EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 28.5.2019
SWD(2019) 200/2 final

DOWNGRADED on 17.6.2019

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

Hybrid threats are a persistent challenge. Building resilience, detecting, preventing and responding to the threats remains predominantly Member States' responsibility, supported and complemented by actions at EU level.

Since 2016, the EU has set up a broad array of hybrid threats related counter measures in a substantial number of policy areas. Notably, the *2016 Joint Framework on Countering Hybrid Threats – a European Union response*[1] foresees 22 actions ranging from improving information fusion and situational awareness, to protecting critical infrastructure, cybersecurity, building resilient societies and stepping up cooperation with the North Atlantic Treaty Organisation. The implementation of the 22 actions has advanced at good pace as illustrated by two progress reports presented to the Council on 19 July 2017[2] and 13 June 2018[3] respectively.

The EU has also strived to adapt to changing security realities. In recognition of the evolving nature of the threat and following a tasking by the March 2018 European Council, in June 2018, the Commission and the High Representative adopted a *Joint Communication Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats*[4]. It reinforces the focus on strategic communications and situational awareness, chemical, biological, radiological and nuclear threats, resilience and cybersecurity as well as counter intelligence. The present, third report presents progress on the implementation of the 2016 Joint Framework and the 2018 Joint Communication taking stock of developments since June 2018. It should be read in conjunction with the progress reports towards an effective and genuine Security Union as well as the annual EU-North Atlantic Treaty Organisation joint progress report on the implementation of the common set of proposals for cooperation.

The implementation of the 2016 Joint Framework and the 2018 Joint Communication is being carried forward through close engagement of and interaction between the EU Member States, EU institutions and entities, and international partners, notably the North Atlantic Treaty Organisation.

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

The Council's Friends of Presidency Group on Countering Hybrid Threats (FoP) has continued its work on a risk survey launched in December 2017 and addressed to the Member States to identify key vulnerabilities, including specific hybrid related indicators, potentially affecting national and pan-European structures and networks. Based on the replies to the survey submitted by Member States until June 2018 and discussion in the Friends of Presidency Group, the Bulgarian Presidency presented to COREPER its report with summary

[1] JOIN (2016) 18 final.
[2] JOIN (2017) 30 final.
[3] JOIN (2018) 14 final.
[4] JOIN (2018) 16 final.

of key finding from national contributions and formulated conclusions with policy recommendations. To date, 24 Member States have provided input to the survey.

In June 2018, the initially one-year mandate of the Friends of Presidency was extended until June 2020 and significantly broadened. The group is now a valuable platform for sharing national experiences with hybrid incidents and best practices, for providing an overview of ongoing efforts on countering hybrid threats within the EU as well as for regular dedicated political discussions on this topic among Member States' practitioners.

Under the Security call of Horizon 2020, the Commission has allocated up to EUR 3.5 million to fund a network of practitioners handling hybrid threats. This pan-European network of practitioners and other actors should monitor research and innovation projects, express common requirements and indicate priorities for standardisation. By doing so, it is expected to contribute to the identification of EU-wide gaps in countering hybrid threats, as well as identifying solutions to be provided by market products, research and development.

EU Hybrid Fusion Cell

The EU Hybrid Fusion Cell, created inside the EU Intelligence and Situation Centre (EU INTCEN) in mid-2016, has continued to raise situational awareness and to provide strategic analysis to the EU decision-makers. This is done in close cooperation with the Intelligence Directorate of the EU Military Staff (EUMSINT) and through various established networks at EU and national level.

The Hybrid Fusion Cell's network of national points of contact for countering hybrid threats, established in 2017, has continued to meet bi-annually to exchange best practices and on issues of current interest. The national points of contact are seen as coordinators in capitals, bringing the various governmental departments together to build countering initiatives and resilience against hybrid threats.

Since its creation, demand for the Hybrid Fusion Cell's products continues to increase. In 2019, the team of analysts is being reinforced but vacancies still need to be filled, including with experts on cyber, counter-intelligence and other areas.

Strategic communications

Significant progress has been made in strengthening cooperation between the Commission services and the European External Action Service to tackle the disinformation from external and internal sources. The *Action Plan against Disinformation*[5], endorsed by the European Council in December 2018, is a key development of the last 12 months and telling example of enhanced cooperation between EU institutions and services, as well as with national authorities, industry and civil society. It sets out coordinated response to disinformation, centred around improving the capabilities to detect, analyse and expose disinformation, strengthening coordinated and joint response with Member States, mobilising the private sector and raising awareness, as well as improving societal resilience. The ten actions are implemented by the European External Action Service and the Commission services, in close cooperation with the European Parliament and Member States and in view of securing free and fair elections to the European Parliament.

As part of the implementation of the *Action Plan against Disinformation*, the Strategic Communication Division of the European External Action Service, its three Task Forces and

[5] JOIN (2018) 36 final.

the Hybrid Fusion Cell have been strengthened with additional staff, including recruitment of disinformation experts, data analysts, outreach officers and hybrid intelligence analysts. In the medium term, allocation of additional posts to tackle disinformation and raise awareness about its impact has been requested for the Strategic Communication Division of the European External Action Service and for the EU delegations in the Western Balkans, as well as in the Eastern and Southern neighbourhood.

In March 2019, a Rapid Alert System was set up to enable Member States and EU institutions to facilitate sharing of data, enable common situational awareness, facilitate the development of common responses, and ensure time and resource efficiency. EUR 1.1 million Preparatory Action under the 2018 EU budget (increased to EUR 3 million in 2019) was launched to further develop professional monitoring of the information environment. A team of over 20 external experts was contracted to support the work of the East Stratcom Task Force by providing tailored monitoring and big data analytics aimed at detecting and exposing of disinformation. The scope of monitoring in additional languages will be expanded in June 2019 to cover disinformation arising from pro-Kremlin sources in the Western Balkans and Southern neighbourhood countries. Further activities on awareness raising, as well as training on detection, analysis and responses to disinformation are foreseen for the latter part of the year and may include EU staff and other key stakeholders.

The Commission has dedicated resources across different services in order to monitor and detect disinformation, coordinate responses and, where appropriate, contribute to the Rapid Alert System.

The Commission, together with the High Representative and the European Parliament, has set up a working tripartite arrangement to address disinformation, focusing on awareness raising about the negative effects of disinformation, detection tools and analysis on disinformation campaigns, targeting both media and the general public. The actions aim at increasing citizens' resilience to disinformation campaigns, especially in an electoral context.

In line with the *Communication on Tackling Online Disinformation*[6], the Commission continues its efforts to increase societal resilience against disinformation by reaching out to citizens with proactive messages and positive narratives on the EU's policies and values. This is achieved in particular through the Commission's daily media outreach and the ongoing corporate communication campaigns InvestEU, EUandME and EU Protects, respectively based on three narrative strands: a Europe that delivers, a Europe that empowers and a Europe that protects. The Commission's contribution to the informal EU27 leaders' meeting in Sibiu (Romania) on 9 May 2019 outlined further measures to communicate effectively across the continent in times of increasing fragmentation and disinformation.[7] The Commission services also engage in quickly rebutting and debunking any type of disinformation that aims to mislead citizens about what the EU stands for. Important actors in this task are the Commission's Representations in the Member States, who are best placed to respond to disinformation locally and with country-specific context. They not only deal with the day-to-day responses to false information offline or online, but also engage in mythbusting activities, such as the initiatives *Bolas de Bruxelas* (Portugal) or *Les Décodeurs de l'Europe* (France).

[6] COM (2018) 236 final and report on implementation adopted on 5 December 2018, COM (2018) 794 final.

[7] Commission Communication *Europe in May 2019: Preparing for a more united, stronger and more democratic Union in an increasingly uncertain world,* COM (2019) 218 final, Part II.

In the context of the implementation of the *EU Code of Practice on Disinformation*[8], a self-regulatory instrument finalised in September 2018, the online platforms (Facebook, Google and Twitter) are developing internal intelligence capabilities to detect, analyse and block malicious activities on their services. The online platforms have provided information on these capabilities in reports submitted in connection with the Commission's monitoring of the *Code of Practice*.[9] Moreover, civil society and media organisations are stepping up fact-checking and research capabilities around disinformation. These stakeholder inputs can support work carried out by the Stratcom 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 the online media landscape, thereby reducing the potential impact of disinformation operations. In addition, these inputs can bolster public awareness and enable media literacy initiatives to enhance the ability of citizens to assess information critically.

In the context of the European Parliament elections and with a view to contribute to the curbing of digital interference risks in this democratic process, the Computer Emergency Response Team for the EU institutions (CERT-EU) launched a new Social Media Assurance service. This service allows the monitoring of the social media accounts, online presence of registered constituents and selected personnel in order to detect impersonation, non-official content and proceed to takedowns, on demand. In the framework of the *European cooperation network on elections*[10], Member States have discussed a wide array of issues relating to electoral integrity, including the work they are doing in the area of countering disinformation in the run up to the elections. They have also had the opportunity to exchange with colleagues from the Rapid Alert System, the European Parliament and civil society organisations on this topic.

Finally, in order to achieve better situational awareness for the EU and its Member States the EU is also engaging within multilateral fora. The G7 Rapid Response Mechanism has been mandated to strengthen G7 coordination to identify and respond to diverse and evolving threats to G7 democracies, including through sharing information and analysis, and identifying opportunities for coordinated response.

Centre of Excellence for Countering Hybrid Threats

The Helsinki based European Centre of Excellence for Countering Hybrid Threats has reached its full operational capacity. The Centre has made impressive progress with a growing membership, consensus approved work programme and a fully functioning budget. It already has 22 members from both the EU Member States and NATO Allies and further countries are expected to join. The Centre continues to provide support in key areas such as training and exercising through dedicated educational events, including seminars, workshops and conferences. In September 2018, it facilitated a scenario-based discussion at a joint meeting of the Political and Security Committee and the North Atlantic Council, which was broadly appreciated. Other examples of the Centre's activities are listed in the dedicated annex to the present report.

The Commission is working closely with the Hybrid Centre of Excellence to develop a conceptual model for the analysis of hybrid threats. The model integrates all relevant parameters, such as actors, tools, domains and timeline, with a view to providing an extensive

[8] https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.
[9] https://ec.europa.eu/commission/news/code-practice-against-disinformation-2019-jan-29_en.
[10] Established pursuant to Commission's Recommendation of 12 September 2018, C (2018) 5949 final.

landscape of hybrid threats and thereby, helping experts to adequately assess crisis incidents and to design counter-measures. The draft model was presented to the Friends of Presidency Group on Countering Hybrid Threats in March 2019 and was subject to peer review by the relevant experts and practitioners from the EU institutions, Member States and academia in the beginning of May 2019. The final product, expected to be released in June 2019, has been designed as a flexible tool, which can be tailored for use by Member States according to the specific issues and circumstances they face.

Based on an exchange of letters, in July 2018, the European Defence Agency (EDA) and the Hybrid Centre of Excellence agreed to work together 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 successful jointly organised workshop on harbour protection in May 2018, the European Defence Agency and the Hybrid Centre of Excellence continue exploring further avenues of cooperation in the area of maritime. The European Defence Agency is also taking forward its work on defence capability development with regards to countering mini-drones, also taking into account the two workshops organised by the Hybrid Centre of Excellence, to which it contributed.

Protection of critical infrastructure

The Commission, in cooperation with Member States, has finalised the work on developing vulnerability indicators for the resilience and protection of critical infrastructure against hybrid threats. The report also covers other related areas, such as societal and media vulnerabilities, which are pertinent to hybrid threats. The manual of indicators was adopted in November 2018 and put at the disposal of Member States *via* the dedicated Critical Infrastructure Information and Warning Network (CIWIN) document repository. Proposed follow-up actions include the engagement of Member States in practical exercises to further test the concept and identify vulnerabilities, gaps and areas for improvement, as well as further work on the areas of detection of a hybrid campaign/attack and attribution of the relevant activities.

Under the call *Protecting the infrastructure of Europe and the people in the European smart cities* of Horizon 2020, the Commission allocates around EUR 7-8 million per project to address both physical and cyber threats to critical infrastructure. In addition, for 2019, an amount of approximately EUR 8 million per project has been foreseen to address security for smart and safe cities, including for public spaces.

Screening of foreign direct investments

In March 2019, the EU adopted *Regulation (EU) No 2019/452*[11] setting up a framework for the screening of investments from non-EU countries that may affect security or public order. Accordingly, by October 2020, a co-operation mechanism (between the Members States and the Commission) will be established to exchange information and to issue comments in relation to foreign direct investment. The new legislation will contribute to strengthening the overall intelligence on foreign direct investment across the EU and consequently, to improving resilience mechanisms against hybrid threats, *inter alia* in the area broadly regarded as critical infrastructure protection and beyond. In their assessments of effects

[11] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (OJ L 791 of 21/03/2019, p.1).

created by a foreign direct investment, Member States and the Commission will examine effects on *inter alia* critical infrastructures (physical or virtual) including energy, transport, water, health, communications, media, data processing or storage, aerospace, defence, electoral or financial infrastructure, and sensitive facilities, as well as land and real estate crucial for the use of such infrastructure; critical technologies and dual use items, including artificial intelligence, robotics, semiconductors, cybersecurity, aerospace, defence, energy storage, quantum and nuclear technologies as well as nanotechnologies and biotechnologies; etc.

Under the framework of foreign direct investments screening, the Commission will also assess - on grounds of security or public order – foreign direct investment's effects on projects and programmes of EU interest, such as the European Global Navigation Satellite System (GNSS) programmes (Galileo and European Geostationary Navigation Overlay Service (EGNOS)), Copernicus, Horizon 2020, Trans-European Networks for Transport, for Energy (TEN-T and TEN-E) and for Telecommunications, European Defence Industry Development Programme (EDIDP) as well as Permanent Structured Cooperation (PESCO).

Security of energy supply and energy infrastructure

The Commission continues close engagement with Member States and third countries on efforts to diversify energy sources, for example by progressing on the geographical supply diversification *via* greater engagement with the United States on Liquefied Natural Gas (LNG) imports to the EU, as well as unlocking the potential of priority projects such as the Southern Gas Corridor and the development of East Med Gas. In addition, the European Parliament and the Council reached in November 2018 an agreement on the Commission's *Proposal for Regulation on risk-preparedness in the electricity sector*[12] as part of the *Clean Energy For All Europeans Package*[13]. Once the *Risk-Preparedness Regulation* enters into force, it will ensure that all Member States put in place appropriate tools to prevent, prepare for and manage electricity crisis on the basis of an assessment of risks and in cooperation with each other. As a first step, a methodology will be developed by the European Network of Transmission System Operators for Electricity (ENTSO-E) and the Agency for the Cooperation of Energy Regulators (ACER) to identify the relevant risks, including consequential hazards such as the consequences of malicious attacks or fuel shortages. Based on the identified risks, each Member State will have to establish a risk preparedness plan that should include, among others, risks stemming from cyber-attacks.

The Commission has been also actively supporting Member States in the implementation of *Regulation (EU) 2017/1938*[14] concerning measures to safeguard the security of gas supplies. In line with *Regulation 2017/1938*, Member States carry out assessments of all risks at the national and regional levels, relevant for the security of gas supplies, including political, technological, commercial, social and natural risks, such as related for instance to cyber-attacks, sabotage and terrorism. On this basis, Member States prepare preventive action plans and emergency plans to ensure the maximum preparedness to avoid disruption of gas supply or mitigate its effects.

[12] COM (2016) 862 final.
[13] https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/clean-energy-all-europeans.
[14] OJ L280/1 of 28.10.2017.

In the area of nuclear infrastructure, the Commission is monitoring the effective transposition and implementation by the Member States of the Euratom nuclear safety legal framework[15]. This includes monitoring - through the European Nuclear Safety Regulators Group - of the implementation of the outstanding safety improvements resulting from the EU stress tests, conducted following the Fukushima accident. The Commission will also follow up on the implementation by the participating countries of the recommendations of the topical peer review on the ageing of nuclear power plants and research reactors conducted in 2017-2018.

Recent projects addressing threats to energy networks and funded under Horizon 2020 Security research are DEFENDER dealing with the protection of critical energy infrastructure and SECUREGAS addressing the security of the European gas networks.

In the defence sector, the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS II) will further explore how to enable reducing the energy footprint and dependence on fossil fuels, through the implementation of energy efficiency and renewable energy production technologies, and policy and behavioural interventions. The European Defence Agency has also launched research projects such as the Smart Camps Technical Demonstrator and Smart Blue Water Camps. With regard to the project on Total Energy and Environment Military Capability Assessment Framework, the sustainable defence concept has been released to the Member States' authorities, with a view to completing the final product in mid-June 2019.

Transport and supply chain security

For all areas of transport, namely civil aviation, maritime transport and land transport, the Commission (together with the relevant agencies[16]) has continued discussions at different fora including expert groups, workshops and meetings with Member States, industry and other stakeholders on emerging security threats of a hybrid nature, to gain knowledge and learn from experiences.

As far as the aviation sector is concerned, the Commission carries out regular monitoring of emerging threats, including hybrid threats, to adapt the aviation security baseline. On overflight of conflict zones, the Commission continues to facilitate the sharing of information between Member States and to carry out specific risk assessments. The European Aviation Safety Agency (EASA), with the support of a network of national contact points, regularly issues recommendations on conflict zones *via* the *Conflict Zones Bulletin*[17]. In addition, the European Defence Agency continues work on identifying risks and increasing resilience with regard to jamming and spoofing in the aviation domain, including for remotely piloted aircraft systems, in coordination with civil aviation authorities.

The European Aviation Crisis Coordination Cell (ECCC) has been reconfirmed through *Regulation (EU) 2019/123 on the implementation of Air Traffic Network Functions*[18]. The

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

[16] European Aviation Safety Agency (EASA), European Maritime Safety Agency (EMSA), European Railway Agency (ERA).

[17] https://www.easa.europa.eu/easa-and-you/air-operations/czibs.

[18] Commission Implementing Regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions, OJ L 28, 31.1.2019, p.1.

Cell is a permanent body in charge of the management of aviation network crisis, including security incidents and cyber-attacks. It is operated by a network manager, who coordinates the responses to the network crisis, involving close cooperation with corresponding structures in the Member States.

With the aim to ensure that the policy response remains fit for current and future challenges in the maritime domain, including the response to hybrid threats, the Commission services in close cooperation with the European External Action Service and Member States, have revised the *EU Maritime Security Strategy Action Plan*[19] (EU MSS AP). In this context, the Commission continues analyse and follow trends in maritime security – covering also piracy and maritime disputes – that could disrupt shipping and trade routes and consequently affect the EU's interests. Hybrid developments, incidents or attacks on the existing and future maritime trans-oceanic trade routes would have significant disruptive effects on the value and supply chains in Europe. The revised Action Plan, adopted in June 2018, takes a step forward in enhancing awareness and management of risks in the maritime domain, including those concerning transport critical infrastructure. In particular, it endorses the enhancement of maritime awareness through improved information exchange across sectors and across borders, as a key feature in addressing maritime challenges, including through the operational implementation of the Common Information Sharing Environment (CISE) and consolidation of existing mandatory EU systems and voluntary networks. It also highlights the importance of further enhancing the inter-agency cooperation on coast guard functions, between the European Fisheries Control Agency (EFCA), the European Maritime Safety Agency (EMSA) and the European Border and Coast Guard Agency (EBCGA/Frontex), to increase maritime awareness, including through the support provided to national authorities. In the context of the Common Information Sharing Environment, the European Defence Agency, in close cooperation with the defence community, continues to support the development of maritime surveillance capabilities. A new reporting tool for the implementation of the *EU Maritime Security Strategy Action Plan* has been made available to EU institutions and national authorities in order to facilitate a constant progress reporting on actions contributing to implementation. This tool will also allow for increasing coordination and awareness concerning the response to hybrid threats, in particular those affecting transport critical infrastructures.

Other transport-related topics and emerging threats are closely followed, for instance in the context of foreign direct investments to port infrastructure, jamming and spoofing of the Global Positioning System/Galileo and satellites, sea lines of communication and shipping as well as the latest developments in the High North/Arctic. In addition, the Commission services and relevant agencies are actively working on the current and future deployment of drones and its security implications.

Threats to transport critical infrastructure are also addressed in Horizon 2020 security research projects, such as for instance SAURON (started in 2017), dealing with maritime port infrastructure and SATIE (expected to start soon), focussing on the security of airports.

Advanced security measures at EU external borders contribute to increased supply chain security. The new system of upgraded cargo information serves early detection of serious security and safety risks and ensures that the appropriate authorities are in a position to take countermeasures, such as preventing loading of the cargo, and to control action immediately.

[19] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/2018-06-26-eumss-revised-action-plan_en.pdf.

This is part of a strategy and an action plan for customs risk management adopted by the Commission in 2014. A second progress report on the implementation of this strategy was adopted and published by the Commission in July 2018.[20]

In the context of Chemical, Biological, Radiological and Nuclear related risks, the Commission has completed a comprehensive one-year (from March 2018 to March 2019) training campaign at the Joint Research Centre's facility in Karlsruhe on radiation and nuclear detection techniques, trends and new challenges, with the participation of 60 customs experts from 22 Member States. In addition, an e-learning training module for customs officers is currently being developed and planned to be ready by the summer 2019.

Space

In relation to countering hybrid threats, the space domain has two distinctive dimensions: i) protection of space infrastructure (both ground and space segments) as critical infrastructure that could be targeted by hybrid actors, ii) space-enabled services can be used as instruments to counter hybrid threats. The latter is most relevant for Galileo timing services, Governmental Satellite Communications (GOVSATCOM) and Copernicus.

As announced in its 2018 Work Programme[21], the Commission launched preparatory work in view of a possible initiative on the use of Galileo in critical infrastructure that depends on satellite navigation for timing and synchronisation (energy, telecommunications and bank/finance transaction networks), making them less dependent on non-European satellite navigation systems.

Secure satellite communication is a cross-cutting capability in countering hybrid threats and the provision of GOVSATCOM services to Union and Member State authorities managing security critical missions and infrastructures will strengthen the ability to exchange sensitive information in a hybrid threats environment across the EU. A preparatory action of EUR 10 million is implemented in 2019-2020 to prepare and demonstrate key aspects of GOVSATCOM, such as a central GOVSATCOM Hub which will connect users with provider of satellite communication[22]. GOVSATCOM is included in the Commission proposal for an *EU Space Programme*[23] starting from 2021. In addition, a project funded under Horizon 2020 and coordinated by the Global Navigation Satellite System Agency (GSA) will start in 2019 to bring together all different users of GOVSATCOM in Member States and the relevant EU agencies[24]. Further, Member States participating in the European Defence Agency have reached agreement on the project arrangement for the GOVSATCOM Pooling and Sharing Demonstration Project, for which the execution phase started in January 2019 and entails starting service provision and first assessment of the governance structure, the operating procedures and the service delivery mechanism.

---

[20] COM (2018) 549 final.

[21] COM (2017) 650 final.

[22] In addition, the Commission's Joint Research Centre contributes through identification of gaps requiring specific research and development actions in the next Multiannual Financial Framework and supports testing, evaluation and certification of GOVSATCOM user terminals.

[23] Proposal for a Regulation establishing the space programme of the Union and the European Union Agency for the Space Programme, COM (2018) 447 final.

[24] 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) and European Fisheries Control Agency (EFCA).

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[25] 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 attack against Galileo system taking into account hybrid threat scenarios with the close support of the EU Hybrid Fusion Cell.

Given that all components of the forthcoming *EU Space Programme* (Copernicus, Galileo, GOVSATCOM, Space Situational Awareness) are critical, in parallel to the Commission's proposal for the *EU 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 the Council Decision 2014/496/CFSP to the whole *EU 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 disinformation. Indeed the EU Satellite Centre (SatCen) provides to the EU Hybrid Fusion Cell fast and flexible satellite imagery services, together with its value added interpretation that allows faster, better and more accurate responses in its identification of facts, interpretation of matters and development of foresight to counter hostile communication campaigns.

Moreover, SatCen'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

In the context of increasing the EU's defence capabilities, by strengthening the European defence technological and industrial base, significant progress has been made on the establishment of the European Defence Fund (EDF). In February 2019, the Council and the European Parliament reached a partial agreement on the Proposal for regulation establishing the European Defence Fund for the 2021-2027 Multiannual Financial Framework[26]. In addition, both pilot programmes to the European Defence Fund within the current Multiannual Financial Framework, i.e. the Preparatory Action on Defence Research (PADR) and the European Defence Industrial Development Programme (EDIDP), are already operational. The third and last, Preparatory Action on Defence Research work programme and the European Defence Industrial Development Programme biannual work programme were

[25] Council Decision 2014/496/CFSP of 22 July 2014 on aspects of the deployment, operation and use of the European Global Navigation Satellite System affecting the security of the European Union and repealing Joint Action 2004/552/CFSP, OJ L 219, 25.7.2014, p. 53.
[26] COM (2018) 476 final.

adopted in March 2019. All related calls for proposals for 2019 have been published[27] and will be open until the end of August 2019. Relevant research and capabilities development projects to strengthen resilience against hybrid threats might be eligible under those funding opportunities. For instance, the work programme of the European Defence Industrial Development Programme for the years 2019 and 2020 contains calls in the domains linked to the hybrid dimension, such as cyber, harbour protection as well as cross-domain capabilities.

The implementation of Permanent Structured Cooperation (PESCO) also contributes to the efforts in 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 framework of the Permanent Structured Cooperation.

With a view to refine the link between research, industrial capability development and technology, including the hybrid threats dimension, work is currently ongoing in the European Defence Agency, together with Member States, to develop Strategic Context Cases, which will be used to support the implementation of 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 cooperation for the short-, mid- and long-term perspective. The Strategic Context Cases will be presented for endorsement by Member States at the European Defence Agency's Steering Board in the Capability Directors' composition on 27 June 2019. The Strategic Context Cases also indicate the link to the High Impact Capability Goals which 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 on Security and Defence.

Protecting public health and food security

The Health Security Committee continued exchanging lessons learned with regards to health sector preparedness for terrorism, including psychological support, emergency planning and coordination mechanisms.

In the June 2018 report on the Chimera exercise[28], a number of important recommendations have been made, for instance to develop common guidelines across the EU and national legislation in relation to hybrid threats; to identify a single-platform for sharing information on hybrid threats; to more broadly share information with third countries; to consider how classified information is used and shared with member states during ongoing terrorism investigations; to develop cyber-attacks preparedness plans for hospitals; where appropriate, to link or integrate rapid alerting and crisis response tools; to improve clinical data sharing at the EU and Member State level. In addition, regular training should be held to improve inter-sectoral crisis management, raise awareness of existing tools and procedures, raise awareness of hybrid threats (especially incorporating cyber-security and bio-terrorism) and how they differ from other threats and share best practice.

In April 2019, in cooperation with the US Federal Bureau of Investigation (FBI) and the US Centres for Disease Control and Prevention (CDC), the Commission organised a workshop in Brussels on joint criminal-epidemiological investigations, with participation of representatives

[27] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home.

[28] https://ec.europa.eu/health/sites/health/files/preparedness_response/docs/2018_hybridthreatsexercise en.pdf.

from the law enforcement community and the public health sector from 22 Member States, as well as the European Centre for Disease Prevention and Control (ECDC) and Europol. The workshop covered *inter alia* an overview of biological agents (bacteria, viruses, and toxins) and their use as weapons as well as an exercise focusing on a biological attack on a large mass-gathering event.

The ongoing Horizon 2020 security research project SAFECARE (started in 2018) addresses threats to health infrastructure with the aim to improving physical and cyber security of hospitals.

Moreover, the EU civil protection mechanism has been recently strengthened by means of amendment to the *Decision 1313/2013/EU on a Union Civil Protection Mechanism*[29]. Accordingly, the EU will step up disaster prevention and preparedness and strengthen its response capacities. As the first step towards the implementation of this policy, the Commission has set up specialised task teams to start working towards the identification, definition and the development of rescEU capacities, including medical and Chemical, Biological, Radiological and Nuclear capacities.

Finally, in February 2019, the Commission participated in a workshop on EU-North Atlantic Treaty Organisation cooperation in civil protection, with a scenario-based discussion on the respective requirements and methods for civil protection in case of an epidemic.

Chemical, Biological, Radiological and Nuclear related risks

In the context of implementation of the *CBRN Action Plan*[30], the Commission, in cooperation with a number of Member States, developed a classified list of more than 20 chemical substances of concern. The list has been compared with similar lists of some international organisations and key international partners and has taken into account factors such as accessibility of precursors, ease of production and applicability in different environments. The list is now the basis for discussions both with Member States and with some 20 detection equipment manufacturers on capabilities to detect these chemicals and on possibilities to enhance the equipment performance with a view to looking into possible voluntary standards in non-aviation areas. In parallel, discussions have been held with the chemical supply chain on how to reduce accessibility of those substances.

The Commission has also finalised the work on a gap analysis on detection of Chemical, Biological, Radiological and Nuclear materials and agents. The (classified) report was sent to Member States in June 2018. The last part of the gap analysis was a cross-border exercise Quinteto+ held in March 2019 involving six Member States. The aim of the exercise was to test the international and cross-border information exchange and police agencies reaction to - in this case - chemical and radiological terrorist threats.

The Commission has also continued to engage with private actors in the supply chain to work together towards addressing evolving threats from chemicals that can be used as precursors. In February 2019, the Commission organised a meeting with online platforms (Amazon, eBay, Facebook, PaylPal, Rakuten and Alibaba) in order to discuss how they could work towards detecting suspicious transactions and reducing accessibility of illegal and/or hazardous substances on their platforms, including chemicals that can be used as precursors.

---

[29] Decision (EU) 2019/420 of the European Parliament and of the Council of 13 March 2019 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism, OJ L 77, 20.3.2019, p. 1, entry into force on 21 March 2019.

[30] COM (2017) 610 final.

The Chemical, Biological, Radiological and Nuclear cluster topic under the Security call of the Work Programme 2018-2020 of Horizon 2020, provides up to EUR 3.5 million in 2019 for projects to be led by a small and medium sized enterprise (SME) and aiming at research and development of novel Chemical, Biological, Radiological and Nuclear technologies.

The Commission is preparing a new joint action with Member States under the *EU Health Programme*[31] to strengthen health preparedness and response to biological and chemical terror attacks, including cross-sectoral collaboration with the security and civil protection sectors and with reference to hybrid attacks. The joint action will address laboratory and treatment capacities and medical countermeasures and is scheduled to commence in the first quarter of 2020. Furthermore, 15 Member States signed a joint procurement framework contract for pandemic influenza vaccine. The Commission is also working with the Health Security Committee and the Preparedness Working Group to define and implement procedures for sharing medical countermeasures through an early warning and response system.

Within the framework of the European Medical Corps, the Commission, in collaboration with the European Burns Association, has developed a European Response Plan for Mass Burn Casualty Disasters, focusing on activities linked to activating the Union Civil Protection Mechanism and on ensuring the best possible conditions for the treatment of patients who are evacuated. The measure identifies key stakeholders in cases where a European response to a mass burn casualty disaster is needed, as well as the core principles on which such a response is based, going into detail on how the response is triggered. In April 2019, the Commission published a call for tender for the design and organisation of a pilot training course for the burns assessment team members.

In October 2018, the Council of the European Union established an autonomous sanctions regime against the use of chemical weapons[32]. In January 2019, ten entries consisting of nine natural persons and one entity were added to the list of natural and legal persons, entities and bodies subject to travel bans, assets freeze and the prohibition to make funds available to them.

In April 2019, the Council adopted a decision[33] to support core activities of the Organisation for the Prohibition of Chemical Weapons, providing EUR 11.6 million funding for the years 2019-2022 to fight against impunity and re-emergence of chemical weapons use, capacity building as well as upgrading of the Organisation's laboratory to a Centre of Chemistry and Technology, with increased capacity to verify chemical substances, research and contribute to capacity building.

Preparation is under way for the Commission to launch a study to assess the implementation by the Member States of radioactive source control measures[34], in particular record keeping and security of high-activity sources.

At the international level, the Commission services, in close consultation with the European External Action Service, have been implementing the Chemical, Biological, Radiological and Nuclear (CBRN) risk mitigation Centres of Excellence initiative, which operates in eight

[31] https://ec.europa.eu/health/funding/programme_en.

[32] Council Decision (CFSP) 2018/1544 and Council Regulation (EU) 2018/1542 of 15 October 2018 concerning restrictive measures against the proliferation and use of chemical weapons.

[33] Council Decision Common Foreign and Security Policy 2019/538 of 1 April 2019.

[34] Council Directive 2013/59/Euratom of 5 December 2013 laying down basic safety standards for protection against the dangers arising from exposure to ionising radiation, OJ L 13, 17.1.2014, p. 1.

regional centres and 61 partner countries outside the EU. Within its network of more than 1000 governmental officials, national and regional action plans are being established on the basis of needs and risk assessments, and in close cooperation with existing international and regional organisations or conventions like: the Organisation for Security and Co-operation in Europe (OSCE), the Organisation for the Prohibition of Chemical Weapons (OPCW), the Chemicals Weapons convention (CWC), the Biological Weapons Convention (BWC), the North Atlantic Treaty Organisation, the United Nations Security Council Resolution 1540 expert Committee, the World Health Organisation (WHO) and the International Atomic Energy Agency (IAEA).

National Computer Security Incidents Response Teams and Computer Emergency Response Team for the EU institutions

The focus of the network of national Computer Security Incidents Response Teams (CSIRTs), designated by the Member States, with the Computer Emergency Response Team for the EU institutions (CERT-EU) has been on building trust and confidence between the teams so that swift and effective operational cooperation on cybersecurity takes place. In addition to meetings, there are working groups on tools, standard operating procedures, Computer Security Incidents Response Teams maturity and also incident and threat information. Members exchange information about existing and known threats and incidents on an *ad hoc* basis. The network also takes part in cyber exercises such as the recent Cyber Europe 2018, which addressed various cyber threats in the aviation sector.

The Computer Emergency Response Team for the EU institutions operates a cyber-threat intelligence fusion cell that monitors a large variety of open and close sources. In case of hybrid threat with a cyber-dimension, the Team produces flash threat assessment memos. Memos are distributed to EU institutions, bodies and agencies, and in some cases to partners like the national Computer Security Incidents Response Teams and the Computer Incident Response Capability (NCIRC) of the North Atlantic Treaty Organisation. In terms of topics, the memos have included cyber-aspects of election interference, cyber-threat to the transportation (aviation), energy, finance or digital sectors.

Cybersecurity related legislation

In the context of implementation of the *Network and Information Security Directive*[35], the Cooperation Group serves as a forum for strategic cooperation, helping Member States to share experiences related to the implementation of the Directive and discuss cybersecurity issues beyond it. The Cooperation Group works on a horizontal basis focusing on cross-sectorial capabilities to pool information and expertise, including thematic work streams, for instance with focus on the so-called *Blueprint Recommendation*[36].

In September 2018, the Commission adopted a *Proposal for Regulation to establish the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*,[37] with a view to stimulating development and deployment of cybersecurity solutions. The legislative procedure is ongoing.

---

[35] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1.

[36] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, OJ L 239, 19.9.2017, p. 26.

[37] COM/2018/630 final.

Finally, a *Cybersecurity Act*[38] was adopted on 17 April 2019, thereby strengthening and modernising the European Union Network and Information Security Agency (ENISA) and putting in place an EU certification framework for information and communications technology (ICT) products and services.

Contractual Public Private Partnership (cPPP) for cybersecurity

The public-private partnership on cybersecurity with the European Cybersecurity Organisation (ECSO) includes more than 250 contributing members from private and public sectors and has developed research and innovation priorities for 2017-2020. Until now, the European Cybersecurity Organisation has complied with Contractual Public Private Partnership commitments for what concerns leveraging the investment factor above the defined target. The partnership with the European Cybersecurity Organisation will end in 2020, but – building on this Contractual Public Private Partnership - the Commission has invested more than EUR 63.5 million in four pilot projects (CONCORDIA, ECHO, SPARTA and CyberSec4Europe) under Horizon 2020 to lay the groundwork for building the expertise ahead of the future European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. The four pilots, involving more than 160 partners, including large companies, small and medium enterprises, universities and cybersecurity research institutes from 26 Member States, will also contribute to a common European Cybersecurity Research and Innovation Roadmap beyond 2020 and a European cybersecurity strategy for industry.

In addition, the Commission also launched in 2019 a full-scale pilot for the definition and testing within a European scheme for cybersecurity certification of Industrial Automation Control System Components (IACS).

Cybersecurity in the transport sector

For different transport modes (aviation, maritime and land transport), 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 Directive*. One example of a recent event was the First Cybersecurity in Transport conference, organised by the Commission and the relevant agencies on 23 January 2019.

The European Strategic Coordination Platform on cybersecurity of the European Aviation Safety Agency (EASA) is in charge of the implementation of the roadmap on aviation cybersecurity and the preparation of the EU Cybersecurity Strategy in aviation. It also proposes cybersecurity measures for aviation stakeholders to cover aviation domains with effect on safety. In addition, the Agency is currently developing theEuropean Centre for Cyber Security in Aviation (ECCSA), which is currently in its pilot phase. The Centre shall serve as a platform for information sharing. The Computer Emergency Response Team for the EU institutions (CERT-EU) is providing expertise on cybersecurity and will play the role of trusted third party host for the information sharing infrastructure.

As there is a need for a holistic approach towards cybersecurity, the Commission supports cross-modal non-regulatory actions, such as information sharing, cyber skills and cyber hygiene, through measures such as for instance a cybersecurity toolkit. It aims at strengthening cyber awareness of staff in the transport sector and providing them with basic

[38] COM (2017)477.

principles of cyber hygiene. This project is expected to be launched the second half of 2019 and will last for approximately 12 months.

The Commission is working on transposition of the new International Civil Aviation Organisation (ICAO) cybersecurity standard[39] representing cybersecurity preventive measures to the *Aviation Security Implementing Regulation*[40].

In June 2018 as well as in spring 2019, the European Defence Agency organised specific cyber seminars bringing together stakeholders from the civilian and military aviation sector to achieve a common understanding of current and future challenges emerging from the modernisation of the air traffic management system.

In the maritime transport sector, shipping industry guidelines on cybersecurity were adopted at the level of the International Maritime Organisation (IMO) with a view of advancing towards a potential regulatory outcome.

In the maritime area, priority has been put on strengthening the cybersecurity on important platforms, through new technology, education and training, in order to make IT systems interoperable and serve as guidelines for future capability development. The revised *EU Maritime Security Strategy Action Plan* has created a framework for relevant agencies, Member States and social partners to organise cross-sectoral maritime security training, educational activities, and exercises, also involving law enforcement and military personnel, focusing on Chemical, Biological, Radiological and Nuclear threats, cybersecurity and protection of critical maritime infrastructure. Implementation of *EU Maritime Security Strategy Action Plan* concerning preparedness and response to hybrid threats, in particular to cyber attacks across the transport sector in ongoing.

Finally, the Commission is exploring ways to involve representatives of the transport sector (primarily competent authorities for the implementation of the *Network and Information Security Directive*) in a sectorial work stream of the Directive's Cooperation Group.

Cybersecurity in the energy sector

In April 2019, the Commission adopted a sector-specific guidance in the form of a *Recommendation on cybersecurity in the energy sector*[41] that identifies the main actions to be taken by the Member States and energy operators in order to preserve cybersecurity and be prepared for possible cyber attacks in the energy sector. This should be read in the context of the *Network and Information Security Directive ("NIS Directive")*[42] and addresses the characteristics of the energy sector, notably real-time requirements, the risk of cascading effects and the combination of legacy systems with new technologies.

---

[39] International Civil Aviation Organisation's Standard 4.9.1 of Annex 17 to Chicago Convention. The new standards entered into force in November 2018.

[40] Commission Implementing Regulation (EU) 2019/103 of 23 January 2019 amending Implementing Regulation (EU) 2015/1998 as regards clarification, harmonisation and simplification as well as strengthening of certain specific aviation security measures (Text with EEA relevance.) C/2019/136, OJ L 21, 24.1.2019, p. 13.

[41] C (2019) 240 final, accompanied by a Staff Working Document, SWD (2019) 1240 final, with the policy framework and additional technical explanations.

[42] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1.

The European Parliament and the Council have empowered the Commission (*Electricity Regulation*[43]) to establish a network code on cybersecurity with the relevant associations of electricity network operators and with the respective regulators at the EU level. Preparatory work in a dedicated expert group has been ongoing since 2017.

Since cooperation and trust among stakeholders and among Member States is key when it comes to cybersecurity, due to the potential cascading and cross-border effects of energy, the Commission is working to raise awareness and to promote broad discussions in the energy sector. To that end, in June 2018, the Commission initiated a dedicated work stream on energy within the Cooperation Group established under the *Network and Information Security Directive*, with the aim of exchanging best practices and sharing experience in identifying, mitigating and managing cyber risks in the energy sector. In addition, the Commission has organised several events to share information and increase awareness (e.g. a high-level event on cybersecurity in the energy sector in Brussels in October 2018).

Cybersecurity in the financial services sector

With cyber threats emerging as one of the most important risks faced today by the financial sector, financial supervisors as well as international fora (in particular G7, the Basel Committee on Banking Supervision, the Financial Stability Board and the Committee on Payments and Market Infrastructures) have been exploring, within different work streams, solutions to better integrate cybersecurity into the financial services policy and regulatory landscape.

In the context of the 2018 *FinTech Action Plan*[44], the Commission identified several areas and aspects where stronger cyber resilience and enhanced information and communications technology (ICT) security of the financial market participants across the Union would contribute to strengthening the stability of the EU highly integrated financial sector.

Building on the Joint Technical Advices published in April 2019 by the three European Supervisory Authorities in the financial sector (the European Banking Authority, the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority), the Commission is reflecting on ways to address the current fragmentation in relation to the scope, granularity and specificity of cyber security-related provisions across the Union financial services legislation.

On the angle of enabling measures for the prevention of cyber threats, in June 2018, the Commission organised a public-private workshop aimed at assessing the existence and extent of any possible regulatory or non-regulatory barrier preventing threat-intelligence sharing. The discussions did not point to clear barriers preventing the flow of threat-related information among financial market participants although further clarification has been sought by the stakeholders.

Based on the outcome of the workshop, the Commission is now an active observer in the European Central Bank's 'European Cyber Resilience Board for pan-European financial infrastructures' (ECRB) sub-working group on information sharing arrangements. This forum gathers private sector participants and authorities (at EU and national level) working on information sharing arrangements, in particular to develop the building blocks that would

[43] Regulation of the European Parliament and the Council on the internal market for electricity (recast), not yet published in the Official Journal.
[44] COM/2018/0109 final.

enable a trusted network for information sharing among pan-European financial infrastructures. Once the building blocks agreed, European Cyber Resilience Board members are expected to take swift steps to make them operational.

Cyber defence

A Memorandum of Understanding signed between the European Union Agency for Network and Information Security (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 May 2018 has strengthened cooperation and synergies between these organisations in line with their respective mandates and contributed 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 are expected to endorse the Strategic Context Case 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.

With the funding available for the Preparatory Action on Defence Research, research on cyber defence is already performed in OCEAN 2020, a large scale demonstrator project with EUR 35 million EU funding. In this project, substantial attention goes to the integration of data from multiple sources in a single pre-defined maritime tactical picture. One of the main challenges with data integration that is addressed is the rapid switching between classified and unclassified channels with cyber issues. 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 10 million to fund one project. This project, which should start in the first half of 2019, will look at the hardware side of cyber defence technologies to protect the system architecture from intrusion or attacks.

Furthermore, the work programme for the years 2019 and 2020 of the European Defence Industrial Development Programme includes two calls addressing topics related to cyber situational awareness and defence capabilities, defence networks and technologies for secure communication and information sharing.

The Cyber Education, Training, Exercises and Evaluation (ETEE) platform, established in 2018 with the aim to addressing cyber security and defence education and training among the civilian and military personnel, is expected to reach its full operational capability in July 2019. Based on a questionnaire addressed to the Member States, a need to train around 1,500 officials yearly has been identified for a high demand scenario. The platform offers training for all Common Security and Defence Policy training levels as identified by the EU Military and Civilian Training Groups, and thus will significantly upscale training opportunities for the Member States. In line with the updated 2018 EU *Cyber Defence Policy Framework*[45], the

[45] Council's document ST 14413/18.

European Defence Agency will further develop courses in collaboration with the European Security and Defence College to meet the Member States' cyber defence education, training and exercises requirements and support the Cyber Education, Training, Exercises and Evaluation platform *inter alia* through progressively integrating cyber education, training, evaluation and exercises modules developed in the frame of the European Defence Agency.

Gathering electronic evidence

The legislative procedures on the Commission's e-evidence proposals (*Regulation on European production and preservation orders for electronic evidence in criminal matters*[46] and *Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*[47]) are ongoing.

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.

Cyber diplomacy toolbox and cyber sanctions

The *Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities*[48] (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 exercise the effective implementation of these guidelines, including by establishing preparatory practices and communication procedures.

In response to European Council in June 2018 and in October 2018, Member States have been working on coordinated attribution of malicious cyber activities at the EU level and strengthening their cooperation with like-minded countries to further deter and respond to malicious cyber activities.

On 12 April 2019, the High Representative published a declaration on behalf of the EU stressing the need to respect the rules-based order in cyberspace, urging actors to stop undertaking malicious cyber activities including the theft of intellectual property, and calling on all partners to strengthen international cooperation to promote security and stability in cyberspace.

Finally, following a joint proposal by the Commission and the High Representative, 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 which constitute an external threat to the EU or its Member States, including cyber-attacks against third States or international

[46] COM(2018) 225 final.
[47] COM(2018) 226 final.
[48] Council's document 9916/17.

organisations where restrictive measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy[49].

International cooperation in cybersecurity

The EU has specific cyber dialogues with the United States, Japan, Brazil, India, South Korea and China. Close consultations with international organizations, such as the North Atlantic Treaty Organisation, the Association of Southeast Asian Nations Regional Forum, the Organisation for Security and Cooperation in Europe, the Council of Europe, and the Organisation for Economic Co-operation and Development are also in place.

Furthermore, the European Union and the Member States engage in the United Nations' two specific processes: an open-ended working group in the context of the developments in the field of information and telecommunications in the context of international security; and a new Group of Governmental Experts to advance responsible State behaviour in cyberspace in the context of international security.

In addition, the Commission has engaged, through the Instrument contributing to Stability and Peace (IcSP), into enhancing stability in Ukraine by reinforcing cybersecurity in elections. The project started in January 2019 for a period of 12 months and contributed to strengthen the capacity of a number of crucial participants of the electoral process in Ukraine by providing cyber hygiene training and technical cybersecurity exercises to decision makers and IT specialists. In addition, the action will foster the exchange of best practices in the area by supporting study visits and peer exchange between the Ukrainian and selected EU Member States' electoral and cyber experts and administrators. Furthermore, to add to the integrity of the election process and maintain public confidence in the electoral process, a post-electoral audit is being undertaken in relation to cyber security and will be complemented by a set of activities targeting disinformation campaigns in cyber space. Besides, in a separate action, the EU assessed the Ukrainian cybersecurity crisis management system and provided recommendations for the improvement of the cybersecurity of elections.

A new EU-funded project aiming at improving cyber resilience in the Eastern Partnership countries was approved in 2019. The programme has two components: cybersecurity and cybercrime. Its objective is to contribute to improving the cyber resilience and criminal justice response of Eastern Partnership countries, by focusing on (1) the development of technical and cooperation mechanisms that increase cybersecurity and preparedness against cyber-attacks, such as strengthening the institutional governance and legal framework, developing the critical information infrastructure structure, and increasing the incident management capacities, and (2) the full implementation of an effective framework to combat cybercrime, including: substantive and procedural criminal legislation; law enforcement and judicial authorities' capacity to investigate, prosecute and adjudicate cases of cybercrime; measures to enable international cooperation; and cooperation between public authorities and private entities.

Further, the Commission has been leading on international cyber capacity (cyber resilience and cybercrime) building links with development cooperation funds. This has translated in two ongoing projects with global reach: Cyber for Development (Cyber4Dev) and Global Action on Cybercrime extended (GLACY+) aiming to strengthen the capacities of countries

[49] 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.

worldwide to increase operational capacities to adequately prevent, respond to and address cyber security incidents and to apply legislation on cybercrime and electronic evidence as well as effective international cooperation in this area. Moreover, in line with June 2018 Council Conclusions, a new action has been tendered to create an EU External Cyber Capacity Building Network aiming at mobilising collective Member States' expertise and supporting effective coordination for EU-funded external cyber capacity building programmes as well as increasing training opportunities in light of proliferating initiatives in partner countries.

Further activities have been undertaken on international cooperation in cybersecurity of financial transactions (e.g. through existing legal instruments, such as the Budapest Convention[50] and existing platforms) and in aviation and maritime transport security (for instance, a project to be launched in the third quarter of 2019 on aviation security covering Africa, Middle East and Asia and including a component on cyber-related risks.

Targeting hybrid threat financing

Since July 2018, the EU has strengthened its anti-money laundering and counterterrorism financing legal framework, in line with the 2016 Action Plan[51]. This includes implementation of the revised *5th Anti-Money Laundering Directive*[52]; new rules facilitating the use of financial and other information; minimum rules concerning the definition of criminal offences and sanctions; safeguards against illicit cash movements; rules to prevent illicit trade in cultural goods. The next step is to ensure the full implementation of the new rules and to consider how to further improve access to and exchange of financial information for counterterrorism purposes.

Building resilience against radicalisation and violent extremism

In September 2018, the Commission adopted a *Proposal for Regulation to prevent the dissemination of terrorist content online*[53]. 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 Council agreed on a general approach in December 2018 and the European Parliament confirmed their first reading position in April 2019. Negotiations between the two co-legislators to agree on a final text are expected to continue after the elections of the European Parliament in the second half of 2019.

The *European Strategic Communications Network*[54] is working on the issue of disinformation and its implications. An analytical paper on how disinformation impacts strategic communications on countering violent extremism has been shared with Member States in July 2018. In more general terms, as a follow-up to the recommendations of the High-Level Expert Group on Radicalisation, the Commission, in collaboration with Member States, is gradually

---

[50] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[51] COM (2016) 50 final.

[52] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) PE/72/2017/REV/1, OJ L 156, 19.6.2018, p. 43–74.

[53] COM (2018) 640 final.

[54] The European Strategic Communications Network (ESCN) is a collaborative network of the Member States, funded by the Commission, which shares analysis, good practice and ideas on the use of strategic communications in countering violent extremism.

setting up an EU cooperation mechanism on the prevention of radicalisation, with a reinforced support and coordination structure within the Commission. Communication and online propaganda is among the key initiatives addressed in the Strategic Orientations 2019 adopted by the Member States' Steering Board, underlining the need to build resilience and promote EU values.

In 2018, EUR 6 million were made available under the Civil Society Empowerment Programme[55] to support 12 campaigns providing alternative narratives to terrorist propaganda and promoting fundamental rights and values. A second call was launched in 2019 for an amount of EUR 4 million.

Also, the Security call of Horizon 2020 will address comprehensive multi-disciplinary and multi-agency approaches to prevent and counter violent radicalisation and terrorism in the EU. DANTE, another project under H2020 has just been finalised and developed methods to detect and analyse terrorist-related online contents and financing activities. Two other projects address similar issues: TENSOR, which will be finished this year, and RED-Alert, which will continue for one more year.

At the international level, the Commission is implementing a range of projects focussing on preventing and countering violent extremism (P/CVE). Through partnerships with e.g. the United Nations, the Hedayah Centre of Excellence on Countering Violent Extremism, the Global Community Engagement and Resilience Fund (GCERF) and more, the Commission is working with partner countries in the Middle East, North Africa, Sahel, Horn of Africa, Western Balkans, and across Asia. With a whole-of-society approach, the aim is to facilitate innovative preventing and countering violent extremism (P/CVE) projects in collaboration with local communities, to strengthen conditions conducive to development, and resilience towards violent extremism.

Prevention and response to threats to elections

The *Election Package*[56], adopted by the Commission on 12 September 2018, encouraged Member States to set up national election networks, involving national authorities with competence for electoral matters and authorities in charge of monitoring and enforcing rules related to online activities relevant to the electoral context. The national election cooperation networks appointed contact points to take part in a European cooperation network for elections. The European cooperation network serves to alert on threats, exchange on best practices among national networks, discuss common solutions to identified challenges and encourage common projects and exercises among national networks. It also supports cooperation with other European level groups and bodies, thereby enabling mutual support and a wider and effective dissemination of relevant alerts and other information. It facilitated participation of its members at a cybersecurity exercise organised in collaboration with European Union Agency for Network and Information Security, and is coordinating closely with the Rapid Alert System. While in the immediate term the focus of the European network are the upcoming 2019 European elections, its broad objective is to support the integrity of elections and electoral processes in the EU in general. Three meetings were held in 2019, with further meetings scheduled later in the year and semi-annual meetings planned from 2020 onwards.

[55] https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/civil-society-empowerment-programme_en.
[56] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights_en.

The 2018 Fundamental Rights Colloquium aimed at reaffirming democracy as a central value common to the European Union and all its Member States, and at looking at how to renew democratic engagement within the European Union and the European societies. The Colloquium included dedicated sessions on the topics of supporting secure electoral process and ensuring fair elections, pluralistic political debate as well as online and offline freedom of expression. High-level national and European policymakers, international organisations, civil society organisations, media and social media representatives, the world of business and education, legal professionals, and many others, exchanged views on how to secure electoral processes from the challenges posed by new threats and safeguard the trust of citizens in elections. The need for urgent action was acknowledged, in particular to address the advances in using digital communication to polarise debate and undermine public trust. A set of conclusions form the event is publicly available on the Colloquium website[57].

Increasing cooperation with partner countries

Hybrid Risk Surveys have been launched in seven partners: Moldova, Georgia, Jordan, Albania, North Macedonia, Kosovo* and Montenegro, with a different degree of maturity. The survey in Moldova is the most advanced one. Following the agreement of the national authorities to a set of recommendations in July 2018, the EU is already providing substantial financial assistance helping Moldova to address these recommendations (e.g. police reform, energy diversification, strategic communications, awareness raising activities on cyber-security and critical infrastructures interconnection).

Replies from Georgia and Jordan to questionnaires launched in 2017 are pending. The four Western Balkan countries have received the questionnaires in January and February 2019. Kosovo has already provided replies, evaluation is ongoing.

EU Playbook and exercises

Following the successful completion of the EU Hybrid Exercise MULTILAYER 18 - EU HEX-ML 18 (PACE), the Final Exercise Report on lessons learned is being drafted and the Final Exercise Report on EU-North Atlantic Treaty Organisation interaction lessons learned has been shared with the Member States for their approval. The latter is also to be shared with the North Atlantic Treaty Organisation.

The work has started at technical level on the new Parallel and Coordinated Exercises concept for the future exercises and a first exchange of views at technical level with the North Atlantic Treaty Organisation is taking place. In parallel, discussions are held to make sure that the timing of the next exercise is properly set avoiding any conflicts or overlaps.

On the basis of the lessons learned from the EU Hybrid Exercise MULTILAYER 18 - EU HEX-ML 18 (PACE), a possible revision of the *EU operational protocol for countering hybrid threats (EU Playbook)*[58] is under consideration.

---

[57] https://ec.europa.eu/info/files/conclusions-colloquium-2018_en.

* This designation is without prejudice to positions on status, and is in line with United Nations Security Council Resolution 1244/1999 and the International Court of Justice Opinion on the Kosovo declaration of independence.

[58] SWD (2016) 227 final.

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

The Centre of Excellence for Countering Hybrid Threats has been asked to analyse the question from an academic point of view. This is work in progress.

Military operations and missions

The *EU Concept for EU-led Military Operations and Missions*[59] sets out fundamental arrangements for leading EU military operations and mission. It is currently undergoing revision *inter alia* to define hybrid threats aspects. The revised concept is expected to be approved in the fourth quarter of 2019.

EU-North Atlantic Treaty Organisation cooperation

Countering hybrid threats remains key area of interaction with the North Atlantic Treaty Organisation. Progress is steady, building upon the momentum established by the 2016 Warsaw Joint Declaration[60] and the 2018 Brussels Joint Declaration[61].

The Parallel and Coordinated Exercises (PACE) are perhaps the most visible example of cooperation. The second iteration took place in November 2018 and was based on a hybrid scenario allowing for a number of meaningful interactions on cybersecurity, disinformation and civil protection as well as by exchanging information at staff-to-staff level with regard to terrorist and criminal/smuggling events.

Cooperation has continued on crisis response and bolstering resilience through cross-participation in exercises, cross-briefings and staff-to-staff dialogue. Notable example of the latter is the staff-to-staff workshop on crisis response mechanisms to support Chemical, Biological, Radiological and Nuclear resilience, which took place in May 2019. The discussion – based on a scenario of a biological attack against a country being both an EU Member State and NATO Ally – allowed to map respective policies, plans and procedures to support resilience as well as the crisis response mechanisms on each side. Staff exchanges also took place regarding the Counter Hybrid Support Teams recently launched by the Alliance 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 the Alliance's Hybrid Analysis Branch on situational awareness, active staff-to-staff interaction between the respective strategic communications teams as well as between hybrid file-holders on partners' capacity building.

Active interaction in the field of cybersecurity and defence has continued across the work strands identified in the Warsaw Joint Declaration. To note a few examples on coordination of cyber training efforts and cross-participation in cyber exercises: North Atlantic Treaty Organisation's staff observed Cyber Europe 2018 and EU staff participated in Cyber Coalition 2018 and the first planning event for Cyber Coalition 2019; in March 2019, the Cybersecurity/ Cyber Defence Course of the European Security and Defence College was opened to the Alliance. The Technical Arrangement on Cyber Defence between the North Atlantic Treaty Organisation Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team for the European Union (CERT-EU) continues to be

[59] Council's document ST 17107/14 dated 19 December 2014.

[60] https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf.

[61] https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf.

implemented in line with existing provisions. In April 2019, in view of the May European Parliament elections, the two held a joint workshop, along with industry experts, to discuss counter-measures to potential threats to devices and systems related to the electoral processes.

The European Defence Agency organised staff-to-staff contacts with the North Atlantic Treaty Organisation, covering harbour protection, countering mini drones and countering improvised explosive devices - areas, which all have a hybrid threats dimension.

CONCLUSION

Against the background of the 2017 and 2018 reports under the Joint Framework and the updates provided in the present one, some key achievements, both on substance and process, can be highlighted, as follows:

The counter-hybrid toolbox has grown to an impressive size. A large number of legislative proposals have been adopted to underpin efforts at national and EU level – the Regulation on the screening of foreign direct investments into the EU is a recent example to the point. Chemical and cyber sanctions regimes have been added to our array of response measures. Countering disinformation, election protection, cybersecurity, defence industry cooperation add on to the list of areas concerned but, by far, do not exhaust it. The challenge is to keep these tracks connected and avoid creating silos.

Work patterns have been transformed, and joined-up approaches are now the norm. Cooperation within and between EU entities – institutions, services and agencies – has been key to steady progress on the hybrid files. The same goes for cooperation with strategic international partners like the North Atlantic Treaty Organisation and third countries in the frame of multilateral formats, notably the G7.

Close coordination between EU entities and the Member States based on a whole-of-society approach – government, civil society, private sector, including, inter alia, media and online platforms – is at the core of our counter-hybrid policies. Responding to threats lies predominantly with Member States as it is intrinsically linked to national security and defence policies. However, the EU institutions provide essential support. Preserving and further reinforcing this fundamental bond would ensure that our counter-hybrid agenda is brought forward and implemented in an efficient and sustained manner.

ANNEX 1

Strategic Communications and the European External Action Service Task Forces

The Strategic Communications Division of the European External Action Service is responsible for designing and leading communications and outreach activities in support to the EU's foreign policy objectives and High Representative's activities. It plays a leading role in tackling disinformation and addressing hybrid threats in particular coming from external sources. With its more strategic and long-term approach to communications, the Division complements the press and media relations work of the Spokespersons' service. As part of the public diplomacy activities of the European External Action Service, the Division develops and implements targeted and tailored communications and outreach actions at the international level, as well as in the EU, to support specific policy initiatives.

The work of the Division is built on five pillars:

1. Building awareness for and better understanding of the EU and its activities among EU internal and external audiences;
2. Supporting fact-based communications among key opinion formers and addressing the issue of disinformation and manipulations of information online;
3. Providing support to EU Delegations and Missions and Operations around the world in their activities to communicate the EU;
4. Supporting policy development with analysis of digital media trends and offering strategic communications advice and training to colleagues;
5. Contributing to internal communications in the European External Action Service and supporting the development of the European External Action Service corporate identity.

As mandated by the *Action Plan against Disinformation*, the Division is strengthening its capacity to better detect, analyse and expose disinformation and raise awareness on the negative impact of disinformation in close cooperation with the Commission, the European Parliament and the Member States. The newly established Rapid Alert System – a cornerstone of the *Action Plan against Disinformation* - is curated and managed by the Division and facilitates sharing of data on disinformation campaigns Member States and EU institutions, enables common situational awareness and facilitates the development of common responses in time and resources efficient way.

Structure, priority areas and resources

The European External Action Service Strategic Communication Divisions currently has three strategic communications Task Forces, covering three priority regions: the Eastern and Southern neighbourhood and the Western Balkans. East Stratcom Taskforce is operational since September 2015 and, as mandated by the Council (March 2015 Conclusions), focuses on three areas: 1) effective communications and promotion of EU policies towards Eastern Partnership Countries; 2) support for media freedom and strengthening of independent media, 3) Improved EU capacity to forecast, address and raise awareness of disinformation activities by external actors. The Task Force forecasts, analyses and responds to pro-Kremlin disinformation cases and campaigns. Over the past three years, it has uncovered over 5,000 individual disinformation cases. Flagship products and initiatives: weekly EUvsDisinfo newsletter, website https://euvsdisinfo.eu/ and numerous communication campaigns in the EaP countries.

The Task Force South is operational since June 2017, established as a follow-up to the Foreign Affairs Council Conclusions on Counter-Terrorism of February 2015, with mandate reconfirmed and adjusted in June 2017 to address new communications challenges in the region. Flagship achievement: Syria Conference campaigns (Brussels II and III).

The Western Balkans Task Force was set up in July 2017 to address the need for the EU to improve its strategic communication on the EU enlargement. The Task Force's communication work presents the benefits of the partnerships, explains EU policies and its assistance for Western Balkan countries and citizens. Flagship activities: Europeans Making Difference campaign, Balkans Cultural Heritage Route, support to communication campaigns in the region. The mandate of the Task Forces has been expanded to also address the issue of disinformation.

The Division's strategic communications officers also cover Africa, Asia & Pacific, Americas, G20 countries and develop communication campaigns and activities on key thematic issues like defence and security, multilateralism, migration, human rights, economic and cultural diplomacy.

ANNEX 2

The European Centre of Excellence for Countering Hybrid Threats – Hybrid CoE

Who we are

The Hybrid Centre of Excellence for Countering Hybrid Treats is a network-based international hub for practitioners and experts building member states' capabilities to counter hybrid threats *via* sharing best practices, testing new ideas and approaches and providing training and exercises.

The Centre has an important role in strengthening EU-NATO cooperation. It has a unique status as a neutral playing field between the two institutions providing a forum for strategic discussions and joint training and exercising.

The method

While understanding the changed security environment is essential, the Centre does not want to focus on admiring the problem, but to provide concrete tools, policy recommendations, skills and best practices that build the ability of our member states, EU and NATO to respond. The aim is to break down silos between different ministries, between institutions and between the public and private sector to strengthen a whole of government and whole of society response to hybrid threats.

The excellence lies in the Centre'scross-governmental, cross-sectoral networks, which consist over 1000 practitioners and experts working with hybrid threat related work tasks in member states, in the EU or NATO. Work is planned and coordinated by the Secretariat located in Helsinki, Finland.

Key metrics

- The Centre was established on 11 April 2017 and inaugurated on 2 October, 2017.
- The current member states are Austria, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Romania, Spain, Sweden, the United Kingdom and the US.
- Participation in the Centre is open to EU Member States and NATO Allies. The EU and NATO are actively attending our activities.
- In 2019, the core budget is EUR 2.3 million.
- Total 26 employees, out of which 11 secondments from the member states (Austria Estonia, Finland, Germany, Latvia, Lithuania, the United Kingdom, the US).
- The Steering Board (SB), consists of representatives of the Centre's member states, it is the principal decision-making body governing the Centre and its work. Staff representatives from the EU and NATO are invited to attend the Steering Board meetings. The Steering Board is to set the policies and approve the work program and approves the budget and the accounts.

Top three products

1) **Countering Electoral Interference training**: The Hybrid Centre's international team of trainers provide member states with a two-day training session on countering electoral interference. Training is carried out in a road show format and the aim is to increase member state's capabilities to harden their election systems, communicate to their public and to the adversary about a potential threat and to develop a comprehensive security approach to counter electoral interference. The project has a specific focus on connecting and increasing the cooperation of intelligence services and strategic communicators to improve situational awareness and response. Training is always tailored to the members states' need, drawing on best practice and peer states lessons learnt.

2) **EU-NATO high level retreat:** The Hybrid Centre of Excellence hosts an annual EU-NATO high level retreat in Helsinki for senior leaders from both organisations. This outcome-focused event gives staff from both institutions the chance to talk about emerging challenges and how the two institutions can develop a coherent response.

3) **Workshop on Civil Protection:** The Romanian Presidency of the Council of the European Union and the Hybrid CoE organized a two-day joint workshop on EU-NATO cooperation in civil protection. The workshop took stock of EU and NATO requirements and methods for civil protection by testing them in a table top exercise dealing with a medical-based scenario. The Centre will follow up on the workshop this year. Support to EU Presidency nations is a critical part of the Centre's work.

Impact

Hybrid Centre of Excellence networks consist of over 1000 practitioners and experts from 21 Member States. The growth in its membership, the level of access it gets in Member State capitals and the number of practitioners who repeatedly return to attend the events are indicators of the Centre's success. The Centre has been also able to affect language used in the EU and the North Atlantic Treaty Organisation's documents. During the first two years of activities, the Centre has provided different kind of trainings (with "before and after assessments") and exercises, workshops, produced policy recommendations, research papers and trend mapping documents. The Centre has organised over 200 events and feedback received has been positive.

Future prospects

On substance, next year the Centre will be focused on clarifying and prioritising our activities into fewer workstrands and areas of focus where we can create even greater impact. On corporate issues, the Hybrid Centre of Excellence would look to achieve moderate membership growth and for secondments to stabilise based on the needs of the organisation.

More info

Follow us in Twitter: @HybridCoE
Learn more about us: www.hybridcoe.fi