Council of the European Union

Brussels, 31 July 2020
(OR. en)

10047/20

HYBRID 23	**ENER 251**
DISINFO 19	**EUMC 146**
COPS 260	**CIVCOM 116**
PROCIV 50	**TRANS 335**
CSDP/PSDC 393	**COEST 150**
CYBER 142	**ESPACE 36**
CFSP/PESC 655	**COTER 70**
JAI 628	**CSC 220**
ECOFIN 695	**IPCR 20**
POLMIL 103	**COSI 123**

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2020) 153 final
Subject:	JOINT STAFF WORKING DOCUMENT **Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats**

Delegations will find attached document SWD(2020) 153 final.

Encl.: SWD(2020) 153 final

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 24.7.2020
SWD(2020) 153 final

JOINT STAFF WORKING DOCUMENT

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

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 EU and its Member States are facing. While building resilience, detecting, preventing and responding to the threats remains predominantly Member States' responsibility, they are supported and complemented by actions at EU level.

Since 2016, the EU has set up a broad array of counter measures in a substantial number of policy areas through the *2016 Joint Framework on countering hybrid threats – a European Union response*[1] and the *2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats*[2]. The implementation of these measures has advanced at good pace as illustrated by three progress reports presented to the Council on 19 July 2017[3], 13 June 2018[4] and 28 May 2019[5] respectively. The implementation of the 2016 Joint Framework and the 2018 Joint Communication has been carried forward through close engagement of and interaction between the Member States, EU institutions and entities, and international partners, notably the North Atlantic Treaty Organization.

The EU has been adapting to changing security realities: hybrid actors keep engaging in new areas, therefore the EU has strived to maintain its policy frameworks and related measures flexible and updated and think ahead proactively to improve its preparedness. In recognition of the evolving nature of the threat and reflecting on, among others, the June 2019 European Council Conclusions and the Strategic Agenda for 2019-2024, the Member States established in July 2019 a Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats. Its main objective is to support strategic and horizontal coordination among Member States in the field of State and societal resilience, improving strategic communication and countering disinformation.

In December 2019, the Council adopted *Conclusions on Complementary Efforts to Enhance Resilience and Counter Hybrid Threats* [6], calling for a comprehensive approach to security and to counter hybrid threats, working across all relevant policy sectors in a more strategic, coordinated and coherent way.

The current COVID-19 crisis, which has been instrumentalised by hybrid actors, notably, for example, through manipulation of the information environment, clearly demonstrates the importance of continuous assessment of our vulnerabilities and the need to address them to bolster our resilience. It also shows willingness of those State and non-state actors that seek to weaken the EU and its Member States to expand any opportunity to the detriment of our societies and our core values.

The present fourth annual report highlights progress on the implementation of the 2016 Joint Framework and the 2018 Joint Communication taking stock of developments since May 2019. It should be read in conjunction with the fifth progress report submitted jointly by the EU High Representative/Vice-President and the Secretary General of the North Atlantic Treaty

[1] JOIN (2016) 18 final.
[2] JOIN (2018) 16 final.
[3] JOIN (2017) 30 final.
[4] JOIN (2018) 14 final.
[5] SWD(2019) 200 final.
[6] 14972/19.

Organization to the respective Councils on the implementation of the common set of proposals (74 common actions).

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

Drawing on the experience and building upon the work carried out by the Working Party on General Affairs + 1 (so-called GAC+1), the Friends of the Presidency Group on the implementation of Action 1 of the Joint Framework on countering hybrid threats (FoP CHT) and other relevant committees and working parties, the Member States established a Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP ERCHT) in July 2019. Chaired by the rotating Presidency of the Council, the Working Party facilitates coordination in the fields related to hybrid threats, disinformation and enhancing State and societal resilience, sharing information and best practices in order to bolster awareness and resilience of the EU and its Member States and to ensure that there are no overlaps or gaps in these fields. The Friends of Presidency group has been deactivated and its mandate repealed.

At a request by the Member States[7], the Commission services and the European External Action Service (EEAS) have analysed the replies provided by the Member States' authorities to the national vulnerabilities survey. Based on the Preliminary Analysis of Action 1 questionnaires and after discussions in the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats on the next steps of Action 1, several areas addressed in the survey have been identified to be further explored by means of in-depth discussions in the Horizontal Working Party. In addition, in view of the constantly changing hybrid threats environment and perpetrators' tactics, the Member States have decided to consider launching a new national vulnerabilities survey, based on a revised questionnaire in line with the evolving challenges and experience in the first iteration of the survey. In accordance with a request by the Member States, the Commission services will present a first draft of the new iteration of the questionnaire for discussion by the Member States in the HWP in the autumn 2020. The Commission services and the EEAS stand ready to support them in this endeavour should the Member States desire so.

EU Hybrid Fusion Cell

The EU Hybrid Fusion Cell (HFC), created inside the EU Intelligence and Situation Centre (EU INTCEN), has a central, coordinating role when it comes to early warning and comprehensive situational awareness on hybrid threats.

In accordance with provisions of the EEAS Intelligence Support Architecture, which defines the role of intelligence and the position of the EU INTCEN in supporting the EU decision-making process, the HFC conducts all-source, intelligence-based analysis of hybrid and cyber threats in close cooperation with the Intelligence Directorate of the EU Military Staff (EUMSINT), forming together the Single Intelligence Analysis Capacity (SIAC). The HFC, in line with its mandate, provides written assessments and verbal briefings to the EU decision-makers and the Member States.

In order to achieve common, inter-institutional, EU-wide approach on hybrid threats and a comprehensive situational picture, the HFC engages with multiple networks, integrating

[7] EUCO 9/19.

relevant bodies of the EU, Member States' intelligence community and governmental structures, academia, partner countries and organisations.

The HFC continued to organize bi-annual meetings of its network of national points of contact for countering hybrid threats. The national points of contact are the key recipients and national coordinators of the HFC-led Hybrid Trends Analysis.

Within existing limitations of classified information sharing, the HFC maintains 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, as well as to explore further potential cooperation avenues.

Institutional resilience

Externally, the Commission is constantly reinforcing cooperation with Member States, in particular with the main host country Belgium on many issues, but also in the counter-intelligence and cyber fields. In addition, cooperation on cyber threats with Member States and other EU institutions has been reinforced and the Commission has been an active part of networks led by the Hybrid Fusion Cell and a partner of the Strategic Communications Taskforces in the EEAS.

As regards cybersecurity of the EU institutions, the Commission has been raising awareness on cyber threats with threat memos distributed across the EU institutions, bodies and agencies (110 threats memos between June 2019 and April 2020) on various matters including election hacking, malicious activities on social media, cyber warfare capacities of state-sponsored actors, cyber espionage, disinformation, etc. Further activities include alerts on cyber threats directly affecting the EU institutions, bodies and agencies (30 threat alerts between June 2019 and April 2020), sharing information with EU INTCEN on cyber threats with a potential hybrid threats implications, participation in and delivering briefings to the national points of contact meetings organised by the Hybrid Fusion Cell.

Internally, the Commission revamped the internal rules on protection of sensitive information. It has bolstered the internal counter-intelligence capacity, through awareness campaigns, security briefings and outreach to staff, but also through strengthened cooperation with its privileged partners, other EU institutions and Member States' services. The Commission adopted principles on outsourcing of information technology systems and new implementing rules on handling classified information, as well as on classified procurement. Moreover, the information technology system has been updated with an objective to handle RESTREINT UE/EU RESTRICTED information, in coordination with the EEAS. The Commission launched as well a project for a system to handle highly classified information in support of new policy priorities, to be deployed in autumn 2020.

Strategic communications

Building on the 2018 *Joint Action Plan against Disinformation*[8] and the *Communication on the Implementation of the Action Plan against Disinformation*[9], significant progress has been made on strengthening the work of the EEAS Strategic Communication.

To maintain the operations that have been established and build further upon the work of the three Strategic Communications Task Forces (East, South, Western Balkans), the EEAS Strategic Communications Divisions have requested increased budget appropriations under

[8] JOIN (2018) 36 final.
[9] JOIN (2019) 12 final.

the Multiannual Financial Framework (MFF) 2021-2027. Now, in its final year, funding for the preparatory action 'Stratcom Plus' will draw to a close at the end of 2020. The December 2019 Council Conclusions[10] recalled the importance of the continued implementation of the *Action Plan against Disinformation*. The conclusions underlined the need for sufficient resources for the three Strategic Communications Task Forces and invited the EEAS to assess the needs and possibilities for reinforcing its strategic communication work in other geographical areas, such as sub-Saharan Africa.

Throughout 2020, staff reinforcements of 27 local agents will be made in EU Delegations in the EU Neighbourhood and in the Western Balkans. In partnership with the Commission Service for Foreign Policy Instruments (FPI), budget appropriations have been requested in the new Multiannual Financial Framework to ensure sustainable future funding at both Headquarters and across EU Delegations.

In line with the *Action Plan against Disinformation*'s pillar-1 objective to improve the Union's capabilities to detect, analyse and expose disinformation, the EEAS Strategic Communications build up in-house data expertise and tools. A dedicated data team supports and expands the Task Force's activities and oversees the implementation of data analytics resources. Technical implementation of a tools suite takes place in collaboration with the Commission services. Due to the increasing demand in data informed products, the data team is foreseen to grow and continues to intensify exchange with relevant European and international partners.

In line with the Action Plan, the EEAS Strategic Communications Division has expanded its work to also include disinformation and manipulative interference in information space from emerging actors. In that regard, the EEAS Strategic Communications Division has been engaging in exchanges with partners inside and outside the European Union. Additionally, contacts and cooperation with researchers have been built up further.

As called for in the *Action Plan against Disinformation*, the Commission, with the assistance of the European Regulators Group for Audiovisual Media Services (ERGA), carried out targeted monthly intermediate monitoring of the *EU Code of Practice on Disinformation*[11] in the run-up to the 2019 elections to the European Parliament[12] and is currently carrying out a comprehensive review of the *Code of Practice* following its first year of operations[13]. In this context, the online platforms (including Facebook, Google, Twitter and Microsoft) have been developing internal capacities to detect, analyse and block malicious activities on their services and have provided information on these capabilities in connection with the Commission's monitoring.

Moreover, the Commission has been deploying new digital infrastructure to establish a European Digital Media Observatory (EDMO) with the aim to scale up cooperation between independent fact-checkers and academic researchers and improve knowledge and scrutiny around the phenomenon of disinformation in the EU. These stakeholders' inputs can support work carried out by the Strategic Communications Task Forces by providing additional evidence about possible disinformation campaigns conducted by hostile actors. They can also contribute more generally to increase the transparency, accountability and trustworthiness of

[10] 14972/19.

[11] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454.

[12] https://ec.europa.eu/digital-single-market/en/news/last-intermediate-results-eu-code-practice-against-disinformation.

[13] https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

the online media landscape, bolster public awareness and enable media literacy initiatives to enhance the ability of citizens to assess information critically.

With regard to the *Communication on Tackling Online Disinformation*[14], the Commission, in close collaboration with the High Representative and the European Parliament, continues to carry out awareness raising activities about the challenge of disinformation at EU level, in the Member States and beyond. The aim is to inform the public about the negative effects of disinformation via in-person workshops, media briefings and audio-visual material disseminated online and offline. Moreover, the Commission regularly communicates on disinformation through the institutional social media accounts and leverages the online blogging platform medium to inform citizens on how to spot disinformation[15] and what the EU is doing to counter disinformation[16]. The Commission also works closely with civil society and academia to exchange best practices and strengthen practitioners' capacities to counter disinformation, for instance through a series of CONNECT University sessions on 'Tackling online disinformation'[17].

In response to a widespread wave of misinformation and disinformation stemming from the coronavirus outbreak, the Commission has created a dedicated corner on 'Fighting disinformation'[18] within its coronavirus response website. This section of the web presence is available in all EU languages and has been dedicated to bringing the attention of users to the dangers of disinformation in the context of the ongoing coronavirus outbreak and directly addressing ongoing widespread myths, misinformation and disinformation about COVID-19, its health implications and the EU's response to the global crisis. In close coordination with various stakeholders including *inter alia* the European Parliament, the High Representative, the Council as well as various institutional actors on the ground such as Commission's Representations, European Parliament's Liaison Offices and Europe Direct Contact Centres, the rebuttals on coronavirus-related misinformation and disinformation have been disseminated and promoted widely in the Member States and beyond.

COVID-19 disinformation has posed a very specific challenge to the European Union and its effective response to the pandemic, as well as to international partners – foreign state and non-state actors have tried to interfere in domestic debates in the EU and globally. As part of the EU response to COVID-19 related disinformation, on 10 June 2020 the Commission and the High Representative have adopted a Joint Communication[19] on tackling COVID-19 disinformation, which sets out five areas how COVID-19 disinformation is to be tackled: understand, communicate, cooperate, transparency, ensuring freedom of expression and pluralistic democratic debate and empowering citizens, raising citizens awareness and increasing societal resilience. The Communication focuses on the immediate response to disinformation around the COVID-19 pandemic, looks at the steps already taken and immediate concrete actions to follow.

In addition, the Joint Research Centre of the Commission has applied its conceptual model on hybrid threats landscape, developed in collaboration with the Centre of Excellence for Countering Hybrid Threats, in order to demonstrate how the COVID-19 crisis could be

[14] COM (2018) 236 final and report on implementation adopted on 5 December 2018, COM (2018) 794 final.
[15] https://medium.com/@EuropeanCommission/stopping-online-disinformation-six-ways-you-can-help-d25489724d45.
[16] https://medium.com/@EuropeanCommission/10-ways-the-eu-is-fighting-disinformation-f07fca60e918.
[17] https://ec.europa.eu/futurium/en/blog/tackling-online-disinformation-series-connect-university-sessions.
[18] https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation_en.
[19] Tackling COVID-19 disinformation - Getting the facts right JOIN(2020) 8 final
https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1006

leveraged by adversaries in order to push for their own geopolitical objectives. Disinformation has a prominent position among such tools including cyber-attacks and efforts to discredit European leadership, just to name a few.

Securing free and fair elections and protecting democratic processes

In line with the comprehensive approach to ensuring free and fair elections, as outlined in the *'Securing Free and Fair European Elections'* package adopted in September 2018, the Commission has continuously engaged with the Member States through the European Cooperation Network on Elections. The Network supports the integrity of elections and electoral processes in the EU by involving national authorities with competence for electoral matters and authorities in charge of monitoring and enforcing the rules on online activities relevant to the electoral context. Through sharing of expertise and best practices, including on threats, gaps and enforcement, the Network stimulates Member States to take actions to address specific risks stemming from lack of transparency, disinformation and other electoral manipulations, as well as to exchange experiences with regards to cooperation achieved and issues encountered in engagement with social media platforms. Furthermore, interlinkages between the Network and the Rapid Alert System have been established.

In the framework of the Network, a mapping was conducted on rules and practices relevant to the electoral context. The Network members participated in a special exercise organised to test cyber resilience in the context of European elections, gathering around 80 representatives from relevant national and EU bodies and testing policies and capabilities against a range of crisis scenarios. The Network held its first meeting in January 2019 and six meetings altogether took place until June 2020. Further regular meetings are envisaged, in order to continue supporting the sharing of expertise and best practices among Member States, including on threats, gaps and enforcement. The Commission's report on the conduct of the 2019 elections to the European Parliament was published in June 2020[20].

In November 2019, members of the Network participated in an EU-US expert-level dialogue on resilience of electoral systems.

The Commission is finalising the preparation of the *European Democracy Action Plan* to take this work forward and seek improving the resilience of our democracies and address the threats of external interference in European elections. The aim will be to counter disinformation and to adapt to evolving related threats and manipulations, as well as to support free and independent media.

The EEAS-managed Rapid Alert System, launched on 18 March 2019, has been active for over a year and has proven its worth beyond the European Parliament elections in May 2019. It provides a unique platform for exchange alerts between the EU institutions and the Member States on all facets related to disinformation and manipulative interference in the information space. Information, analysis and insights are being shared on a daily basis, helping to create a comprehensive overview over the information environment and disinformation efforts. During the COVID-19 pandemic, the Rapid Alert System has facilitated dedicated exchanges on the accompanying disinformation spread by State and non-State actors on this topic specifically.

In line with its mandate, the Rapid Alert System (RAS) has increased cooperation with the G7 Rapid Response Mechanism (RRM), by providing a separate collaboration space for RAS Points of Contact in the EU institutions and Member States with the G7 RRM Coordination Unit. Exchanges with the North Atlantic Treaty Organization are also ongoing, as well as with

[20] COM(2020) 252 final

the Centre of Excellence for Countering Hybrid Threats in Helsinki. At the request of the EEAS, the Centre of Excellence for Countering Hybrid Threats provided a scenario based discussion drawing on its counter electoral interference work for the EU Rapid Alert System, ahead of the European Parliament elections.

The EEAS Strategic Communications team is furthermore in close contact with other international groups working on this issue, like the Canberra Group on Strategic Communications, but also on a bilateral level, to ensure a close cooperation with key partners, effective information sharing and a thorough understanding of the disinformation environment.

Discussions with the social media platforms have continued as well. They were launched ahead of the European Parliament elections in May 2019 to enable a quick exchange on disinformation campaigns arising as well as to better understand the scope, impact and effectiveness of the platforms' actions when it comes to disinformation. This work has been kept up, amongst others with an expert workshop bringing together the platforms and experts from civil society to facilitate the whole-of-society approach, in full cooperation with ongoing work on the *Code of Practice* by the Commission.

Centre of Excellence for Countering Hybrid Threats

The Helsinki based European Centre of Excellence for Countering Hybrid Threats has made impressive progress with a growing participation, consensus approved work programme and a fully functioning budget. As of April 2020, it has 27 members from both the EU Member States and the North Atlantic Treaty Organization Allies. Further countries are expected to join. The Centre of Excellence continues to provide pro-active support in key areas through dedicated educational events, including seminars, workshops and conferences.

The Centre's profile as an expert hub has been reinforced. Cooperation with all EU Member States, the EEAS, the Commission, the General Secretariat of the Council, the European Defence Agency, the European Security and Defence College and the European Parliament has raised awareness and contributed to shared assessment on hybrid threats. Close cooperation with the rotating Council Presidencies has contributed to the agenda of Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP ERCHT). In addition, during the Finnish Presidency of the Council, the Centre of Excellence supported more than 30 hybrid related events in various formats and contributed to all hybrid scenario-based discussions.

The Commission has worked closely with the Centre of Excellence to develop a conceptual model for the analysis of hybrid threats and presented it to the HWP ERCHT in early 2020 as part of a final review process. The framework has been tested in the COVID-19 case and results were presented to the HWP ERCHT in July 2020.

Under the Secure Societies of Horizon 2020, up to EUR 3.5 million of funding for a pan-European network of practitioners has been allocated to the EU-HYBNET project with the Helsinki University of Applied Sciences LAUREA as coordinator and in total 25 participants from 14 countries (13 Member States and Norway), including the Centre of Excellence for Countering Hybrid Threats and the Commission's Joint Research Centre. The project started its activities in April 2020 and focuses on monitoring relevant developments in research and innovation with respect to countering hybrid threats, including recommendations for uptake and industrialisation and on defining common European requirements.

The Centre of Excellence has become an associate network partner at the European Security and Defence College and a member of the European Doctoral School on the Common Security and Defence Policy.

Cooperation between the Centre of Excellence 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). The focus is in particular on harbour protection, mini drones, Chemical, Biological Radiological and Nuclear (CBRN) related threats as well as countering improvised explosive devices (C-IED). Following the first successful joint workshop in May 2018, a second joint workshop on harbour protection, open to all relevant stakeholders, took place in October 2019. Since February 2019, the EDA has been contributing to the workshops organised under the HyFUTech (Hybrid Warfare: Future and Technologies) project led by the Centre of Excellence, 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.

In November 2019, the EDA and the Hybrid Centre of Excellence conducted back to back a number of cyber and hybrid related events in the context of the Finnish Presidency: the 25th EDA Project Team Cyber Defence Meeting with Member States, the EDA "Federation on Cyber Ranges" Demonstration and the Centre of Excellence Symposium on "Cyber Power in Hybrid Warfare".

Protection of critical infrastructure

In 2019, the Commission completed the evaluation of the *Directive 2008/114/EC on European Critical Infrastructure*[21], taking into account *inter alia* hybrid threats aspects. In its findings[22], the Commission found that while the Directive has brought EU added value, the technological, economic, social, policy/political and environmental context in which critical infrastructure in Europe operates has changed considerably since the Directive entered into force. In view of these changes and the challenges they pose to critical infrastructure operations, including security aspects, the Directive has now only partial relevance. This means that, while some elements of the Directive remain useful, others are of limited value today and should be revisited to better achieve the Directive's objectives. The evaluation showed an evolution in the threats facing critical infrastructure in Europe, with both new challenges emerging (such as unmanned aerial vehicles or artificial intelligence) as well as an increased risk from certain types of threats (e.g. hybrid threats, cyberattacks).

Nine Horizon 2020 Secure Societies projects were supporting critical infrastructure protection policy measures in various areas, including air and maritime transport, energy and services. In the 2019 call, five additional projects for a total amount of around EUR 30 million were selected to cover additional areas (space, railways, e-commerce supply chains and smart cities).

In its Work Programme for 2020, as well as in the Security Union Strategy[23] and in line with December 2019 Council Conclusions, the Commission announced its intention to present a proposal for additional measures on critical infrastructure protection before the end of 2020.

Energy security of supply and energy infrastructure

[21] OJ L 345, 23.12.2008, p. 75.
[22] SWD (2019) 310 final.
[23] COM(2020)605

Additional measures have been undertaken to increase security of energy supply in the EU, including at regional level, such as equipping interconnection points with the capacity to flow gas in both directions (so-called reverse flows).

In accordance with the *Regulation 2017/1938 on security of gas supply*[24], all regional and national security of supply risk assessments (taking into account political, technological, commercial, social and natural risks, e.g. cyberattacks, sabotage, terrorism) have been finalised and a large number of Member States have already adopted their preventive action plans and emergency plans. For the rest, the plans established under the previous *Regulation 2010/994 on security of gas supply*[25] remain in place. Member States are currently working on technical, legal and financial arrangements to implement the solidarity provisions contained in the *Regulation 2017/1938*. In the meantime, solidarity provisions can be applied on an *ad-hoc* basis.

Following the entry into force of the *Regulation 2019/941 on risk-preparedness in the electricity sector and repealing the Directive 2005/89/EC*[26], there are now concrete terms and obligations regarding the provision of solidarity and mutual assistance among Member States both in the field of gas and electricity. During a crisis, as a last resort measure and after exhausting all possible national measures, Member States can trigger a request for solidarity to other Member States to ensure a supply of gas to their households and a limited number of essential social services. Similarly, in the case of electricity, Member States may require assistance from other Member States to prevent or manage electricity crisis for the purpose of protecting public safety and personal security. The provision of solidarity or assistance is mandatory for Member States receiving a request and is based on the principle of a fair compensation. The Commission has issued guidance for Member States on the implementation of solidarity and assistance, in particular on compensation[27]. The first bilateral arrangements enabling a firm and permanent framework for solidarity in the gas sector have been agreed and will be procedurally finalised before the summer 2020.

To improve the protection of critical energy infrastructure, on which all other critical sectors rely upon, in June 2020 the Commission launched the Thematic Network on Critical Energy Infrastructure Protection. The network will foster collaboration among operators of critical infrastructure in the energy sector (oil, gas, electricity).

Preparatory work was launched in the area of supply chain security for critical energy technologies. An assessment was started in May 2020 to identify the critical supply chains for energy security and clean energy transition, and to propose measures for improving their resilience against pandemic and other threat scenarios.

In the defence sector, the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS II)[28] – a Commission funded initiative managed by the European Defence Agency (EDA) – continues in phase III (2019-2023) addressing energy security challenges including energy efficiency and buildings performance, renewable energy solutions and the protection of defence-related critical energy infrastructure as well as policy

[24] OJ L 280, 28.10.2017, p. 1.
[25] OJ L 295, 12.11.2010, p. 1.
[26] OJ L 158, 14.6.2019, p. 1.
[27] Commission Recommendation (EU) 2018/177 of 2 February 2018 on the elements to be included in the technical, legal and financial arrangements between Member States for the application of the solidarity mechanism under Article 13 of Regulation (EU) 2017/1938 of the European Parliament and of the Council concerning measures to safeguard the security of gas supply, OJ L 32, 6.2.2018, p. 52.
[28] See more information on CF SEDSS: https://eda.europa.eu/european-defence-energy-network/consultation-forum.

and behavioural interventions. The Forum aims at assisting the Ministries of Defence (MoDs) and related stakeholders to reduce their energy costs and ecological footprint while increasing operational efficiency and resilience. In this context, the Forum explores the benefits that could be achieved in the defence and security sector from the implementation of the Commission's related energy policy framework[29].

To support the efforts of the MoDs to increase the resilience of defence-related critical energy infrastructure against hybrid threats and address relevant vulnerabilities, a specific study will be developed as part of the CF SEDSS III phase III, entitled "Protecting of defence-related Critical Energy Infrastructure against Hybrid Threats". This study will provide the MoDs with a solid conceptual basis in order to develop the appropriate measures in the domain of preparedness and response for ensuring the resilience of those critical energy infrastructures that the defence sector depends on for their viability and effectiveness. The study will take into account the joint Centre of Excellence for Hybrid Threats-Joint Research Centre conceptual paper on hybrid threats as well as the lessons learned from the table-top exercise on hybrid threats that the Consultation Forum will conduct during phase III with the support of the Commission.

The EDA has also launched research projects such as the Smart Camps Technical Demonstrator and Smart Blue Water Camps and the Total Energy and Environment Military Capability Assessment Framework, 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 just initiated a project (ARTENET) with the primary objective to explore the role of artificial intelligence and its potential applications to military energy domain. The EDA continues, since 2016, to collect data and to establish a database on MoDs' energy consumptions aiming to gain an overview and to reinforce the position of the defence sector in the EU energy landscape; an initiative that is still ongoing and planned to be further developed within 2020.

Transport security

For all areas of transport, namely civil aviation, maritime transport and land transport, the Commission, together with the relevant agencies, has continued discussions with Member States and Contracting Parties to the Agreement on the European Economic Area, industry and other stakeholders on emerging security threats of a hybrid nature, to gain knowledge and learn from experiences.

In the area of land transport security (being a prerogative of the Member States and with no common EU rules), the Commission continues its work to improve security and ensure a sufficient coordination at EU level. The Commission adopted an *Action Plan*[30] listing concrete actions to improve passenger railway security, including the establishment of an EU Rail Passenger Security Platform bringing together Commission, Member States and key stakeholders. Its work has delivered best practices documents in the areas of risk assessment, insider threats, and detection technologies suitable for railways[31]. Moreover, the Commission

[29] The CF SEDSS III will identify the implications (benefits, opportunities and barriers) regarding the implementation of the following directives and regulations in the defence sector: Energy Efficiency Directive (EED), Renewable Energy Directive (RED), Energy Performance of Buildings Directive (EPBD), Directive on European Critical Infrastructures (ECI), Regulation on Security of Gas Supply; Regulation of Risk Preparedness in the Electricity Sector, and when relevant, the Regulation on the Governance of the Energy Union and Climate Action. For more information about the scope of the CF SEDSS see https://eda.europa.eu/european-defence-energy-network/phase-iii.

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

[31] Idem.

has published a security guidance toolkit for commercial road transport to help protect against truck hijacking, theft and unlawful intrusions[32]. The Commission is currently preparing a delegated act detailing standards on the level of service and security of safe and secure truck parking areas in the EU and procedures for the certification of such parking areas.

As far as aviation security is concerned, the Commission continued to ensure a high level of protection in EU airports, supported by the Commission inspections system, in accordance with EU legislation in place. In 2019, the Commission carried out 28 comprehensive inspections and assessments covering airports, air carriers and entities in 23 countries.

The Commission continued to carry out its regular monitoring of emerging threats, including hybrid threats, to adapt the Aviation Security (AVSEC) baseline. The Commission continued to facilitate sharing of information between Member States and to carry out specific risk assessments on overflight of conflict zones. Based on the mechanism of regular risk assessments as well as their follow up and reviews, the European Union Aviation Safety Agency (EASA) with the support of a network of national contact points continues to issue recommendations in this regard in its *Conflict Zones Information Bulletin*[33].

Unmanned aircraft systems (UAS, or simply drones) have the potential to be used by different malicious actors, including the ones involved in hybrid actions, to conduct surveillance, disrupt critical infrastructure operations or attack high-value targets. The Commission is squarely engaged in supporting the Member States in countering such misuse through a combination of measures. Some of these are legislative (for instance, the technical requirements and rules for drones' operators[34], adopted in 2019) and seek to empower competent authorities to exclude non-cooperative drones from restricted airspace, notably by providing for the registration of drone operators, the mandatory remote identification of drones, and by contributing to the greater preparedness of airports.

Following drone incidents at EU airports in 2018 and in 2019, the Commission and EASA are exploring possible preparedness, preventive and response measures.

Further, the Commission is currently preparing a proposal for a European unmanned traffic management concept (the U-Space), which should make it easier for authorities to distinguish between cooperative and non-cooperative, potentially malicious drones overhead. In order to support authorities dealing with non-cooperative drones specifically, the Commission is taking additional steps, such as supporting the development of different forms of guidance materials (e.g. by EASA), financing innovative counter-drones projects and studies, and building bridges between different affected sectors (e.g. law enforcement, aviation, critical infrastructure, prisons, customs/borders, personal protection, mass events) and types of stakeholders. Besides Member States authorities, these include third countries, international organisations, industry, academia and civil society. Finally, the Commission has envisaged launching an initiative aimed at facilitating a more coordinated European approach to the testing of different counter-drones technologies, which are in many cases expensive and not independently validated.

In February 2019, the European Defence Agency (EDA) and the EU Military Staff organised a joint workshop to support Common Security and Defence Policy operations by proposing short term solutions to fill gaps in countering unmanned aerial systems, as identified through the EU Headline Goal Process, while putting these actions in the context of longer term

[32] https://ec.europa.eu/transport/themes/security/land_security/road-security-toolkit_en.
[33] https://www.easa.europa.eu/easa-and-you/air-operations/information-on-conflict-zones.
[34] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, OJ L 152, 11.6.2019, p. 45–71.

capability development activities, in line with challenges and Avenues of Approach identified in the related Strategic Context Case (SCC) Air Superiority. Member States agreed to organize a follow-up event on this topic in the course of 2020, which will involve both governmental and private sector stakeholders.

EASA is preparing new measures to manage information security risks that may compromise the confidentiality, integrity and availability of information being stored, transmitted or processed through the aeronautical information systems used in civil aviation. This initiative is expected to efficiently contribute to the protection of the aviation system from cyberattacks and their consequences. The provisions shall apply to competent authorities and organisations in all aviation domains (i.e. design, production, management of continuing airworthiness, maintenance, air operations, aircrew, air traffic management/air navigation services and aerodromes)[35].

On maritime security, the Commission continued to support, in line with the revised *EU Maritime Security Strategy Action Plan (EUMSS AP)*[36], a coordinated response to all challenges affecting people, activities, and infrastructure in the maritime domain, including to hybrid threats. A new implementation report on the *EUMSS AP* is envisaged for September 2020, based on the inputs from the Member States and EU institutions and agencies. In line with the above, the Commission ensured, supported by the Commission Maritime Security Inspections system, that ships, ports and port facilities (port terminals) in the EU are properly secured and protected, in accordance with international and EU legislation in this field. In 2019, the Commission carried out 96 maritime security inspections, covering national administrations, ports, port facilities and ships.

Promoting the EU legislation in this domain, and following studies on ferry and cruise ship security, the Commission organised meetings and discussions with stakeholders to explore deliverables on passenger ship security, focusing on protecting passengers. The Commission plans to carry out a risk assessment and to develop guidelines for best practices in passenger ship security.

The Commission analysed trends in maritime security - covering also piracy and maritime disputes - that could disrupt shipping and trade routes and that could affect EU interests. In view of the fact that 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 developments, incidents or attacks on existing and future maritime trans-oceanic trade routes could have significant disruptive effects on value and supply chains in Europe. For example, series of maritime shipping attacks in the Gulf of Aden and around Bab-el-Mandeb and Hormuz Straits were particularly monitored for possible highly disruptive effects to EU and global shipping and trade.

Regarding maritime surveillance, a Transitional Phase[37] has been 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 in 2021. In addition, at the end of 2019, the last three national interoperability projects (out of 13 in total), funded under the European Maritime and Fisheries Fund (EMFF), have been finalised. They aim at improving information technology interoperability between national maritime authorities under CISE framework and thereby enhancing maritime

[35] See https://www.easa.europa.eu/sites/default/files/dfu/NPA%202019-07.pdf.
[36] Maritime Security Strategy (EUMSS) Action Plan, as adopted by the General Affairs Council on 26 June 2018.
[37] The CISE transitional Phase is managed by EMSA and benefits for the scientific and technical support of the Commission's Joint Research Centre.

awareness through improved information exchange across sectors and borders. Further work shall also take into account voluntary, sectoral and cross-border initiatives such as the MARSUR project set up in the European Defence Agency's framework.

In order to support and develop further EU-level preparedness to counter and prevent maritime hybrid threats at political, operational and technical levels, the Centre of Excellence for Countering Hybrid Threats organised a series of events leading to development of a taxonomy of maritime hybrid threat with 10 scenarios. Some of the scenarios were tested in the scenario-based discussions organised by the Finnish Presidency or presented in an exercise format to the Political and Security Committee. The Centre of Excellence continues its work to educate institutions' and Member States' maritime operators as well.

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) is ongoing in the following five areas: information sharing, surveillance and communication services, capacity building, risk analysis and capacity sharing. The main aim of this cooperation, in line with the *EU Maritime Security Strategy Action Plan (EUMSS AP)* is to assist national authorities in the performance of their coast guard functions.

The European Coast Guard Functions Forum (ECGFF) represents the gathering of coastguard authorities, agencies and other bodies at regional, national or European level, strongly supported by the Commission. The current French Presidency of this Forum is focusing on consolidating the information exchange in the maritime field, continuing to operationalise the cooperation on European Coast Guard Functions and ensuring the complementarity with the coordinated activities of the relevant European agencies.

With a view to enhancing border security and detection capacity against the illicit entry of chemical, biological, radiological and nuclear material, two e-Learning modules of a comprehensive training on radiation and nuclear detection techniques, trends and new challenges for customs experts from Member States have been made operational as of June 2020 in addition to the previous one-year training campaign at the Joint Research Centre's facilities in Karlsruhe. In addition, funding instruments such as Horizon 2020 have been used to facilitate research on new technologies and solutions to enhance for example detection capabilities of border and customs security authorities.

The third progress report on the implementation of the *Customs Risk Management Strategy and Action Plan*[38] will be submitted to the Council by the end of 2020. A revised strategy and a new action plan on customs risk management will be adopted in the first quarter of 2021. It will allow Member States and the Commission to oversee the launch of new actions with a view to meeting new challenges. Thanks to a new monitoring system, it will improve the ability of Member States and the Commission to measure progress in terms of greater protection balanced with trade facilitation, by collecting and analysing evidence-based data. The revisited strategy will also further integrate non-revenue issues, such as safety and security related risks, in particular in the area of prohibitions and restrictions. It will provide the tool for a responsive and structured governance enabling Member States to address properly risks and shall make joint data analytics a core element in the risk management framework.

[38] COM(2014) 527 final.

Space

In recent years, new safety and security threats have emerged. These threats are increasingly cross-border (e.g. terrorism, natural disasters related to climate change) and cross-sectorial (e.g. cybercrime, coronavirus pandemic), highlighting the need for closer cooperation, and better use of our common or shared tools and capabilities.

The EU space programmes Galileo and Copernicus are excellent examples of EU initiatives, developed with amazing foresight 20 years ago, which have now resulted in EU level autonomous infrastructures providing services directly relevant to resilience, safety, and security. For security actors (police, border management, civil protection, fisheries control, defence, etc.), access to EU autonomous space enabled services, in particular for the trio communication, navigation and Earth observation, is essential. Therefore, also in order to counter hybrid threats and to provide protection to citizens, it is of great importance to be able to rely on EU space infrastructure.

In the area of satellite navigation, the Commission is currently undertaking a new initiative to foster the use of Galileo in critical infrastructure that depends on space services for timing and synchronisation (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) and Globalnaja Nawigacionnaja Sputnikowaja Sistiema (GLONASS)). The initiative considers awareness actions on Galileo's and European Geostationary Navigation Overlay 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. The Commission launched an impact assessment study in August 2019, which will be concluded in 2020. In addition, an online open public consultation was published between March and June 2020.

Satellite communication is the area where space solutions deliver cross-cutting capability in countering hybrid threats. 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 in a hybrid threats environment. While the initiative will officially become a component of the European Space Programme as of 2021 (on par with Galileo, Copernicus and Space Situational Awareness), preparatory actions (with funds from the European Parliament) are already being implemented, in coordination with Member States and relevant EU agencies. The relevant activities have started, based on a Contribution Agreement with the European GNSS Agency (GSA) for the implementation of GOVSATCOM, signed in April 2020.

In addition, a project funded under Horizon 2020 and coordinated by the Global Navigation Satellite System Agency (GSA) is expected to start in September 2020 to establish a Network of Users for governmental Satellite Communications in Member States and the relevant EU agencies[39], aiming at achieving a reliable collaboration and coordination between them. Furthermore, 15 Member States participating in the European Defence Agency (EDA) plus the ATHENA Mechanism are contributing to the Project Arrangement for the European Defence Agency's GOVSATCOM Pooling and Sharing Demonstration Project, which has

[39] 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).

been in execution phase since in January 2019 and has been already providing the first Governmental SATCOM services.

Concerning the security of EU space assets, the Council and the High Representative have been given specific responsibilities by the Council Decision 2014/496/CFSP[40] to avert a threat to the security of the Union or one or more Member State(s) or to mitigate serious harm to their essential interests arising from the European Global Navigation Satellite System (GNSS) or in the event of a threat to the operation of the system or its services. The European External Action Service 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.

Given that all EU Space Programme components (Galileo, Copernicus, future GOVSATCOM and SST) are critical, in parallel to the Commission's proposal for the Space Programme under the next Multiannual Financial Framework, the High Representative made a proposal to the Council with the view to extend the scope of Council Decision 2014/496/CFSP to the whole Space Programme.

In addition, space-enabled services, in particular Earth-observation capability, can be used as instruments to provide counter intelligence in order to counter fake news. Indeed the EU Satellite Centre (SatCen) provides to the EU INTCEN fast and flexible satellite imagery services, together with its value-added interpretation that allows faster, better and more accurate identification of facts and interpretation of matters.

Moreover, the Satellite Centre's competences have been exploited for the benefit of Copernicus, both through its operational support to the European Border and Coast Guard Agency (Frontex) in the context of border surveillance and as provider of the Copernicus "Support to EU External Action" (SEA) service. Copernicus provides situational awareness through satellite images on activities on the ground, thus contributing to some of the security needs of the European Union and supporting countering hybrid threats through for instance border surveillance, crisis prevention and recovery, monitoring and assessment of critical infrastructure etc. Initial work on the evolution of the Copernicus Security Service has started with the aim to enhance the security capabilities and provide adequate response to the evolving security challenges that Europe is facing. This illustrates the benefits of a "joined-up inter-agency and cross-sectorial approach" for enhancing synergies between Union activities.

Defence capabilities

With a view to refine the link between research, industrial capability development and technology, including the hybrid threats dimension, the European Defence Agency (EDA) has developed, together with Member States, Strategic Context Cases (SCC), which are used as a guidance to implement the EU Capability Development Priorities. The aim is to translate the EU Capability Development Priorities agreed by Member States into concrete collaborative projects and programmes, which will also contribute to countering hybrid threats, by indicating future avenues of approach for collaborative activities in the short-, mid- and long-term perspective. The first edition of the SCC was presented for endorsement by Member States at the EDA's Steering Board in the Capability Directors' composition on 27 June 2019. The SCC fully reflect the High Impact Capability Goals (HICGs) that have been defined in the context of the EU Headline Goal Process, referring to the military requirements for facing hybrid challenges and threats in the vicinity of Europe in support of the EU Level of Ambition (LoA) on security and defence.

[40] OJ L 219, 25.7.2014, p. 53

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.

The work programme of the two pilot programmes of the European Defence Fund (Preparatory Action on Defence Research (PADR) and European Defence Industrial Development Programme (EDIDP)[41]), also included several project categories related to strengthening the resilience against hybrid threats. This includes cyber capabilities (e.g. for increased cyber situational awareness and countering cyber attacks), cross-domain capabilities (EDIDP calls 2019-2020[42]), maritime resilience and surveillance (e.g. capabilities for improved harbour protection), as well as chemical, biological, radiological and nuclear (CBRN) capabilities for threat detection and counter measures (call 2020). In response to the 2019 EDIDP call, 40 proposals have been submitted and the Commission in June 2020 selected for funding 16 proposals involving 223 legal entities and grants exceeding EUR 200 million. In addition, in April 2020, new calls for 2020[43] were opened with a submission deadline on 1 December 2020.

Regarding PADR, following the launch of the last four calls in March 2019, close to 100 proposals have been submitted. The total budget for these calls amounted to EUR 23 million. After the technical evaluation of the proposals, seven projects were selected for awarding a grant agreement and they are expected to start in the summer of 2020. In addition, one call was published with the topic on Future Disruptive Technologies, inviting cutting-edge, high-impact research proposals. The process allowed gathering valuable experience for the implementation of the future European Defence Fund, in which up to 8 % of the budget will be devoted to research and development on disruptive technologies. The Commission adopted the last list of eight selected projects under this call in June 2020. In total, 18 projects from 2017-2019 calls have been supported under the Preparatory Action 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. With a proposed budget of EUR 8 billion, the Fund will provide a major contribution for the European defence industry strengthening its innovation and manufacturing potential. Capabilities developed with the support of the Fund will reinforce the defence capacity of the Union including improving the resilience against hybrid threats.

In the context of the cyclic Headline Goal Process (HLGP) the Council has revised, in 2019, the EU CSDP military "needs" (Requirement Catalogue) and defined what the EU "has", in terms of military forces and capabilities declared as potentially available to CSDP missions and operations by MS' in the Force Catalogue. So forth, requirements and available capabilities to face a hybrid threat in the context of CSDP missions and operations have been analysed in view of contributing to the EU LoA on security and defence.

---

[41] Regulation (EU) 2018/1092 of the European Parliament and of the Council of 18 July 2018 establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union's defence industry, OJ L 200, 7.8.2018, p. 30

[42] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-search;freeTextSearchKeyword=;typeCodes=1;statusCodes=31094501,31094502,31094503;programCode=EDIDP;programDivisionCode=null;focusAreaCode=null;crossCuttingPriorityCode=null;callCode=Default;sortQuery=openingDate;orderBy=asc;onlyTenders=false;topicListKey=topicSearchTablePageState

[43] https://ec.europa.eu/research/participants/data/ref/other_eu_prog/edidp/wp-call/edidp_call-texts-2020_en.pdf

With the aim of achieving the EU CSDP military LoA, the Council has identified, throughout the HLGP process, a list of short and medium HICGs which comprise several capability gaps related to hybrid threats (such as CBRN defence, Cyber defence, Command and Control measures and STRATCOM needs). In the context of the Coordinated Annual Review on Defence (CARD) and through bilateral dialogues with participating Member States, conducted jointly by the EDA and the European Union Military Staff (EUMS), a specific analysis of the HICGs implementation throughout national programmes has been conducted in 2019. With the contribution of the EUMS, the results will be reflected in the CARD Aggregated Analysis to be presented to the EDA Steering Board on 25 June 2020 and subsequently to the European Union Military Committee (EUMC). Further work will build on the HICGs revision that will be conducted by the Council in the context of the HLGP Progress Catalogue throughout the summer 2020.

Protecting public health and food security

Apart from being instrumentalised by the hybrid actors to spread disinformation and thus posing risks to the public health, the COVID-19 pandemic has had an unprecedented impact on medical and healthcare staff, patients and health systems in Europe. As such, it has revealed a clear need to strengthen the EU crisis management capacity. Several EU financial instruments have been used to provide support for cooperation, capacity-building and research activities in the field of fight against serious cross-border health threats. These include the EU Health Programme, Innovative Medicine Initiative, Horizon 2020 and the Emergency Support Instrument. In the Multiannual Financial Framework (MFF) 2021-2027, new EU health programme, EU4Health will invest EUR 9.4 billion to:

- Strengthen crisis-preparedness and response to cross-border health threats, in line, where relevant, with the One health approach;
- Strengthen health systems, their resilience to crises, and their capacity to promote health and prevent diseases;
- Improve the availability of medicines and other crisis relevant products;
- Support integrated work among Member States and national health systems.

A Joint Action under the EU Health Programme will start in 2020 under Norwegian coordination with a view to strengthening health preparedness and response to biological and chemical attacks, through increased laboratory and treatment capacities and medical countermeasures and cross-sectoral collaboration. The partners and work package descriptions are already in place.

In 2019, the Commission signed a joint procurement framework contract with the company Seqirus for pandemic influenza vaccine involving 11 Member States. The conditions agreed will guarantee access to a defined part of the production capacity of the company Seqirus for up to six years, the total duration of the contract. A second contract with another company is under negotiations.

At the request of the Preparedness Working Group of the Health Security Committee , a two-days workshop was held in January 2020 with experts in the field as well as relevant practitioners from Member States. The focus of the discussions was on the health security threat posed by synthetic opioids, with topics covering the accessibility of synthetic opioids especially fentanyls, the evidence of weaponisation, the first response, clinical management and decontamination. Different working groups focused on clinical management, first responders and international and cross-sectoral aspects, developing relevant recommendations. The final report is currently under development.

In terms of improving resilience to hybrid threats within existing preparedness and coordination mechanisms in civil protection, a Staff Working Document[44] was presented in January 2020 on mass burn casualty response mechanism and a pilot training course for burns assessment teams was organised in February 2020. Moreover, nine projects are being funded under the Union Civil Protection Mechanism to increase urban resilience and further 12 projects on critical infrastructure including overarching systems.

The *Animal Health Regulation*[45] becomes applicable as of April 2021. The new rules will allow for greater use of new technologies for animal health activities, in terms of surveillance of pathogens, and traceability, including electronic identification and registration of animals. It will also offer other tools to support prevention and control of animal diseases, such as vaccination and vaccine banks. This will provide for better early detection, prevention and control of animal diseases and zoonoses, including emerging diseases linked to climate change and help to reduce the occurrence and effects of animal epidemics and better prevent pandemics using a One Health approach.

The *Plant Health Regulation*[46] became applicable in December 2019. It contains new measures to deal with surveillance and eradication as well as containment measures for high risk plants and pests. The new rules aim at enhancing the effectiveness of measures for the protection of plants. They also aim to ensure safe trade, as well as to mitigate the impacts of climate change on the health of agricultural crops and forests. Among the measures included in this legislation is the list of the most dangerous pests. For each of the listed pests, EU Member States are required to carry out annual surveys, draw up and keep up to date a contingency plan, perform simulation exercises, communicate with the public, and adopt an eradication plan. All these actions contribute to the EUs' coordinated, harmonised preparedness strategy for protecting agriculture, forests, environment and the economy from dangerous pests.

In February 2019, the Commission adopted the *Commission implementing Decision (EU) 2019/300 establishing a general plan for crisis management in the field of the safety of food and feed*[47]. This Decision repeals and replaces a former Decision of 2004, and establishes a revised general Plan for crisis management in the field of the safety of food and feed. This new Decision will help managing more effectively multi-country food/feed-borne incidents. Two types of situations are covered by the Plan: situations requiring enhanced Union coordination and situations requiring the setting up of a crisis unit bringing together the Commission as well as relevant Member States and Union agencies. The Plan sets out the practical procedures necessary for enhanced preparedness and for the management of incidents at Union level, including a communication strategy in accordance with the principle of transparency.

For situations of serious cross-border threats to health, the Commission has been working on the creation of a strategic stockpile at the EU level of essential medical countermeasures (vaccines and therapeutics), personal protective equipment, medical equipment and laboratory supplies. To this end, the medical stockpiling rescEU capacities have been adapted by means

[44] SWD(2020) 3 final.
[45] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:084:TOC.
[46] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R2031.
[47] OJ L 50, 21.2.2019, p. 55

of the *Commission Implementing Decision (EU) 2020/414*[48]. The implementation is ongoing with first direct grant to build the strategic stockpile signed and first items also delivered.

The Commission has been working to establish the necessary capacities under rescEU to respond to low probability risks with a high impact. Accordingly, the new *Commission Implementing Decision (EU) 2020/452*[49] designates certain capacities to respond to medical emergencies or incidents involving chemical, biological, radiological, nuclear or explosive substances to be fully financed by the EU with a view of ensuring their availability for deployment under the Union Civil Protection Mechanism.

Chemical, Biological, Radiological and Nuclear related risks

The *ad-hoc* group on chemical, biological, radiological and nuclear (CBRN) detection continued its work. Following the establishment of a list of 22 chemicals (January 2019) that are of most concern in terms of misuse for terrorist purposes, the group worked on the list of 21 chemical precursors that are susceptible to be used for manufacturing the 22 chemicals of concern. This work will further be integrated into rescEU CBRN capacity development under the Union Civil Protection Mechanism.

In addition, the Commission has launched a study that will examine ways to strengthen protection against the illicit use of dangerous chemicals in Europe. It will provide a fact-base needed for further dialogue with the relevant stakeholders including private actors, both when it comes to restricting access as well as better detection of these chemicals.

Preparation of a study to assess the implementation by Member States of radioactive source control measures, in particular record keeping and security of high-activity sources, is ongoing. The kick-off meeting for the study took place in January 2020 and the on-line questionnaire was sent to Member States in mid-April 2020.

In relation to CBRN risks, several large projects in third countries are in different states of implementation under the framework of the EU CBRN Centres of Excellence Initiative. In the Middle East, support has been provided to the first responders in case of CBRN related incidents. A second large project reinforced the capabilities of the medical responders in CBRN related cases. Experts trained during this project are considered world class and are currently training other experts in the neighbouring regions. In parallel, a project on protection of critical infrastructure related to CBRN risks (including water facilities in Jordan and critical command chain in Lebanon) is under implementation. In South East and Eastern Europe regions (Ukraine, Caucasus, Western Balkans), two projects have been completed and put to test, one on CBRN support to first responders and the second one in the field of forensics. A project on CBRN waste management is also under implementation.

Several projects dealing with CBRN were running under Horizon 2020, covering research on new tools and procedures (including funding of more than EUR 10 million within a specific cluster), as well as networking and training activities.

Cybersecurity

[48] Commission Implementing Decision (EU) 2020/414 of 19 March 2020 amending Implementing Decision (EU) 2019/570 as regards medical stockpiling rescEU capacities (notified under document C(2020) 1827) (Text with EEA relevance).

[49] Commission Implementing Decision (EU) 2020/452 of 26 March 2020 amending Implementing Decision (EU) 2019/570 as regards capacities established to respond to low probability risks with a high impact (notified under document C(2020) 2011) (Text with EEA relevance)

The Work Stream 7 (WS7) on large-scale cyber incidents of the Network and Information Security (NIS) Cooperation Group involves representatives from the Member States, the Commission and the EU Agency for Cybersecurity (ENISA). The Group has been working to implement the *Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises* (Blueprint)[50]. Since January 2019, the WS7 has been working on the operational level of Blueprint, building on the outcome of Blue OLEx 2019, a table-top exercise on the operational level of Blueprint organised by NIS Cooperation Group in July 2019 in Paris. The WS7 has now set up a Cyber Crises Liaison Organisation Network (CyCLONe), responsible for liaison with the relevant national authorities and for cross-border cooperation with respect to large-scale cyber incident and crisis management, and completed the first draft of CyCLONe Standard Operational Procedures (SOPs). This is required to enable interaction between national cyber crisis managing authorities at EU level. In addition, the Commission and ENISA will support Member States in the operation of the network of cyber crisis national authorities, notably by providing the appropriate information and communication technology tools for communication and information sharing.

Moreover, the Commission has announced its intention to explore possibilities for establishing a "Joint Cyber Unit"[51].

Following the Commission *Recommendation (EU) 2019/534 on the Cybersecurity of 5G networks*[52] adopted in March 2019, the NIS Cooperation Group presented an EU coordinated risk assessment of cybersecurity of 5G networks on 9 October 2019[53] and a "toolbox" of mitigating measures on 29 January 2020[54]. The EU toolbox was developed and agreed in cooperation between the Member States, the Commission and ENISA. The EU toolbox sets out, in a coordinated way, mitigating measures and risk mitigation plans, designed to address effectively major risks to 5G networks, such as criminal hacking, espionage and sabotage. On 29 January 2020, the Commission issued a *Communication on 'Secure 5G deployment in the EU- Implementing the EU toolbox*[55], in which it recommended to Member States to take concrete and measurable steps by 30 April 2020, with a view to implementing the set of key measures outlined in the EU toolbox conclusions. The report by the NIS Cooperation Group on the state of implementation of the key measures in the toolbox will be published in July 2020. The Recommendation of 2019 foresees its own review in the last quarter of 2020.

All Member States have notified the full transposition of the *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*[56] (NIS Directive). The Commission is currently performing in depth-checks of the notified measures. The Cooperation Group established by this Directive features sectoral activities (in particular on transport and energy) aimed at ensuring consistency between the implementation of the Directive and other initiatives on cybersecurity.

[50] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1581925949338&uri=CELEX:32017H1584
[51] https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf
[52] C(2019) 2335 final.
[53] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security
[54] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures (Publication of the NIS Cooperation Group), 29 January 2020.
[55] COM(2020) 50 final.
[56] OJ L 194, 19.7.2016, p. 1.

Implementation of the *Cybersecurity Act*[57] is ongoing. With its strengthened and focused mandate, ENISA will better contribute amongst other, to the EU and Member States activities in the areas of operational cooperation, crisis management, capability development and awareness raising thereby strengthening the resilience of the EU to cyber – and hybrid - attacks. Moreover, the Cybersecurity Act puts in place an EU cybersecurity certification framework for information and communications technology products and services. It will improve cybersecurity of products and services across the EU.

Contractual Public Private Partnership (cPPP) for cybersecurity

The contractual Public Private Partnership with the European Cybersecurity Organisation (ECSO) including more than 250 contributing members from private and public sectors has foreseen an alignment between private investment and EU investment under Horizon 2020 (up to EUR 450 million in 2016-2020 on research and innovation on cybersecurity technologies to better protect users and infrastructures against cyber and hybrid threats). This is expected to trigger a total of EUR 1.8 billion of investment in digital security and privacy industry in Europe by 2020. The latest monitoring report confirms that the above is on track[58].

Moreover, the Commission proposed in September 2018 the creation of a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres[59], with the aim *inter alia* to pool investments on cybersecurity technology and further deepen cooperation in the cybersecurity technology sector. The Croatian Presidency of the Council obtained a renewed negotiation mandate to re-enter trilogues with the European Parliament in June. The Commission encourages Member States and the European Parliament to proceed swiftly with the agreement on the text of the Regulation.

Cybersecurity in the transport sector

For the different transport modes (aviation, maritime and land transport), the Commission is working to increase their resilience to and protection from cyber-security incidents and attacks. 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 cyber threats are consistent with cross-sectorial capabilities covered by the Network and Information Security (NIS) Directive. The Commission organised, together with the EU Agency for Cybersecurity (ENISA), a series of workshops in 2019 on cybersecurity in the maritime, rail, and aviation sectors, bringing together different transport mode authorities, NIS implementation authorities, and stakeholders. Also in 2019, ENISA and the European Maritime Safety Agency (EMSA) organised a workshop on strengthening cybersecurity in ports.

The *EU Maritime Security Strategy Action Plan (EUMSS AP)* includes actions aimed at improving the integration of cybersecurity in the maritime domain in terms of capabilities, research, and technology building on civil-military coordination and synergies with EU cyber

[57] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7. 6. 2019.
[58] Monitoring report on cPPP, available at https://www.ecs-org.eu/documents/publications/5db82678564e8.pdf
[59] Proposal for Regulation to establish a Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres, COM(2018) 630 final.

policies, in line with the NIS Directive. It also promotes preparedness and response to hybrid threats, in particular cyber-attacks. Moreover, the Commission continued to ensure compliance with the cybersecurity-related obligations under existing EU maritime security legislation[60].

The Commission started to develop a holistic and interactive cybersecurity toolkit for transport (covering all transport modes), with a kick-off meeting held at the beginning of 2020 and to be finalised and presented before the end of the year. It will include recommendations of good practices to support security managers and professionals in the transport sector to better identify, assess and mitigate cyber security risks.

A coordinated approach to the consolidation of cyber-security in the maritime domain is promoted by the EUMSS AP in its main strands of work, such as maritime surveillance, capability development and risk management. Regarding **maritime surveillance**, in the beginning of 2020, the Commission launched a dedicated study aiming to develop and implement an information technology (IT) security framework for the Common Information Sharing Environment (CISE) network and information exchange. Developed in the framework of the Transitional phase, this work aims to consolidate the operationalisation of the future network.

In the **aviation sector**, in line with the new International Civil Aviation Organization (ICAO) cybersecurity standard, the Commission updated its Aviation Security legislation to address cybersecurity through the incorporation of requirements in the areas of training, security awareness, and background checks on staff having critical roles in information technology systems. The European Union Aviation Safety Agency (EASA) through its European Strategic Cybersecurity Platform (ESCP) continued to implement the roadmap on aviation cybersecurity where the Commission as well as all the aviation stakeholders are actively involved. One of the Platform's main goals has been to prepare the EU Cybersecurity (in aviation) Strategy[61] and to propose cybersecurity measures for aviation stakeholders to cover aviation safety and security. Since an initial pilot phase launched by the Agency in 2017, the European Centre for Cyber Security in Aviation (ECCSA) now operates as a platform for information sharing, threat analysis and standardisation programme. Close links have been established with the Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU) and with EUROCONTROL for providing expertise on existing threats and incidents.

Moreover, a gap analysis of existing cybersecurity rules in aviation has been conducted by the EASA, which resulted in the *Notice of Proposed Amendment 2019-07 on the Management of information security risks*[62]. It contains proposals for integrating those provisions in EU law.

In addition, the European Aviation Crisis Coordination Cell (EACCC), which was developed in 2011 in the aftermath of the volcanic ash crises, has now been established under the EU Network Manager[63], a function currently performed by EUROCONTROL. The aim is to train, monitor and coordinate responses to aviation network crises. Furthermore, the ongoing SESAR project modernising the Air Traffic Management also embeds cybersecurity as an integral part.

---

[60] https://eur-lex.europa.eu/legal-content/En/LSU/?uri=CELEX:32004R0725

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

[62] https://www.easa.europa.eu/sites/default/files/dfu/NPA%202019-07.pdf

[63] Commission Implementing Regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011, OJ L 28, 31.1.2019, p. 1–45

In the context of emergency response, EASA formally cooperates with CERT-EU since 2017. The aim is to handle cyber security threats in commercial aviation. With the accreditation of the European Air Traffic (ATM)-CERT established under EUROCONTROL, a major step has been taken to monitor cyber incidents in air transport in Europe and worldwide.

In terms of building aviation security capacity in third countries, building on the achievements of the Civil Aviation Security in Africa and the Arabian Peninsula (CASE) project (closed in April 2020), a new project on aviation security was launched in December 2019 covering Africa, Middle East and Asia. It aims at improving aviation security ecosystem in partner countries primarily identified as priorities under the EU integrated risk assessment. This new project includes a component on cybersecurity capacity building, based on the standards set out by the International Civil Aviation Organization regulations.

The European Defence Agency (EDA), in collaboration with EUROCONTROL organised a workshop on cyber awareness, education and training at the end of 2019, bringing together civil and military aviation stakeholders, to achieve a common understanding of current and future cybersecurity challenges and raise the importance of appropriate consideration of the human factor within the overall aviation system. This event also highlighted the need to equip personnel with the necessary knowledge and skills to effectively assess cybersecurity risks and better counter cybersecurity threats, including hybrid threats.

Cybersecurity in the energy sector

In October 2019, a dedicated sectorial work stream of the Network and Information Security (NIS) Cooperation Group published a reference document on the sectorial implementation of the Network and Information Security Directive in the energy sector[64]. It presents an overview of the status of implementation of Article 5 of the Directive for the energy sector, analyses key findings, challenges and sectorial specificities. The document provides good practices and examples of implementation of the main Directive's requirements: identification criteria, security measures and incident reporting requirements specific for the energy sector.

In July 2019, the Commission organised a high-level event on cybersecurity in the energy sector. The key conclusions were that energy security will stay essential and energy cybersecurity is a growing challenge. The energy grid will increasingly get smarter and more digitalised, while system security needs to be tested periodically and information sharing is crucial. Cybersecurity certification needs to be targeted to where it adds most value and a network code on cybersecurity for cross-border electricity flows is needed to improve and harmonise action. Moreover, the shortage in cybersecurity skills needs to be addressed.

By means of the *Regulation (EU) 2019/943 on the internal market for electricity*[65], the Commission has been empowered to establish a network code on cybersecurity in cooperation with the relevant associations of electricity network providers and regulators. The work is ongoing and the targeted stakeholder consultation was completed in May 2020. 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.

[64] Report available at: https://ec.europa.eu/digital-single-market/en/news/eu-wide-cybersecurity-legislation-report-implementation-eu-rules-energy-sector.
[65] OJ L 158, 14.6.2019, p.54.

In line with the *Regulation (EU) 2019/941 on risk preparedness in the electricity sector*[66], Member States are obliged to prepare, by January 2022 (and to update every four years thereafter), risk preparedness plans for electricity with certain mandatory elements; dealing with crisis situation; monitoring security of supply.

Cybersecurity in the financial services sector

The Commission is an active-observer in the European Central Bank's European Cyber Resilience Board for pan-European financial infrastructures' (ECRB) working group on information sharing. The group gathers both private sector participants and authorities (at EU and national level) to work on developing information sharing arrangements to further enhance the cyber resilience of the EU financial sector. In February 2020, the group announced the development of the building blocks enabling a trusted network for information sharing among pan-European financial infrastructures. The group is currently working to operationalise the initiative and in the coming months will publish the framework for the Cyber Information and Intelligence Sharing Initiative (CIISI-EU) to encourage other jurisdictions to follow. 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

Cooperation has been taken forward between the EU Agency for Cybersecurity (ENISA), the Computer Emergency Response Team for the EU institutions (CERT-EU), the European Defence Agency (EDA) and the European Cybercrime Centre of Europol (EC3) in the framework of their joint Memorandum of Understanding. Over the reporting period, the four agencies have conducted a number of joint activities allowing strengthened cooperation and synergies between these organisations in line with their respective mandates, in turn contributing to further developing the provision of expertise, operational and technical support to the EU and the Member States in the area of cybersecurity.

Several Member States are developing and contributing to two cyber defence-related projects under Permanent Structured Cooperation (PESCO): "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security" and "Cyber Threats and Incident Response Information Sharing Platform". In June 2019, Member States endorsed the Part I (Strategic context, European Capability Landscape, Major challenges in the domain, recommended Avenues of Approach) of the Strategic Context Case (SCC) on the 2018 EU Capability Development Priority *Enabling Capabilities for Cyber Responsive Operations* to facilitate and guide the implementation of cooperative solutions for capability development in the following areas: cooperation and synergies with relevant actors across cyber defence and cybersecurity areas; cyber defence research and technology activities; systems engineering frameworks for cyber operations; education, training, exercises and evaluation (ETEE); addressing cyber defence challenges in Air, Space, Maritime and Land. In February 2020, the EDA Steering Board endorsed the Part II of the SCC, which outlines current and potential EDA activities and projects in the domain. Implementation of SCC commenced within given resources and is expected to deliver first results by end of 2020.

Due to growing digitalisation of the defence capabilities and a cross-cutting, horizontal nature of cyber threats, the European Defence Industrial Development Programme (EDIDP) and the Preparatory Action on Defence Research (PADR) can support cyber defence projects in all military domains (land, air, space, sea and cyber). Two specific cyber and information and

[66] OJ L 158, 14.6.2019, p. 1.

communication technologies (ICT) calls have been issued under the EDIDP addressing the development of software-defined networks, communication capabilities, cyber defence situational awareness, cyber toolbox and cyber threat hunting. The total indicative budget earmarked for those projects is EUR 32 million.

In the PADR, within the project OCEAN2020, a significant part of the total budget of over EUR 35 million has been devoted to developing cyber related solutions. Moreover, projects selected for funding under 2018 and 2019 calls included research on electronic components enabling communication functionalities. Among them, the CROWN project aimed at developing a compact, lightweight multi-function radiofrequency system prototype integrating radar, electronic warfare and communication, while the project QUANTAQUEST focused on quantum sensing for navigation and timing and quantum communication to secure Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR).

In addition, a call on European high-performance, trustable (re)configurable system-on-chip or system-in-package for defence applications was launched in 2018 with an indicative budget of EUR 12 million to fund one project. This project, which is in the grant agreement process for a start in the first half 2020, will look at the hardware side of cyber defence technologies to protect the system architecture from intrusion or attacks.

In line with the updated 2018 EU *Cyber Defence Policy Framework*[67], the EDA continues to further develop courses in collaboration with the European Security and Defence College (ESDC) to meet the Member States' cyber defence education, training and exercises requirements. The full operational capability of the Cyber Education, Training, Exercises and Evaluation (ETEE) platform, established with the aim to address cyber security and defence education and training among the civilian and military personnel, was reached in September 2019. Five cyber courses (four awareness and one technical) developed in collaboration with the ESDC were provided throughout the academic year (2018-2019) with around 150 participants trained. Additional activities, for example, progressive integration of cyber education, training, evaluation and exercises modules developed in the frame of the EDA, have been planned and implemented during the current academic year (2019-2020).

The Cyber Security/Cyber Defence curriculum of the ESDC has been opened to the North Atlantic Treaty Organization staff and Third Countries that have signed a security agreement with the EU. Cooperation with the North Atlantic Treaty Organization's entities is continuing and expanding.

In addition, the Centre of Excellence for Countering Hybrid Threats 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 Common Security and Defence Policy 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 Centre of Excellence has also been invited to contribute to the identification and development of new Cyber/Hybrid Pilot Courses in support of the Cyber ETEE platform.

Gathering electronic evidence

The legislative procedures on the Commission's e-evidence proposals: *Proposal for regulation on European production and preservation orders for electronic evidence in*

[67] Council Document ST 14413/18

criminal matters[68] and *Proposal for directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*[69] are ongoing. Once adopted, these instruments will help law enforcement and judicial authorities to obtain electronic evidence that is needed for criminal investigations, e.g. on cybercrime. This includes emails or messages exchanged via apps, as well as information to identify a perpetrator as a first step.

The Council reached a General Approach on both the Regulation and the Directive in December 2018 and March 2019, respectively. Trilogues can start as soon as the European Parliament adopts its position on the legislative package.

Under the framework of International Digital Cooperation, the SIRIUS project implemented by Europol and Eurojust with support from the Commission contributes to improving cross-border access to electronic evidence, and thereby to effective implementation of the forthcoming legal measures regarding the e-evidence legislative package. The Commission is currently also establishing the e-Evidence Digital Exchange System between Member States. This system will allow for a faster and more secure transmission of European Investigation Orders and mutual legal assistance and related communication, including the electronic evidence sought.

Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "cyber diplomacy toolbox"), including a horizontal cyber sanctions regime

The *Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities*[70] (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. Following the 2017 June Conclusions, the relevant preparatory Council bodies have put in place implementing guidelines in October 2017. The implementing guidelines outline the measures as well as the decision-making procedure to invoke those measures. Following their adoption, the EU has continued to implement the guidelines, including by putting in place preparatory practices and communication procedures.

In response to the European Council of June 2018 and October 2018, Member States continuously improved the EU's ability to prevent, deter, detect and respond to malicious cyber activities, including by annual exercises, strengthening shared situational awareness and improving cooperation with international partners and the private sector. To build up the EU and its Member States' capacity to respond to and to deter cyber-attacks, on 17 May 2019, the Council established a framework which allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the EU or its Member States[71]. This sanctions regime against cyber-attacks threatening the Union or its Member States, consisting of a travel ban and asset freeze for natural persons and an asset freeze for entities, reflects the growing need to protect the integrity and security of the EU, its Member States and its citizens against cyber threats and malicious cyber activities. Restrictive measures may also be applied in response to a cyber-attack with a significant effect against third States or international organisations, where such measures are considered necessary to achieve the objectives of the Common Foreign and

[68] COM/2018/225 final - 2018/0108 (COD)
[69] COM/2018/226 final - 2018/0107 (COD)
[70] Council document 9916/17
[71] Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

Security Policy. Currently, no natural persons or legal entities are listed under this sanctions regime. Moreover, Member States in 2019 adopted guidelines on "Coordinated Attribution at EU level".

On 21 February 2020, the High Representative published a declaration on behalf of the EU condemning the cyber-attack that targeted Georgia on 28 October 2019 and underlined its political commitment to continue to assist Georgia in increasing its cyber resilience[72]. On 30 April 2020, following the increase in malicious cyber activities in the context of the COVID-19 pandemic, the High Representative published a declaration on behalf of the EU condemning malicious cyber activities targeting essential operators in Member States and noting the EU's resolution to prevent, discourage, deter and respond to such activities[73].

International cooperation in cybersecurity

Given the commitment of the European Union and the 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 the international security: the Open-ended Working Group linked to the developments in the field of information and telecommunications in the context of international security and the Group of Governmental Experts (GGE) to advance responsible State behaviour in cyberspace in the context of international security. The EU and its Member States contribute to the discussions to make constructive progress with the implementation of the 2010, 2013, 2015 GGE reports. These cover, among other, how international law applies, the implementation of agreed non-binding voluntary norms of responsible state behaviour and confidence building measures, as well as the development of practical means to implement them, including through targeted capacity building.

Taking into account the global nature of the threat, building and maintaining robust alliances and partnerships with third countries is fundamental to the prevention and deterrence of cyber-attacks as well as to advancing international stability and security. The EU has achieved setting up specific cyber dialogues with the United States, Japan, Brazil, India, South Korea and China. Close consultations with regional and international organisations are also in place, notably with the North Atlantic Treaty Organization (NATO), the Association of Southeast Asian Nations (ASEAN) Regional Forum, the Organization for Security and Cooperation in Europe (OSCE), the Organization of American States (OAS), the Council of Europe, and the Organisation for Economic Co-operation and Development (OECD).

The EU has a close partnership with NATO in favour of an open, free, stable and secure cyberspace. Active interaction in the field of cyber security and defence has continued between staffs with exchanges on concepts and doctrines to establish a comprehensive overview of mutually beneficial conceptual ideas and documents in the cyber domain, reciprocal participation in cyber exercises, informal exchanges of information on existing and planned training and education courses, and of threat indicators, cross-briefings, including on the cyber aspects of crisis management, and regular meetings. On technical level, the Technical Arrangement on Cyber Defence between the NATO Computer Incident Response

[72] https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/
[73] https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/

Capability (NCIRC) and the Computer Emergency Response Team for the European Union (CERT-EU) continued to be implemented in line with existing provisions.

Cybersecurity capacity building is one of the priorities of the *Digital Agenda for the Western Balkans* outlined in the *Commission Communication: A credible enlargement perspective for and enhanced EU engagement with the Western Balkans*[74]. Under the Instrument for Pre-Accession Assistance (IPA II), the Commission approved in 2019 a regional programme, which aims to strengthen cyber resilience to better address the challenges of cyber threats and improve the overall security.

The 18 March Joint Communication on the Eastern Partnership policy beyond 2020[75] highlighted cyber resilience as one of the central policy priorities of the EU towards its Eastern partners. Based on the relevant EU standards and legislation, the EU will support the Eastern Partnership countries to implement robust and functioning cybersecurity frameworks. To this end, the EU Cyber Resilience programme for the Eastern Partnership countries, which includes a regional cybersecurity project, aims to bring the Eastern Partner countries closer to the core pillars of the EU standards, legal and policy framework, namely the Network and Information Security (NIS) Directive, EU Agency for Cybersecurity (ENISA) guidelines, and best practices and, where possible, the recently adopted EU Cybersecurity Act. The project was launched in January 2020 for a duration of 36 months.

In Ukraine, the EU carried out a number of activities in the run-up to presidential and general elections, including cyber exercises for main bodies responsible for the cybersecurity of elections, cyber hygiene training for political parties and preparation of the post-electoral assessment of the main threats during elections. In addition, the EU signed in February 2020 the EU e-government and digital programme for Ukraine, which is the largest bilateral EU programme of this kind in a third country. This programme has a cybersecurity component, including cyber exercises at technical and strategic level and other activities supporting the capacities of key bodies responsible for cybersecurity in Ukraine.

Under the *Annual Action Programme (AAP) 2018 for Georgia*[76], the new programme on security and good governance "Security, Accountability and Fight against Crime in Georgia (SAFE)" includes a component on 'hybrid and emerging threats' in order to strengthen cyber security capacities and to further improve resilience against cybercrime and threats posed to critical infrastructure.

The implementation of the SAFE Programme is under preparation. As part of SAFE, a Twinning on support to cyber security system development with the Data Exchange Agency and the Cyber Security Bureau of the Ministry of Defense will start in 2020. A second Twinning on cyber crime and critical infrastructure will be prepared as soon as Georgia advances with its strategy and law on critical infrastructure.

It should be noted that the SAFE Programme has been designed in a way to address also vulnerabilities identified under the currently ongoing hybrid risk survey. Furthermore, the bilateral Programme on "*Support for the Implementation of the EU-Georgia Association Agreement*" (AAP 2018 for Georgia) foresees capacity building for the Georgian Government as regards strategic communication and to respond to disinformation campaigns as part of hybrid and emerging threats.

[74] COM (2018) 65 final.
[75] JOIN(2020) 7 final
[76] C(2018) 8064 final

Screening of foreign direct investment

In accordance with the *Regulation 2019/452 establishing a framework for the screening of foreign direct investments into the Union*[77] adopted in March 2019, the Commission is preparing to launch a co-operation mechanism between Member States and the Commission in October 2020. This will serve to exchange information and to issue Member States' comments or Commission' opinions in relation to foreign direct investments likely to affect security or public order.

In addition, in response to the urgency of the COVID-19 outbreak, on 25 March 2020, the Commission issued *Guidance to the Member States concerning foreign direct investment and free movement of capital from third countries, and the protection of Europe's strategic assets*[78], ahead of the application of the *Regulation 2019/452*.

Targeting financing of hybrid activities

Since July 2018, the EU has strengthened its anti-money laundering and counterterrorism financing legal framework, in line with the 2016 Action Plan[79]. This includes implementation of the revised fifth Anti-Money Laundering Directive[80]; new rules facilitating the use of financial and other information[81]; minimum rules concerning the definition of criminal offences and sanctions; safeguards against illicit cash movements[82]; rules to prevent illicit trade in cultural goods[83].

Furthermore, in July 2019, the Commission adopted a Communication "*Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework*"[84] that gives an overview of four further reports with the aim of supporting European and national authorities in better addressing money laundering and terrorist financing risks. The Supranational Risk Assessment report[85] and its annex in the form of a staff working document[86] provides an update of sectorial risks associated with money laundering and terrorist financing. The report assessing the framework for cooperation between Financial Intelligence Units[87] analyses issues that are still remaining, such as access by FIUs to information, information sharing between FIUs, IT tools as well as the limited scope of the FIU's platform and suggests concrete changes, such as for instance a new support and coordination mechanism. The report on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts[88] sets out a number of elements to be considered for a possible interconnection of bank account registries and data retrieval systems and calls for

[77] OJ L 79, 21.03.2019, p. 1.
[78] C (2020) 1981 final.
[79] COM(2016) 50 final.
[80] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ L 284, 12.11.2018, p. 22–30.
[81] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, OJ L186, 11.7.2019, p.122-137.
[82] Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 OJ L 284, 12.11.2018, p. 6.
[83] Regulation (EU) 2019/880 of the European Parliament and of the Council of 17 April 2019 on the introduction and the import of cultural goods OJ L 151, 7.6.2019, p. 1.
[84] COM (2019) 360 final
[85] COM (2019) 370 final
[86] SWD (2019) 650 final
[87] COM (2019) 371 final
[88] COM (2019) 372 final

further legislative action in this regard. Finally, the report on the assessment of recent alleged money laundering cases involving EU credit institutions[89] analyses ten recent publicly known cases of money laundering in EU banks to provide an assessment of some of the current shortcomings and to outline possible remedial solutions, for instance through further harmonisation across Member States and strengthened supervision.

Based on the observations in these reports and calls from the European Parliament and the Council, the Commission adopted on 7 May 2020 an Action Plan for a Comprehensive EU policy on preventing money laundering and terrorist financing[90]. The Action Plan is built on six pillars: (i) the effective application of EU rules, i.e. the close monitoring of the implementation of EU rules by the Member States, (ii) a single EU rulebook to align previously diverging interpretations of the rules by the Member States, (iii) an EU-level supervision to close gaps in national supervision of AML/CFT rules, (iv) a coordination and support mechanism for Member States' Financial Intelligence Units, (v) the enforcing of EU-level criminal law provisions and information exchange by facilitating cooperation and exchanges of information between law enforcement authorities and (vi) a stronger role for the European Union at the global level, i.e. a more active involvement within the Financial Action Task Force (FATF) in shaping international standards.

Building resilience against radicalisation and violent extremism

Communication and online propaganda remains a key priority addressed in the Strategic Orientations 2020[91] adopted by the Steering Board for Union actions on preventing and countering radicalisation[92], underlining also the need to build resilience and promote EU values. Looking at the challenges posed by COVID-19, members of the Steering Board for Union actions on preventing and countering radicalisation agreed in June to explore further how to strengthen digital resilience in a more holistic manner, taking into account interrelations between terrorist or extremist propaganda, disinformation, hate speech etc.

As far as the EU-funded European Strategic Communications Network is concerned, until December 2019 it worked with Member States, among others, on the issue of disinformation and its implications on their work on preventing radicalisation. In 2020, the exchanges continue in a different format and focus on adjacent topics like extremists' and terrorists' narratives on COVID-19 and the strategic communications response. Communication and online propaganda remains a key initiative addressed in the Strategic Orientations 2020 adopted by the Steering Board of the Network to support EU actions on preventing and countering radicalisation, underlining the need to build resilience and promote EU values.

In September 2018, the Commission adopted a *Proposal for Regulation to prevent the dissemination of terrorist content online*[93]. It provides for clear rules on the prevention, identification, and swift removal of terrorist content online, to be imposed in a uniform manner across the Union, as well as robust safeguards to protect freedom of expression and information. The European Parliament and the Council resumed negotiations in October 2019, which are expected to be concluded in the course of 2020.

Voluntary cooperation together with the industry has continued within the framework of the EU Internet Forum where solutions to emerging trends are being discussed, including the

[89] COM (2019) 373 final
[90] COM (2020) 2800 final
[91] Strategic Orientations on a coordinated EU approach to the prevention of radicalisation, see: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=39835&no=1.
[92] https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626
[93] COM/2018/640 final.

increasing use of the online space by violent right wing extremists. Following the livestreaming of the attacks in Christchurch, a political commitment was given at the 5th EU Internet Forum, on 7 October 2019 for the *EU Crisis Protocol*[94], a voluntary mechanism to help coordinate a rapid, collective and cross-border response to the viral spread of terrorist and violent extremist content online. In the first half of 2020, two meetings of the EU Internet Forum have so far focused on providing guidance and greater understanding across sectors to address the abuse of the internet by violent right wing extremists and terrorists as well as identifying emerging trends.

Under the Instrument contributing to Stability and Peace (IcSP), a number of global P/CVE-specific actions have been launched around the world under the Strengthening Resilience to Violent Extremism (STRIVE) programme. These actions aim to facilitate innovative P/CVE projects in collaboration with local communities, to strengthen conditions conducive to development and resilience towards violent extremism through a whole of society approach. Some of them also address the impact of media on preventing violent extremism in the Middle East, North Africa, Sahel, Horn of Africa, Western Balkans and across Asia. This is among others done with organisations like Hedayah and the Global Community Engagement and Resilience Fund (GCERF).

To support the Civil Society Empowerment Programme (CSEP) and campaigns providing alternative narratives to terrorist propaganda and promoting fundamental rights and values, the Commission awarded at the end 2019 grants amounting to EUR 5.6 million to eight projects. To date, the programme was supported with EUR 13.7 million to twenty CSEP projects in total.

In the Secure Societies part of Horizon 2020, a dedicated topic that was published in March 2020, addresses comprehensive multi-disciplinary and multi-agency approaches to prevent and counter violent radicalisation and terrorism in the EU, including on violent extremism online (e.g. social media) and terrorist propaganda, as well as evaluation and impact of counter-narratives and alternative narratives. Besides this, two recent projects addressing methods to detect and analyse terrorist-related online contents and financing activities (TENSOR, finished November 2019, and RED-Alert, finished in May 2020) have been funded under Horizon 2020 so far.

Communication and online propaganda remains a key initiative addressed in the Strategic Orientations 2020 adopted by the Steering Board for Union actions on preventing and countering radicalisation[95], underlining the need to build resilience and promote EU values.

Increasing cooperation with partner countries

Responses to Hybrid Risk Surveys questionnaires were delivered by Georgia, Albania, North Macedonia, Kosovo* and Montenegro in the first part of 2019. Based on the replies provided, the EEAS and the Commission prepared a report in February 2020, which identifies the key vulnerabilities of each partner and formulates specific recommendations to increase each partners' resilience against hybrid threats. The priority is now to follow-up on the recommendations and to identify together with the four Western Balkans partners actions to mitigate the vulnerabilities identified, while with Georgia priority fields for further engagement have been agreed.

---

[94] 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.

[95] https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626

* 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 survey in Moldova, finalised in the second part of 2017 and transitioned into the project phase, has been put on hold due to political developments and can be relaunched only based on the principle of strict conditionality and respect for the rule of law and democratic standards and linked to concrete reform deliverables.

Reply from Jordan to the questionnaire launched in 2017 is pending due to the lack of the Information Exchange Agreement that would allow classified information exchange between the EU and Jordan.

Montenegro joined the Centre of Excellence for Countering Hybrid Threats in June 2019. Centre of Excellence organised a successful Elections interference training session in January 2020, which also had a general impact on hybrid awareness of local relevant authorities. There is a growing interest from partners to establish a link with the Centre of Excellence, which could indeed deliver important assistance to these countries' preparedness (e.g. exercises, conceptual work).

EU Playbook and exercises

Following the successful completion of the Parallel and Coordinated Exercises (PACE) pilot project in 2017 and 2018, the mutual exchange of the lessons identified in these interactions was completed in summer 2019. The EU and the North Atlantic Treaty Organization have each started work to implement relevant lessons.

Building on this experience, discussions were launched at technical level between EU and the North Atlantic Treaty Organization staffs with a view to developing the plan for implementing Parallel and Coordinated Exercises in the years to come. Cross-briefings to relevant committees were held in autumn 2019.

Discussions on the new PACE plan are still ongoing at the staff level. While the new plan is being discussed and agreed, EU-NATO cooperation in the domain of exercises continues, including by mutual invitations to participate in respective exercises on a voluntary basis.

During 2019, EU staff participated in NATO's Crisis Management Exercise 2019 (CMX19), setting up an EU response cell that covered all possible reactions from the EU. NATO staff have been invited to participate in the relevant planning and conduct parts of the EU Integrated Resolve Exercise to be held in 2020.

The EU Playbook[96] is under review.

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

Following limited progress in implementing Action 20 of the 2016 Joint Framework on countering hybrid threats over the past four years, in June 2019, the Council invited Member States "to discuss the lessons identified following the first activation of Article 42(7) TEU" [97]. Subsequent discussions at various levels, including Defence Ministers, Defence Policy Directors and the Political and Security Committee (PSC), have shown that further work is required on increasing the common understanding on some of the aspects of Article 42(7) TEU, in particular on practical modalities for its implementation. PSC agreed in May 2020 to take work forward on the basis of further exercises and scenario-based discussions in the

[96] Joint Staff Working Document, EU operational protocol for countering hybrid threats 'EU Playbook', SWD(2016) 227 final.
[97] Council Conclusions on Security and Defence in the context of the EU Global Strategy, 17 June 2019, 10048/19

coming months, which will also comprise hybrid scenarios as well as scenarios relevant to Article 222 TFEU.

CSDP operations and missions

The revised "EU Concept for EU-led Military Operations and Missions", approved in December 2019[98], 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, two concepts with a link to countering hybrid threats, "EU Concept on Cyber Defence for EU-led Military Operations and Missions" and "EU Concept for CBRN Explosive Ordnance Disposal in EU-led Military Operations", are under revision.

Moreover, the new conceptual documents "EU Concept on Consequence Management after CBRN Incident for EU-led Military Operations and Missions" and Standard Operational Procedure (SOP) on countering Hybrid threats in CSDP Military Operations and Missions are under development. All of these documents are expected to be approved in fourth quarter of 2020.

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. A mini-concept on civilian CSDP support to countering hybrid threats has been developed.

EU-North Atlantic Treaty Organization 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[99] and the 2018 Brussels Joint Declaration[100]. Details of notable interactions are contained in the 5th Joint Progress report on the EU-NATO cooperation, presented to the respective Councils in June 2020. Cooperation has continued on crisis response and bolstering resilience through cross-participation in exercises, reciprocal cross-briefings and regular staff-to-staff dialogue. Notable example of the latter is the EU-NATO CBRN capacity building seminar with the participation of EU Member States/NATO Allies organised under the auspices of the Czech Permanent Representation, which took place in January 2020. As well, the EU and NATO exchanged concepts and best practices in the context of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("cyber diplomacy toolbox"). In June 2019, a staff-to-staff EU-NATO High level retreat was organised by the Centre of Excellence for Countering Hybrid Threats. 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 addition, the following practical arrangements can be highlighted: regular and structured staff-to-staff exchanges between the EU Hybrid Fusion Cell and NATO's Hybrid Analysis Branch on situational awareness, active staff-to-staff interaction between the respective strategic communications teams as well as between hybrid file-coordinators.

[98] ST14777/19
[99] https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf
[100] https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf

The Commission, the General Secretariat of the Council and the High Representative have been working at staff level with the North Atlantic Treaty Organization on designing an implementation plan for new Parallel and Coordinated Exercise activities. The aim of the plan is to continue exercising based on the pilot project that took place in 2017-2018 and the lessons learned from the exercises carried out in the past. The ultimate objective is to increase the mutual understanding, preparedness, cooperation and coordination for facing crisis coming from common hybrid threat.

Staff to staff contacts continued between the European Defence Agency and the North Atlantic Treaty Organization, covering harbour protection, countering mini drones and countering improvised explosive devices - areas, which all have a hybrid threats dimension.

CONCLUSION

The present report shows good progress in terms of EU level coordination and support to Member States' efforts to countering hybrid threats. Joined-up work has become the norm in cooperation within EU institutions and bodies. This ensures seamless coordination both in internal policies and in the external dimensions. In addition, there is a special and multifaceted cooperation with NATO and an expanding engagement with like-minded partners in multinational formats such as G7 or international cooperation on countering foreign interference led by Australia.

The common understanding of the terminology has developed significantly and today, there is awareness in all Member States on hybrid influencing and interference. Work has been ongoing in almost all Member States on establishing the appropriate structures for the whole of government approach and make initiatives to educate citizens in line with the whole of society approach. At national levels, an established Government level coordination and sufficient societal awareness would be the ultimate goal.

The newly established Horizontal Working Party chaired by the rotating Presidency was among the highlights of counter-hybrid work in 2019 an important milestone and at the same time a signal from Member States that they are ready for and willing to pursue a more structured coordination and cooperation with each other and the EU.

As the counter-hybrid threats work strands and toolbox have become increasingly complex in the face of the ever evolving nature of the threats, Member States expressed their interest in the December 2019 Council Conclusions to have an overview of the measures taken so far and of the relevant documents adopted. A mapping has been prepared by the Commission services and the EEAS. Both the mapping and the report are being presented in parallel to and at the occasion of the Security Union Strategy. When it concerns hybrid threats, the Strategy announces that the Commission and the High Representative will set out the future orientation of EU work and approach to counter them, with the aim to further consolidate and deepen efforts at EU level in this important field for the security of the Union and its citizens.