event of a threat to the operation of any of those systems or the provision of those services. The EEAS has developed operational scenarios with Member States experts to counter attacks against the Galileo systems taking into account hybrid threat scenarios with the close support of the EU Hybrid Fusion Cell.

[55] Council Decision (CFSP) 2021/698 – replacing Decision 2014/496/CFSP.
In particular, Council Decision (CFSP) 2021/698 has extended Decision 2014/496/CFSP scope to the systems and services under the five components of the Union Space Programme.

Defence capabilities

The 2018 Capability Development Priorities, together with the Strategic Context Cases, served as a basis for the first full **Coordinated Annual Review on Defence (CARD)** cycle that produced the CARD Aggregated Analysis in June 2020 and the CARD Report[56] in November 2020. CARD Aggregated Analysis provided the Member States with a list of 55 collaborative opportunities in capability area and 56 collaborative opportunities in the research area. Among them, there are areas with identified hybrid threats potential, such as counter Improvised Explosive Devices (C-IED) and Explosive Ordnance Disposal (EOD), Harbour protection and counter Unmanned Aerial Systems (C-UAS). Furthermore, the CARD Aggregated Analysis led to three specific operational collaborative opportunities with a high potential of boosting the Union's operational CSDP performance in the short and medium term. One of them are non-kinetic capabilities with a focus on strategic communication, cyber effects and response action. These capabilities are strongly related to countering potential hybrid threats. As some capability areas identified in the CARD framework could have a potential to deliver significant impact on the coherence of the European Defence Landscape, including operational benefits, the following six focus areas have been developed: Main Battle Tank, Soldier Systems, European Patrol Class Surface Ships, C-UAS – Anti-Access/Area-Denial, Defence in Space, and Enhanced Military Mobility. Member States were invited to express further interest to cooperate in these areas which could include countering the hybrid threats-related dimensions.

Furthermore, the implementation of **Permanent Structured Cooperation (PESCO**) contributes to the efforts of countering hybrid threats through the fulfilment of the more binding commitments, as agreed by the participating Member States, as well as the projects, which are being implemented in the PESCO framework. During the PESCO Strategic Review undertaken in 2020 participating Member States pointed to the evolving security scenario and discussed setting more precise objectives in areas of cooperation, such as countering hybrid threats.

Progress has also been made on **funding hybrid threats related aspects of defence capabilities,** the work programmes of the two pilot programmes of the European Defence Fund namely the Preparatory Action on Defence Research (PADR) and European Defence Industrial Development Programme (EDIDP), included several topics related to strengthening the resilience against hybrid threats. This includes, but not limited to, cyber capabilities (e.g. for increased cyber situational awareness and countering cyberattacks), cross-domain capabilities (EDIDP calls 2019-2020), maritime surveillance capabilities (EDIDP 2020 call), as well as chemical, biological, radiological and nuclear (CBRN) capabilities for threat detection and counter measures (EDIDP 2020 call). Overall, 18 projects have been supported under the PADR with EUR 90 million contributing to the development of technological solution that could be applied to address hybrid threats.

In parallel, the preparation of the capability priorities for the European Defence Fund under the Multiannual Financial Framework 2021-2027 have been initiated. Research and development cooperative projects supported by the European Defence Fund will reinforce the defence capacity of the Union including improving the resilience against hybrid threats.

[56] https://eda.europa.eu/docs/default-source/reports/card-2020-executive-summary-report.pdf

Protecting public health and food security

The COVID-19 crisis has highlighted weaknesses of emergency preparedness and response mechanisms in Europe. Both EU public and private capacities in the field of preparedness and crisis management, particularly regarding medical countermeasures, are fragmented and dispersed. This fragmentation provides potential vulnerabilities to hybrid threats. As presented in the communication of 11 November 2020, "Building a European Health Union: Reinforcing the EU's resilience for cross-border health threats"[57], the future European Health Emergency Preparedness and Response Authority (HERA) would play a critical role in strengthening overall resilience to health threats. HERA will ensure a solid framework for EU preparedness, surveillance, risk assessment, early warning and response to all serious cross-border threats to health. In parallel to the establishment process of HERA, preparatory actions are being launched under the current and future EU financing programmes in the field of health. These actions allow to test a number of solutions that could serve as a blueprint for future HERA functions and provide indications on the added value of its interventions, and possible areas for improvement.

On 17 February 2021, the Commission launched an ambitious plan – the HERA Incubator – focusing on EU preparedness against COVID-19 variants. Under the HERA Incubator, the Commission is supporting EU countries in their efforts to detect, monitor and assess variants of the SARS-CoV-2 virus and complementing efforts to develop and significantly increase production of COVID-19 vaccines.

The initiatives already put forward by the Commission for the establishment of a stronger European Health Union will strengthen the overall heath security and resilience framework for Europe. These initiatives include a revamped cross-border health threats legal framework, extended and improved crisis-related mandates for both the European Centre for Disease Prevention and Control and the European Medicines Agency, and the Pharmaceutical Strategy for Europe, adopted on 25 November 2020[58].

Different types of health, political, economic, or environmental crises as well as hybrid threats also have the potential to disrupt food systems. The *Farm to Fork Strategy*[59], part of the *European Green Deal*[60], envisages the development of a **Contingency Plan by the Commission**, to be activated when there is a crisis that affects the entire or part of the food system in the EU and puts **food security** within the EU in danger. This Plan will contain a set of procedures to be followed in times of crises, and include the development of a common EU food crisis response mechanism, coordinated by the Commission and involving Member States. The plan will cover different food system-related sectors that may be affected by a crisis, including agriculture, fisheries and aquaculture, food safety, workforce, health and transport issues.

To achieve coordination at EU level, the mechanism would take the form of a permanent forum, created by the Commission and in which Member States and possibly food supply chain stakeholders would be represented. It would build on existing coordination processes

[57] COM(2020)724
[58] https://ec.europa.eu/health/sites/default/files/human-use/docs/pharma-strategy_report_en.pdf
[59] COM(2020) 381 final
[60] COM(2019) 640 final

and in the event of an actual crisis would convene and serve as the main operational mechanism for coordinating a response. The contingency plan to ensure the EU's food supply and food security in the event of future crises is expected to be adopted by the Commission in the fourth quarter of 2021. This plan would complement and apply without prejudice to the existing plan for crisis management in the field of safety of food and feed, adopted by the Commission in 2019 and which is regularly applied when food safety incidents emerge.

Furthermore, since 2019, the EU has reinforced and strengthened components of its **disaster risk management** by upgrading the EU Civil Protection Mechanism. The latest element introduced - rescEU - has the objective of enhancing both the protection of citizens from disasters and the management of emerging risks. In addition, rescEU establishes a new European reserve of resources (the 'rescEU reserve') which includes a fleet of medical evacuation planes, as well as a stockpile of medical equipment and field hospitals that can respond to health emergencies, and chemical, biological, radiological, and nuclear incidents.

Chemical, Biological, Radiological and Nuclear (CBRN) related risks

Following the development of the **list of high-risk chemicals** that are of most concern in terms of misuse for terrorist purposes the Commission started working with manufacturers with a view to enhancing detection equipment's performance and adjusting it to the evolving chemical threat. In parallel, the Commission, in cooperation with Member States' law enforcement authorities, has been conducting tests of detection equipment to assess their performance and to adapt procedures. In 2020, the Commission launched a study looking at the feasibility of restricting access to certain high-risk chemicals. The results are expected in 2021 and will help in defining the next steps in this area.

Additionally, EDA's CapTech CBRN & Human Factors launched a **CBRN Framework Service Contract for the development of studies, reports and demonstrators** in 2020. The first three specific contracts will regulate Personal Protective Equipment, Detection Identification and Monitoring of CBRN and Protection of Critical Infrastructure from CBRN. The scenarios related to CBRN hybrid threats will be reviewed in the second half of 2021 and finalised by second quarter 2022.

Cybersecurity

On 16 December 2020, the Commission presented a new **EU Cybersecurity Strategy**[61], which aims to bolster Europe's collective resilience against cyber threats. In this context, the Commission presented a proposal for a ***Directive on measures for high common level of cybersecurity across the Union***[62] (**NIS2 Directive**). In addition to the existing seven sectors[63] addressed in the NIS Directive, the proposal includes new sectors and services. A proposed size-cap rule will determine the entities active in the sectors covered by the NIS2 Directive that would fall within its scope.

The NIS2 Directive strengthens security requirements with a list of focused measures including incident response and crisis management, supply chain security, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption. It also

[61] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391
[62] COM(2020) 823 final
[63] energy, transport, banking, financial market infrastructure, health, drinking water and digital infrastructure

streamlines incident-reporting obligations with more precise provisions on the reporting process, content and timeline. The proposal introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States. It enhances the role of the NIS Cooperation Group in shaping strategic policy decisions on emerging technologies and new trends, increasing information sharing and cooperation between Member State authorities. It also improves operational cooperation including on cyber crisis management.

Further, the cybersecurity strategy announces the creation of a **Joint Cyber Unit**. The Joint Cyber Unit would not be an additional, standalone body, nor would it affect the competences and powers of national cybersecurity authorities or EU participants. Rather, it will serve as a virtual and physical platform for cooperation for the different cybersecurity communities in the EU with an operational and technical focus. The Joint Cyber Unit will better protect the Union against major cross-border cyber incidents, acting as a backstop avoiding the spread of systemic threats.

Following the Commission *Recommendation (EU) 2019/534 on the Cybersecurity of 5G networks*[64] adopted in March 2019 and the presentation of the NIS Cooperation Group of a "toolbox" of mitigating measures on 29 January 2020[65]. The Commission presented in December 2020 a report on the impacts of the Recommendation on **5G cybersecurity**[66]. This report shows that considerable progress has been made since the toolbox was agreed, and that most Member States are on track to complete a significant part of the toolbox implementation in the near future. The Commission called on Member States to complete the implementation of the main Toolbox measures by the second quarter of 2021. For the way forward, the review helped identify a set of objectives and actions presented in an annex to the Cybersecurity Strategy. Three key objectives have been outlined, namely ensuring further convergence in risk mitigation approaches across the EU, supporting continuous exchange of knowledge and capacity building, and promoting supply chain resilience and other EU strategic security objectives. The NIS Cooperation Group is now continuing the coordinated work on 5G cybersecurity at EU-level and is working on the implementation of the different actions laid out in the Cybersecurity Strategy, with the support of the Commission and the EU Agency for Cybersecurity (ENISA).

In addition, the *Cybersecurity Act*[67] foresees the adoption by the Commission of a **Union Rolling Work Programme** (URWP). The first URWP will identify strategic priorities for future European cybersecurity certification (e.g. standardisation, security by design, regulatory coherence, metrics to measure schemes' efficiency, international cooperation) as well as areas where certification would be beneficial but it is assumed that further preparatory work e.g. standardisation is necessary (artificial intelligence, secure development lifecycle).

Contractual Public Private Partnership (cPPP) for cybersecurity

The Contractual Public Private Partnership (cPPP) for cybersecurity is technically no longer in force. In practice, the cooperation with the European Cybersecurity Organisation continues

[64] COM (2019) 2335 final.
[65] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures (Publication of the NIS Cooperation Group), 29 January 2020.
[66] SWD (2020) 357 final
[67] OJ L 151, 7. 6. 2019

under the general umbrella of Cybersecurity and the Cybersecurity Strategy as it has evolved into the "**European Cybersecurity Industrial, Technology** and **Research Competence Centre and the Network of National Coordination Centres**" [68]. The legislation creating the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres was adopted by the European Parliament in second reading on 19 May 2021. The initiative aims at strengthening European cybersecurity capacities, promoting research excellence and reinforcing the competitiveness of the Union's industry in this field. It will coordinate and implement cybersecurity funds from the Digital and Horizon Europe Programmes, as well as from Member States.

Cybersecurity in the transport sector

The **resilience and protection of all transport modes** (aviation, maritime and land transports) from cyber-security incidents and attacks is one of the key objectives of the Commission. Discussions with Member States and industry stakeholders for an optimum EU response in the different transport modes continued. The cyber-security dimension linked to increased digitalisation in transport and intelligent transport systems, including automation and autonomous systems, remained key priority areas also covering safety aspects.

The Commission regularly monitors and ensures that sectorial initiatives on cybersecurity are pursued in consistency with cross-sectorial requirements covered by the *Network and Information Security (NIS) Directive* to avoid duplication and conflicting obligations. Transport is also one of the sectors covered by the Commission's proposal for a revised *Directive on Security of Network and Information Systems* (NIS2 Directive)[69].

In December 2020, the Commission published a ***transport cybersecurity toolkit***[70], with the aim to raise awareness on cyber-risks and build preparedness in the transport sector. This toolkit contains recommended practices to mitigate some of the cyber threats that may affect the transport sector.

The Commission continued to ensure compliance with the cybersecurity-related obligations under existing EU **maritime security** legislation[71]. The European Maritime Safety Agency (EMSA) continued to closely follow cyber-security aspects affecting the maritime area and contributing to a number of relevant initiatives and actions. These actions included for example a mapping exercise on maritime cybersecurity. In December 2020, the European Union Agency for Cybersecurity (ENISA) published *Guidelines for cyber risk management in ports*[72].

In the framework of the European Union Maritime Security Strategy (EUMSS), the Commission promotes a comprehensive approach to maritime security risk management, in particular by conducting common risk analysis and identifying possible gaps and overlaps in this domain, while also taking into account cyber and hybrid threats, climate challenges and maritime environmental disasters. The EDA continues to address cybersecurity requirements in capability development to support maritime security.

[68] 2018/0328(COD)
[69] COM(2020) 823 final
[70] https://ec.europa.eu/transport/themes/security/cybersecurity_en
[71] OJ L 129, 29.4.2004, pp. 6-91
[72] https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports/

Furthermore, the Commission supports the work of the European Coast Guard Function Forum and encourages the sub-working group dedicated to tackle cyber threats in the maritime domain. The developed terms of reference include tasks such as the setting up a common cybersecurity database for the maritime domain; develop cross sectoral coordination with other transportation sectors and promote common risk management processes.

In the aviation sector, the implementation of Aviation Security legislation to address cybersecurity was supported by an Information Note to help Member States' authorities and industry through providing guidance and best practices. The European Union Aviation Safety Agency (EASA) through its European Strategic Cybersecurity Platform (ESCP) continued to implement the *EU Cybersecurity in Aviation Strategy*[73]. In particular, EASA has been developing, with the help of the ESCP, an Opinion proposing a new Implementing Regulation and a new Delegated Regulation on Information Security management. The European Centre for Cyber Security in Aviation (ECCSA) continued to operate as a platform for information sharing, threat analysis and standardisation programme. To further strengthen coordination and cooperation with relevant organisations and institutions in the field of cybersecurity, cyber defence, and aviation cyber, the EDA was granted membership by the ECCSA to receive timely cyber threat and risk information and to inform participating Member States if appropriate. Moreover, EASA established the Network of Cybersecurity Analysts to raise awareness of the importance of cybersecurity risks in civil aviation and support Member States to analyse information security incidents that have an impact on or could potentially affect aviation safety.

Furthermore, the ongoing Single European Sky ATM Research (SESAR) project modernizing European Air Traffic Management also embeds cybersecurity as an integral part. In addition, the Commission, assisted by EASA, actively participated in international fora managed by ICAO, the European Civil Aviation Organisation (ECAC) and Eurocontrol to contribute to their work on further developing policies and cooperation at multilateral and European level in the area of aviation cybersecurity.

Cybersecurity in the energy sector

By means of the *Regulation on the internal market for electricity*[74], the Commission has been empowered to establish a **network code on cybersecurity** in cooperation with the relevant associations of electricity network providers and regulators. In January 2021, the Commission requested the Agency for the Cooperation of Energy Regulators (ACER) to prepare a non-binding framework guideline for the development of the network code. The network code on cybersecurity will contain sector-specific rules for cybersecurity aspects of cross border electricity flows, on common minimum requirements, planning, monitoring, reporting and crisis management. Ensuring resilience of energy networks against both cyber threats and hybrid threats is becoming increasingly important as wide-spread use of information and communication technology becomes the foundation for the functioning of infrastructures underlying the energy systems. Preparatory technical work for the network code was carried out by network operators and finalised at the beginning of 2021.

[73] https://www.easa.europa.eu/sites/default/files/dfu/Cybersecurity%20Strategy%20-%20First%20Issue%20-%2010%20September%202019.pdf

[74] OJ L 158, 14.6.2019, p. 54–124

The dedicated sectorial work stream of the Network and Information Security **(NIS) Cooperation Group assessed the *Commission Recommendation on cybersecurity in the energy sector***[75] in terms of implementation and exchanged experiences with Member States on the implementation of the NIS Directive in the energy sector.

Cybersecurity in the financial services sector

The Commission continues to be an active-observer in the European Central Bank's European Cyber Resilience Board for pan-European financial infrastructures' (ECRB) working group on information sharing. In August 2020, the ECRB published the *Cyber Information & Intelligence Sharing Initiative (CIISI) - EU ECRB **Community Rulebook***[76] which sets out the governance of CIISI-EU, its building blocks, the principles for information and threat intelligence sharing, as well as the taxonomies, frameworks, terminology and conventions to be used. The group is currently finalising the last steps to operationalise the initiative.

In September 2020, the Commission launched a proposal for a ***Regulation and a Directive on a Digital Operational Resilience Act***[77] (DORA) in financial services. DORA allows financial entities to set-up arrangements to exchange cyber threat intelligence in order to raise awareness on information and communication technology (ICT) risk, minimise its spread, support financial entities' defensive capabilities and threat detection techniques. The development at EU scale of information sharing arrangements and good practices on cybersecurity threats is an important step in the process of building the digital operational resilience of the Union's financial sector.

Cyber defence

Over the reporting period, **cooperation activities between** the EU Agency for Cybersecurity (**ENISA**), the Computer Emergency Response Team for the EU institutions **(CERT-EU**), the **EDA** and the European Cybercrime Centre of Europol (**EC3**) in the framework of their joint Memorandum of Understanding continued.

Furthermore, a number of Member States are developing and contributing to four cyber defence-related projects under **Permanent Structured Cooperation** (PESCO): "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security", "Cyber Threats and Incident Response Information Sharing Platform", "Cyber and Information Domain Coordination Centre" and "EU Cyber Academia and Innovation Hub".

The EDA, within the framework of the **Key Strategic Activities work**-strand, analysed the areas of "Cyber Defence Research and Technology" and "Cyber Defence Situational Awareness and the Protection of military CIS" to identify key technologies, industrial capabilities and skills whereby dependency from non-EU players could put at risk the EU's freedom of action in the defence domain.

In the European Security and Defence College (ESDC) an updated **cyber training plan** for 2020 was established and implemented with the support of EDA and ESDC's network partners. Two pilot activities were proposed by the EDA during the current ESDC academic

[75] OJ L 96, 5.4.2019, p. 50–54
[76] https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ciisi-eu_community_rulebook.pdf
[77] COM(2020) 595 final, COM(2020) 596 final

year – "Cyber Awareness Train-the-Trainer" course (specialised at awareness level) and "Cyber Implications to CSDP Operations and Missions Planning Course (specialised, at strategic/policy level)". For the creation of a cyber-skilled EU workforce and the updated role of the ESDC, further actions will be planned within the scope of implementation of the new EU Cybersecurity Strategy. The Cyber Security and Cyber Defence curriculum of the ESDC has been opened to NATO staff and third countries that have signed a security agreement with the EU.

In addition, the EDA and the ESDC conducted several planning activities, including trainings in cyber, critical infrastructure and hybrid domains, and planning of exercises such as the Cyber Phalanx 2021 (CYPH21). The Hybrid CoE and the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD CoE) are also involved in the development and conduct of the pre-learning course on CYPH21.

In line with the updated 2018 EU ***Cyber Defence Policy Framework***[78], the EDA continues to further develop courses in collaboration with the ESDC to meet the Member States' cyber defence education, training and exercises requirements. Additional activities, for example, progressive integration of cyber education, training, evaluation and exercises modules developed in the frame of the EDA, have been implemented during 2019-2020.

In addition, the Hybrid CoE is contributing to the EDA project "**Cyber Pilot Courses Development Scheme**", aiming at developing new cyber pilot courses in the area of standardized cyber awareness and cyber implications to the CSDP operation and mission planning. The project will also assess the need for additional cyber courses. Most of malicious cyber activities may affect areas of hybrid threats, therefore, the Hybrid CoE has also been invited to contribute to the identification and development of new Cyber/Hybrid Pilot Courses in support of the Cyber education, training, exercise and evaluation (ETEE) platform.

Gathering electronic evidence for criminal investigation

On 10 February 2021, the European Parliament and the Council started discussions on the Commission's ***e-evidence proposals***[79]. Once adopted, these instruments will help law enforcement and judicial authorities to obtain swift access to electronic evidence that is needed for criminal investigations, e.g. on cybercrime, terrorism or other forms of organised crime. This includes emails or messages exchanged via apps, as well as information to identify a perpetrator as a first step.

Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, including a horizontal cyber sanctions regime

The *Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities*[80] (the '**cyber diplomacy toolbox**') is part of the EU's wider approach to cyber diplomacy, which contributes to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations. The Framework holds a mechanism to jointly collect and assess situational awareness, measures to prevent, discourage, deter and respond during and

[78] 14413/18
[79] COM (2018) 225 and 226 final
[80] 9916/17

following malicious cyber activities affecting the EU or its Member States, as well as practices to cooperate and coordinate with international partners to this effect.

Member States continuously work to improve the EU's ability to prevent, discourage, deter, and respond to malicious cyber activities, including by annual exercises. Moreover, the 16 December 2020 Joint Communication on the EU's Cybersecurity Strategy for the Digital Decade[81] includes proposals for further strengthening the EU cyber diplomacy toolbox.

The **EU has responded to malicious cyber activities on multiple occasions**, notably through several public statements. Most recently on 16 April 2021, the High Representative published a declaration on behalf of the EU expressing solidarity with the United States on the impact of the SolarWinds cyber operation[82]. Furthermore, the Council adopted two cyber sanctions packages in July and October 2020. In total, the EU listed 8 individuals and 4 entities and bodies under the cyber sanctions regime that are responsible or involved in significant cyber-attacks targeting the EU and its Member States. The EU cyber sanctions regime was renewed for a further year in May 2021[83].

International cooperation on cyber issues

Given the commitment of the EU and Member States to promote a strategic framework for conflict prevention, stability and cooperation in cyberspace, where the rule of law is upheld and human rights and fundamental freedoms are respected, the EU engages in further **discussions in the United Nations on cyber issues**. In particular, they take place in two specific processes related to international security: the Open-ended Working Group (OEWG) linked to developments in the field of information and telecommunications and the Group of Governmental Experts (GGE) to advance responsible state behaviour in cyberspace in the context of international security. In March 2021, the OEWG agreed upon a consensus report[84] endorsing the 2010, 2013 and 2015 GGE reports, notably on the application of international law, and the non-binding voluntary norms of responsible state behaviour. To further advance the implementation of the framework, the EU promotes a Programme of Action to Advance Responsible State Behaviour in cyberspace, which offers a platform for cooperation and exchange of best practices within the UN, and proposes to establish a mechanism to put in practice the norms of responsible state behaviour and promote capacity building. The EU and Member States will continue the establishment of a Programme of Action, including in the context of the new OEWG, which has its organisational meeting in June 2021. In addition, the UNGGE concluded on its 6th iteration in May 2021.

Taking into account the global nature of hybrid threats, building and maintaining robust alliances and partnerships with third countries is fundamental to advancing international stability and security in cyberspace. The EU has established specific **cyber dialogues** with the United States, Japan, Brazil, India, South Korea and China. In addition, the Trade and

[81] JOIN(2020) 18 final

[82] https://www.consilium.europa.eu/en/press/press-releases/2021/04/15/declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-the-united-states-on-the-impact-of-the-solarwinds-cyber-operation/

[83] Council Decision (CFSP) 2021/796 of 17 May 2021 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

[84] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

Cooperation Agreement[85] (TCA) with the UK includes the ambition to establish a regular dialogue on cyber issues. The establishment of a dedicated EU-Ukraine cybersecurity dialogue is an important development to enhance cyber cooperation. Close consultations with regional and international organisations are also in place, notably with NATO. Under the EU Cybersecurity Strategy the EU announced the ambition to strengthen and expand its engagement on cyber with third countries, regional organisations as well as the multi-stakeholder community in view of exchanges and sharing best practices, and strengthening cooperation promoting its values and vision for cyberspace.

On technical level, the **Technical Arrangement on Cyber Defence** between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team for the European Union (CERT-EU) continued to be implemented in line with existing provisions. The Malware Information Sharing Platform (MISP) is being leveraged to this end. In addition, coordination meetings between the staffs are held on a regular basis and exchanges on best practices for technical topics also continue.

Screening of foreign direct investment

Regulation (EU) 2019/452 establishing a ***framework for the screening of foreign direct investments***[86] into the European Union sets up a cooperation mechanism between Member States and the Commission, and also contains certain requirements in terms of Member State screening mechanisms. The enabling framework entered into force in April 2019 but was applied as of November 2020. The Regulation serves to enable exchange of information between Member States and the Commission and enables Member States to provide comments and the Commission to issue an opinion with regard to foreign direct investments likely to affect security or public order in more than one Member State or posing a risk to a project or programme of Union interest.

In addition, in March 2020 the Commission issued **Guidance to the Member States concerning foreign direct investment** and free movement of capital from third countries[87], and the protection of Europe's strategic assets, ahead of the full application of the Regulation.

Building resilience against radicalisation and violent extremism

Communication and online propaganda remain a key priority addressed in the ***Strategic Orientations 2021***[88] adopted by the Steering Board for Union actions on preventing and countering radicalisation[89], underlining the role of the COVID-19 crisis and lockdowns in creating a fertile ground for radicalisation, including by spreading conspiracy theories.

Often a continuum between radicalisation, acts of racist and xenophobic hate crime, hate speech and violent right-wing terrorism can be observed. In this context it is worth mentioning the Commission's efforts to curb the spread of illegal hate speech, in particular

[85] OJ L 444, 31.12.2020, p. 14–1462
[86] OJ L 79I , 21.3.2019, p. 1–14
[87] 2020/C 99 I/01
[88] https://ec.europa.eu/home-affairs/sites/default/files/pdf/2021_strategic_orientations_on_a_coordinated_eu_approach_to_prevention_of_radicalisation.pdf
[89] https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626

online. The *2008 Framework Decision on combating racism and xenophobia*[90] prohibits hate speech defined as public incitement to violence or hatred on the basis of certain characteristics, including race, colour, religion, descent and national or ethnic origin. The Commission has supported the implementation of the Framework Decision, including through policy initiatives such as the voluntary **Code of conduct on countering illegal hate speech online**[91], which was agreed in 2016 with the major IT Companies. The Code of conduct has achieved considerable progress in particular in ensuring a prompt response to hate speech notifications.

To limit the ability of terrorists to spread their messages inciting or recruiting individuals to their cause, or glorifying terrorist attacks and therefore foster radicalization the ***Regulation to address the dissemination of terrorist content online***[92] was adopted by the Council and the European Parliament on 28 April 2021. The Regulation provides clear rules on the identification and swift removal of terrorist content, to be imposed in a uniform manner across the Union, as well as robust safeguards to protect freedom of expression and information.

In the **EU Internet Forum** the Commission is engaging with tech platforms to address emerging challenges on a voluntary basis. Work is ongoing together with Member States to develop a list of right-wing terrorist groups and symbols banned in the EU, to support the platforms' content moderation decisions. Work is also ongoing to ensure the effective implementation of the *EU Crisis Protocol*[93], a voluntary mechanism to help coordinate a rapid, collective and cross-border response between law enforcement and tech companies to the viral spread of violent extremist and terrorist content online. The Protocol was activated for the first time in October 2020, in the aftermath of the attack on Samuel Paty, a French teacher, where pictures of the victim were circulating online for the purpose of glorifying the attack. The Commission, together with EUROPOL, is also engaging with the Christchurch Call for Action[94], and with the Global Internet Forum on Counter Terrorism[95], to ensure a global response when the EU's Crisis Protocol is activated. The EU Internet Forum is also organising technical meetings on the exploitation of video-platforms by extremists, as well as on the risks of algorithmic amplification of violent extremist content.

In line with the **Counter Terrorism Agenda** and building on the achievements of the EU-funded European Strategic Communications Network, the Commission supports Member States in the development of their strategic communication capabilities including post-terrorist attack responses, through exchange of expertise and tailored consultancy at the European level. The Commission also supports the dissemination of counter- and alternative narratives developed by civil society and similar efforts at national level.

[90] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32008F0913
[91] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en
[92] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021R0784&from=EN
[93] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20191007_agenda-security-factsheet-eu-crisis-protocol_en.pdf
[94] Christchurch Call | to eliminate terrorist and violent extremist content online
[95] GIFCT | Global Internet Forum to Counter Terrorism
* 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.

The Commission supported the **Civil Society Empowerment Programme** (CSEP) with EUR 13.7 million. The programme provides alternative narratives to radicalised discourses and terrorist propaganda, and promotes fundamental rights and values. In 2021, the Commission intends to evaluate CSEP's impact and disseminate lessons learnt and good practices.

Increasing cooperation with partner countries

In the framework of the implementation of action 18 of the Joint Framework on countering hybrid threats, **Hybrid Risk Surveys** have been launched in the Republic of Moldova, Georgia, the Republic of Albania, Kosovo*, the Republic of North Macedonia and Montenegro. Based on the analysis by the EEAS and Commission services of the responses provided by Georgia, Albania, Kosovo, North Macedonia and Montenegro, sets of recommendations on priority domains were prepared by the EU and agreed with partners in early 2020. The survey in the Republic of Moldova, finalised in the second part of 2017 and put on hold due to political developments, is ready to be relaunched based on the principle of strict conditionality and respect for the rule of law and democratic standards, and linked to concrete reform deliverables.

For those partners which have responded to the Hybrid Risk Survey, support measures to mitigate the identified risks can be provided through existing projects or ad hoc support, such as the Commission's Technical Assistance and Information Exchange instrument (TAIEX). In June 2020, the TAIEX Team conducted an **expert mission to support Montenegro** in drafting its regulation on the sectoral criteria for the designation of critical infrastructure. In November 2020, TAIEX held a **multi-country workshop** which was established in order to address the consequences of the COVID-19 pandemic. Enlargement and Neighbourhood beneficiaries[96] received assistance on emerging security threats and cybercrime. In February 2021, a **TAIEX expert mission** was also organised to support the Government of the Republic of **Moldova** in establishing an interagency framework for countering hybrid threats. Several activities have been prepared and implemented in **Georgia**. Among others, the presentation of "The landscape of Hybrid Threats: A Conceptual Model" was provided for Georgian hybrid stakeholders. This presentation is planned to be organised for **Western Balkan partners** as well, while the mapping of ongoing support activities by other stakeholders continues, to avoid duplications with the implementation of the risk survey recommendations. In November 2020, a two years twinning project started to strengthen Georgia's cybersecurity legal and institutional frameworks and increase the security level of the country's networks and information systems.

Cybersecurity capacity building is one of the priorities of the ***Economic and Investment Plan for the Western Balkans***[97], adopted by the Commission in October 2020. The plan gives special importance to accelerating reforms to enhance cybersecurity capacity and the fight against cybercrime in the region. Building upon these commitments, the Commission is preparing activities with the Western Balkans on cybersecurity capacity-building in 2021. A first step will be to conduct a study with EU Member States entities to assess the capacity-building needs of the region in light of the EU acquis, policies and best practices. A tailor-

[96] Except Belarus
[97] SWD(2020) 223 final

made regional action will be developed in response to the study and presented for funding under the Instrument for Pre-Accession Assistance (IPA III).

In the Eastern Neighbourhood, the regional cybersecurity project continues to bring the Eastern Partner countries closer to the core pillars of EU standards, legal and policy frameworks, namely the *Network and Information Security (NIS) Directive*, but also the *EU Cybersecurity Act*. The project was launched in January 2020 for a duration of 36 months and is ongoing.

In Ukraine, the ongoing EU cybersecurity capacity building measures include an e-government digital programme (EU4DigitalUA) and regional programmes that address the reform of cybersecurity institutions and the reinforcement of operational capacities. As part of these measures, cyber exercises took place in the first half of 2021. The "task-driven threat hunting exercise" trained comprehensive cyber capacity skills at technical level, as well as awareness at managerial level on the effects that cyber incidents can cause. The EU has also supported the review process of the Ukrainian cyber security strategy. As a follow-up to the October 2020 EU-Ukraine Summit, the first EU-Ukraine cyber dialogue took take place in June 2021.

In October 2020, the EU adopted a programme aiming to enhance Ukraine's overall resilience, including to hybrid threats explicitly as well as to contribute to strengthening its reform progress and countrywide societal cohesion. In this vein, the action intends to respond to most recent and developing destabilisation factors like the COVID-19 pandemic and its societal and economic impacts. The programme targets the key resilience dimensions of social capital, human security and information integrity in vulnerable regions in southern and eastern Ukraine. On various occasions, Ukraine has been encouraged to launch a Hybrid Risk Survey.

The **Commission via its Service for Foreign Policy Instruments** (FPI) has been promoting international cooperation in cybersecurity in different areas and with different actions. The objective of the Cyber4Dev[98] and EU CyberNet[99] projects is to enhance cyber resilience of third countries while promoting an inclusive multi-stakeholder and rights-based approach and ensuring compliance with the rule of law and good governance principles. Another objective of EU CyberNet is to strengthen the global delivery, coordination and coherence of the EU's external cyber capacity building projects, and to reinforce the EU's own capacity to provide technical assistance to third countries in the field of cybersecurity and cybercrime.

Further, FPI aims to strengthen the capacities of countries worldwide to apply legislation on cybercrime and electronic evidence and enhance their ability for effective international cooperation in this area in compliance with international human rights standards and the rule of law (GLACY+[100]). To support the EU's cyber diplomacy and a multi-stakeholder dialogue and cooperation with partner countries the EU CyberDirect[101] project has been initiated, working in complementarity with the Enhance Security Cooperation in and with Asia (ESIWA).

Commonly addressing hybrid threats is a priority identified at the last EU-US Summit on 15 June. In their joint statement, "Towards a renewed Transatlantic partnership", the EU and

[98] https://cyber4dev.eu/
[99] https://www.eucybernet.eu/
[100] https://www.coe.int/en/web/cybercrime/glacyplus
[101] https://eucyberdirect.eu/

US commit to "increase cooperation and exchange information and expertise to increase resilience against and to counter foreign information manipulation and interference, all forms of coercion including economic pressure, hybrid threats, malicious cyber activities, terrorism and violent extremism, and other common security threats".

EU Playbook and exercises

By the end of 2020, an agreement to **rollover the Parallel and Coordinated Exercises** (PACE) **plan** was achieved by the EU and NATO. This new PACE plan consists on the repetition of the previous concept for the period 2022-2023. The EU will be the leading organization with the EU Integrated Resolve 22 crisis management exercise, in autumn 2022, and NATO will be the leading organization in the first semester of 2023 with the CMX 23 Crisis Management Exercise.

During 2020/21, NATO staff has participated in the **EU Integrated Resolve 20 exercise** in the areas of strategic communication, cyber defence and military mobility. The EU-NATO staff interaction on civil protection/CBRN could not be achieved due to the complexity of the planning, which resulted in a postponement of the second part of the exercise to spring 2021.

Due to the ongoing COVID-19 crisis, the review process of the **EU Playbook**[102] is ongoing, since various lessons learnt that have an impact on broader EU crisis management arrangements will need to be reflected therein.

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

Following the June 2020 Council Conclusions on security and defence[103], in order to further increase the common understanding of the implementation of Article 42(7) TEU, the Political and Security Committee (PSC) conducted three **scenario-based discussions on the mutual assistance clause.** These discussions touched inter alia upon links with Article 222 TFEU, possible links with other international organisations, hybrid and cyber scenarios, as well as possible options for supporting the attacked Member State, if so requested. On the basis of these three exercises, PSC will revert to a discussions on lessons learnt and next steps.

CSDP operations and missions

The revised "**EU Concept for EU-led Military Operations and Missions**"[104], approved in December 2019, sets out the fundamental arrangements for leading EU military operations and missions. The update is reflecting the latest conceptual developments in planning and conducting military operations and missions, including namely hybrid threats and other topics like information superiority and shared situational awareness, human rights and gender, environmental protection, energy efficiency and cultural property protection issues.

In parallel, the "**EU Concept for CBRN Explosive Ordnance Disposal in EU-led Military Operations**"[105] was revised and approved in October 2020 and a new "**EU Concept on**

[102] SWD(2016) 227 final
[103] 8910/20
[104] ST14777/19
[105] ST 11968 2020 INIT

Consequence Management after CBRN Incident for EU-led Military Operations and Missions"[106] was approved in April 2021. Another concept "**EU Concept on Cyber Defence for EU-led Military Operations and Missions**"[107] is under revision. Both concepts are linked to countering hybrid threats in CSDP military operations and missions.

Moreover, the new conceptual document "**EU Guidance on countering Hybrid threats during the planning phase of EU-led CSDP military operations and missions**"[108] has been developed and approved in May 2021.

In December 2018, the Council endorsed the **Civilian CSDP Compact**[109]. The Civilian CSDP Compact highlights that civilian CSDP missions should contribute inter alia to the EU's wider response to tackling new security challenges, including those linked to cyber security and hybrid threats. A mini-concept on cyber security and cybercrime has been shared with Member States in November 2020. The mini-concept on cyber security and cybercrime proposes to assist the host State in increasing resilience of against cyber security related threats and malicious activities and to strengthen preparedness of dedicated units to tackle cyber security related threats and malicious activities as well as cybercrime. To enhance civilian CSDP efforts in these fields, a variety of tasks could be envisaged, including strategic advice and capacity building.

Civilian CSDP missions can also contribute to addressing hybrid threats including through building resilience in their host States, supporting civilian security sector reform (SSR) or through work conducted by strategic communication advisors and analysts. While three civilian missions deal with hybrid threats directly (EUAM Ukraine, EUMM Georgia and EUAM RCA), other civilian missions regularly produce internal and external reports aiming for increased situational awareness that can also cover hybrid threats. A **mini-concept on civilian CSDP support to countering hybrid threats**[110] has been developed and approved by EU Member States in May 2021. To effectively tackle hybrid challenges, the document proposes to (1) prioritise the protection of missions against hybrid attacks and (2) where appropriate, assist the host State in increasing resilience against hybrid threats. The EEAS also developed "Baseline on Disinformation for the CSDP missions"[111].

EU-North Atlantic Treaty Organisation cooperation

Countering hybrid threats remains a key area of interaction with the North Atlantic Treaty Organization (NATO). Progress is steady, building upon the momentum established by the 2016 Warsaw Joint Declaration[112] and the 2018 Brussels Joint Declaration[113]. Details of notable interactions are contained in the **sixth Progress Report on the implementation of the common set of proposals**[114] presented by the High Representative of the Union for Foreign Affairs and Security Policy and the Secretary General of NATO to the respective

[106] ST 8047 2021 INIT
[107] ST 14767 2016 INIT
[108] ST 8448/21 INIT
[109] 13571/20
[110] WK11851/2020 REV2
[111] 9262/21
[112] https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf
[113] https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf
[114] 9122/21

Councils at the end of May 2021. Cooperation has continued on crisis response and bolstering resilience through **reciprocal cross-briefings and regular staff-to-staff dialogue**.

A dedicated **staff-to-staff session** to discuss EU and NATO's respective cyber crisis management mechanisms as well as a parallel activity in the context of the EU Integrated Resolve exercise 20 (EUIR 20) were organised, to gain better understanding and look at potential complementarities and interactions. Staff exchanges continue to take place with the annual EU-NATO Cyber security and defence staff talks, of which the last iteration was held in January 2021, offering an opportunity to provide updates on respective policy developments and priorities, while assessing opportunities for further cooperation. In terms of strengthening cooperation on cyber exercises through reciprocal participation, CYBER PHALANX 21, an EU Command Post Exercise, now to be held in September-October 2021, was opened for NATO staff participation in planning and conduct phases. EU staff (EUMS/CERT-EU) participated in the annual NATO Cyber Coalition exercise in November 2020.

Staff exchanges continue to take place in the context of the implementation of the Action 18 of Joint Framework and the Counter Hybrid Support Teams launched by NATO with a view to assessing further opportunities for mutually complementary action. In the context of the implementation of the new initiatives in the field of hybrid threats, as introduced by the EU Security Union Strategy, two workshops have been organised to synchronise work on resilience. Close cooperation and coordination continues in the field of situational awareness and disinformation.

The EU Hybrid Fusion Cell and its counterpart in NATO, the Hybrid Analysis Branch, are officially in charge of analysing hybrid threats in both organisations and informing decision-makers. The two teams continued regular staff-to-staff exchanges on common areas of focus.

Cooperation between the EDA and NATO has further developed in a number of areas which are relevant in a hybrid context. In the domain of cyber defence, cooperation focuses on education, training and exercises, which is key to ensure an appropriate level of readiness against an increasing number of cyber threats. Cooperation on energy and environment has further developed, with NATO staff participation in the EU Consultation Forum for Sustainable Energy in the Defence and Security Sector, notably regarding the protection of defence-related critical energy infrastructure against hybrid threats. Staff to staff contacts have also continued on harbour protection, countering mini drones and countering improvised explosive devices areas, which all have a hybrid threats dimension.

CONCLUSION

During the five years since the *2016 Joint Framework on countering hybrid threats – a European Union response* was established, a lot of progress has been achieved to enhance the EUs preparedness and response to hybrid threats.

The fifth progress report documents the magnitude of policy areas that are relevant for countering hybrids threats, their interconnectedness, and the importance of continuing in applying and further intensifying the whole-of-government and whole-of society approach.

As a whole, the progress reported on in all relevant areas shows the continued efforts that are ongoing at EU level to increase our situational awareness, improve our resilience across all critical sectors, and to be able to recover from and adequately respond to hybrid attacks.

Significant achievements were made to **raise awareness and increase the understanding of hybrid threats**. Of particular relevance is the *Conceptual Model on hybrid threats* developed in 2020 by the Commission's Joint Research Centre and the European Centre of Excellence for Countering Hybrid Threats. By establishing a good foundation for building a common understanding of the nature and scope of the hybrid threats concept, it provides a basis for future work within a whole-of-society-approach.

Progress was achieved in **enhancing our situational awareness**. Intelligence-based analytical assessments was reinforced through the strategic and trend analysis reporting by the Hybrid Fusion Cell to the decision-makers in the EU institutions and Member States, supported by reinforced engagement of Member States.

The report highlights the good progress made in many areas **to improve resilience against hybrid threats and enhance the EU's ability to quickly recover from and respond to such attacks**. The report takes stock of progress that has been made in ensuring that Member States and entities providing essential services within Europe are better equipped to deal with hybrid risks and in enhancing resilience against hybrid threats in sectors such as energy, water, and transport. New initiatives, including the proposal for a *Directive on the resilience of critical entities*, further advance our efforts in this direction. Once adopted, it will provide, together with the *Network and Information Systems Directive* (NIS2), high resilience and security standards for essential services in the EU.

The *cyber diplomacy toolbox* provides EU and Member States with the **capacity to prevent, deter and respond to malicious cyber activities** that can be part of hybrid attacks and thus put a common response tool at the disposal of EU and Member States. Possible ways how to respond to and deter the use of other hybrid threats and tools, are being explored.

The progress report **confirms the strengthening of the whole-of-government and whole of society approach both at EU and Member States levels.** Through the dedicated Horizontal Council Working Party, Member States continued in mutual coordination, in exchanging views and in contributing to shaping new initiatives. Efforts to counter hybrid threats, that remain a critical issue for the EU institutions as well, are being taken and enhanced, through implementation of mainstreaming hybrid consideration into policy making, among others.

To counter **the increased hybrid threats activities to influence democratic elections** enhanced efforts were made, such as through the European Democracy Action Plan.

The **international element** is of particular importance as the European Union's security environment has changed dramatically. Key challenges to peace and stability in the EU's Eastern and Southern neighbourhood continue to underscore the need for the Union to adapt and increase its capacities as a security provider, with a strong focus on the close relationship between external and internal security. The progress report confirms that the EU has taken forward its international cooperation on cyber issues through UN processes and expert groups as well as on bilateral basis. Cooperation with partner countries continued among others in the framework of Hybrid Risk Surveys and resultant cooperation.

Mutually beneficial cooperation with NATO and an expanding engagement with like-minded partners in multinational formats such as the G7 represent yet another layer improving the situational awareness, resilience and crisis response of the European Union and its Member States.

Last, but not least, **the COVID-crisis** demonstrates how a **health crisis triggered the utilisation of specific hybrid techniques**, by attacking critical infrastructures but also **by**

spreading disinformation through digital media in order to reach geopolitical objectives. Targeted actions have been undertaken to tackle COVID-19 disinformation and also more broadly activities have been stepped up to strengthen strategic communication. The new guidance for strengthening the *Code of Practice on Disinformation* is a good example of efforts to ensure greater transparency and accountability of platforms' policies on disinformation which will contribute to adequate response against disinformation.

As stated in the EU Security Union Strategy, in the current geopolitical context, there is no time for complacency and efforts have and will be continued to protect the EU and its Member States against attacks on our core values and on our democratic societies.