Council of the European Union

**Brussels, 18 June 2018**
**(OR. en)**

**10135/18**

| | |
|---|---|
| **HYBRID 9** | **ENER 238** |
| **COPS 212** | **EUMC 104** |
| **PROCIV 39** | **CIVCOM 111** |
| **CSDP/PSDC 334** | **TRANS 267** |
| **CYBER 140** | **COEST 121** |
| **CFSP/PESC 568** | **ESPACE 30** |
| **JAI 646** | **COTER 77** |
| **ECOFIN 625** | **CSC 194** |
| **POLMIL 83** | **IPCR 14** |

**COVER NOTE**

| | |
|---|---|
| From: | Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director |
| To: | Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union |
| No. Cion doc.: | JOIN(2018) 14 final |
| Subject: | JOINT REPORT TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018 |

Delegations will find attached document JOIN(2018) 14 final.

Encl.: JOIN(2018) 14 final

EUROPEAN
COMMISSION

Brussels, 13.6.2018
JOIN(2018) 14 final

# JOINT REPORT TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL

## on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018

## INTRODUCTION

The Joint Framework on countering hybrid threats - A European Union response[1] places situational awareness, resilience and response at the heart of the EU action to hybrid threats. Improving our capacity to detect and understand malicious hybrid activities early and enhancing the resilience of critical infrastructure (e.g. transport, communications, energy, space and finance) of our societies and institutions are fundamental to improve our ability to withstand and recover from attacks. Countering hybrid threats requires actions from both Member States and the European institutions. The first report on the implementation of the 22 actions identified in the Joint Framework was presented to the Council on 19 July 2017[2]. This 2018 update provides an overview of progress since the summer of last year.

Considerable progress has been made in all four priority areas of action:

- Improving situational awareness
- Building resilience
- Strengthening the ability of Member States and the Union to prevent and respond to crisis, and to ensure quick and coordinated recovery
- Enhancing cooperation with NATO to ensure complementarity of measures

### RECOGNISING THE HYBRID NATURE OF THREATS

#### ***Action 1: Member States to launch a hybrid risk survey***

A Friends of Presidency Group, chaired by the rotating Presidency, has been established by the Council to take work forward. In December 2017, Member States launched a survey to assess their key vulnerabilities to hybrid threats. Based on Member States' responses the Presidency will present a report to COREPER likely before the end of June 2018.

With a view to the expiration of the Group's mandate at the end of June 2018, the FoP, at their meeting in April, started discussions on the future mandate based on the Presidency's proposal. This would extend the present mandate until 2020 and broaden its content; according to the present draft the mandate would include tasks related to analysing options to strengthen Member States' preparedness and resilience, observing national developments and help coordinate policies in the hybrid domain, support Council work on EU-NATO cooperation in the field of countering hybrid threats and exchanging information and developing a common understanding on hybrid threats.

### ORGANISING THE EU RESPONSE: IMPROVING AWARENESS

#### ***Action 2: Creation of an EU Hybrid Fusion Cell***

The EU Hybrid Fusion Cell, situated within the EU Intelligence and Situation Centre as part of the EU's civil/military Single Intelligence Analysis Capacity, draws on both civil and military analysts and contributions of Member States intelligence and security services. It achieved its full operational capacity in July 2017, a status confirmed during the 2017 Parallel and Coordinated Exercise with NATO (PACE17). The EU Hybrid Fusion Cell receives and

---

1 JOIN (2016) 18 final.

2 Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats – a European Union response, JOIN(2017) 30 final.

analyses classified intelligence and open source information concerning hybrid threats from a wide range of stakeholders. Reports and analyses are then shared across the EU institutions and Member States to inform decision-making. The EU Hybrid Fusion Cell to date has produced over 100 products pertaining to hybrid threats. CERT-EU (EU institutions' Computer Emergency Response Team) contributes to the work of the EU Hybrid Fusion Cell by sharing information on emerging or ongoing cyber-threats. However, in the domains of Chemical, Biological, Radiological and Nuclear threats, Cyber and Counter-Intelligence, specific expertise is currently limited.

In order to amplify this work, the EU Hybrid Fusion Cell has established a network of National Points of Contact. To date, 26 out of 28 Member States have identified focal points who meet regularly to share their expertise with the Cell.

Furthermore, this network is mirrored by an equivalent joint EEAS-Commission network focused on delivering against various resilience actions. These meetings are held on a monthly basis, with a focus on thematic issues including transport, infrastructure, energy, cybersecurity and hostile intelligence activities.

At the strategic level, the EU Hybrid Fusion Cell is developing its relationship with the European Centre of Excellence for Countering Hybrid Threats in Helsinki by participating in workshops, exercises as well as through routine discussions on topics to build competence in countering hybrid threats.

Under the framework of the Joint Declaration, staff-to-staff engagement with NATO's Hybrid Analysis Branch is daily and ongoing. A ground-breaking parallel and coordinated assessment on a hybrid topic was published in September 2017 and products scheduled for delivery in 2018 will focus on hybrid challenges emanating from the Southern and Eastern neighbourhoods.

***Action 3:* Strategic communications**

Strategic communications have gained additional momentum in the EU with many different actors developing capabilities. The Communication "Tackling online disinformation: a European approach"[3] of 26 April 2018 recognises disinformation as a hybrid threat, and sets out a number of actions, including a strengthened network between the Commission, the European External Action Service and Member States. The positive experiences of the East Stratcom Task Force, created with a mandate of the European Council in March 2015, need to be underpinned and strengthened, as proposed in the Joint Communication: Facing hybrid threats: protecting Europeans[4].

Most of the East Stratcom work focusses on supporting the EU Delegations in the Eastern partnership region and Russia mainly and to some extent in Central-Asia to improve delivering positive messages and to increase outreach to in-country or regional audiences. The Commission supports these activities with a multi-annual regional information and communication programme. The East Stratcom Task Force regularly coordinates its activities also with the Member States and NATO. Besides monitoring disinformation, the East Stratcom Task Force has awareness-raising activities in Eastern Partnership countries and Member States about the impact of Russian disinformation. It also stepped up training for staff in Eastern Partnership countries for enhancing their Stratcom capabilities and their resilience to disinformation. More cooperation with NATO Headquarters and the Centres of Excellence in Riga and Helsinki is foreseen in the future, such as sharing of analyses and training seminars of journalists from the Eastern Partnership region or Russia.

[3] COM(2018)236 final

[4] Reference to be inserted when known

Following the EU's new Western Balkans Strategy, a Task Force focused on the Western Balkans has been set up for communicating EU policies more effectively and to wider audiences in the region, whilst raising awareness about and addressing disinformation activities targeting the Western Balkans. The Task Force and the Commission have established an intensive cooperation aiming at more strategic and targeted communication and messaging towards the region, based on best practices and a focus on thematic campaigning. However, there is a lack of awareness of growing threats targeted to the institutions specifically. There is a need to build a culture of security awareness and to increase the capabilities of the institutions to address hybrid threats.

The Task Force South, established in 2017, adjusted its mandate to reflect a shift away from the prism of counter-terrorism towards a more nuanced approach to improving communication and outreach to the Arab World including in Arabic. As Daesh or ISIS is not the only threat in terms of radicalisation, the Task Force works to mitigate the widespread misinformation and misperception of the EU. This is done by developing, in close cooperation with the Commission, positive narratives about the European Union and its policies to build a greater understanding of the Union, communicating more strategically about the Union's activities in the Arab world, and promoting shared values and interests. The Commission supports these activities with a multi-annual regional information and communication programme.

***Action 4:*** ***Centre of Excellence for 'countering hybrid threats'.***

The European Centre of Excellence for Countering Hybrid Threats established in 2017 serves as a hub of expertise supporting the participating countries' individual and collective efforts to counter hybrid threats, through research, training, education and exercises. The Centre is open for participation to both EU Member States and NATO allies. Recently Italy, the Netherlands, Denmark and the Czech Republic became members bringing the total to 16 countries. Both the EU and NATO are on the Steering Board as observers.

In 2018, the Centre agreed on a budget and a work plan, has developed its conceptual framework and created three Communities of Interest: on Hybrid Influencing, Vulnerabilities and Resilience and Strategy and Defence. A sub-group on non-state actors has been established and looks at how different terrorist groups and proxies operate. The Centre has published a number of hybrid analyses and hosted several high level meetings to build a common understanding of hybrid threats, share best practice and seek common responses across the EU and NATO communities.

## ORGANISING THE EU RESPONSE: BUILDING RESILIENCE

Building resilience requires actions in many policy areas. These actions are not necessarily specific to the hybrid nature of the threats, but taken together, they can ensure that a more resilient EU is better equiped to face hybrid threats. Therefore, when relevant in the description of the progress made under each action below, references are made to the specific policy framework and actions taken by theUnion, in particular those actions taken as part of the work towards a Security Union. This report should therefore be read in conjunction with the monthly progress reports towards an effective and genuine Security Union, adopted on the same day.[5]

***Action 5:*** ***Protection and resilience of critical infrastructure***

The Commission has developed a draft manual of vulnerability indicators and resilience for

[5] COM(2018) 470 final.

hybrid threats to critical infrastructures in the EU. This draft manual is now in the process of validation through consultations with Member States. The final version of the manual is expected to be adopted in November 2018. Furthermore, the vulnerability indicators will be tested during the 2018 Parallel and Coordinated Exercise with NATO (PACE 18), but also by individual Member States that have indicated interest. Particular attention should be paid to the further development of detection indicators aimed at facilitating early warning at the early onset of hybrid attacks on critical infrastructure. Hybrid threats will also be considered in the upcoming evaluation of the European Directive on the Protection of Critical Infrastructure. Furthermore, the Commission is strengthening the scientific support to address the multiple and transversal characteristics of hybrid threats, focusing in particular on identification of vulnerabilities, early detection and indicators, resilience, awareness raising and exercises.

Moreover, in order to protect key assests of the Union, the Commission has put forward a proposal for a Regulation establishing a framework for screening of foreign direct investments into the European Union if they are likely to affect security or public order[6]. The Commission proposal concerns direct investments by third-country persons or undertakings which may, inter alia, affect the critical infrastructures (including energy, transport, communications, data storage, space and other sensitive facilities), critical technologies (including artificial intelligence, cybersecurity, technologies in potential dual use applications), the security of supply of critical inputs or investments allowing to access sensitive information or ability to control such information.

The Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS II), as part of the second phase, of the European Defence Agency will further support the development of the conceptual paper prepared by the Protection of Critical Energy Infrastructures (PCEI) Experts Group translating it into a guiding policy document at the EU level. This proposes a framework for identifying best management practices for Ministries of Defence in strengthening the protection and resilience of all defence-related Critical Energy Infrastructures (CEI).

***<u>Action 6:</u>*** ***Increasing the EU energy security of supply and increasing of resilience of nuclear infrastructures.***

Following its commitment in September 2017 (Joint Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[7]), the Commission will continue supporting the European Energy Information Sharing and Analysis Centre on cybersecurity.

In order to prevent gas supply crises, the Member States are implementing the Security of Gas Supply Regulation that was adopted last year while the Commission is facilitating its implementation and the cooperation between the Member States within the risk groups. The common risk assessments have to be notified to the Commission by 1 October 2018. The Commission will receive the preventive action plans and the emergency plans by 1 March 2019. The Member States should conclude the bilateral solidarity arrangements by 1 December 2018.

To address the existing regulatory gap in electricity risk preparedness, the Risk Preparedness Regulation, that is undernegotiations, would entail rules on how to assess risks, an obligation for the Member States to prepare risk preparedness plan with certain mandatory elements, how to deal with crisis situation, how to monitor security of supply. The risk preparedness plans should also include agreements on regional cooperation, especially arrangements how to manage situation of simultaneous electricity crisis. In the implementation of the Risk Preparedness Regulation, the Member States would have to prepare the first national risk preparedness planstwo years after entry into force the Regulation. Afterwards, plans should be

6 COM(2017) 487 final

7 JOIN (2017) 450 final

updated every three years. The future Risk Preparedness Regulation will also require carrying out regular and joint exercises between Member States to simulate electricity crisis. The Commission has already started preparation of such joint exercises with interested Member States, the Joint Research Center and the Electricity Coordination Group.

For the resilience of nuclear infrastructures, information exchange with and between the Member States and the Commission on Nuclear Security Issues will be improved in the short term, and an analysis for additional initiatives is foreseen. An analysis of the nuclear safeguards regulation, and for a possible guidance to assist Member States in better handling of (radioactive) High Activity Sealed Sources will be performed. In the longer term, the Commission intends to strengthen the activities in the nuclear domain where Member States have a common interest and where there is an agreed benefit of information exchange and collaboration. It will also examine appropriate measures for the effective implementation, within the EU, of the international Convention on the Physical Protection of Nuclear Material and Nuclear Facilities.

As far as the defence sector is concerned, the Consultation Forum for Sustainable Energy in the Defence and Security Sector prepared the "Roadmap for Sustainable Energy Management in the Defence and Security" to support the defence sector in improving infrastructure energy management. The Consultation Forum will continue to explore how to enable the defence sector to become more efficient with energy resources and review a number of technologies for generating projects for potential exploitation by the defence sector (e.g. wind energy, solar, smart grids, energy storage, biofuels, biomass and waste to energy).

In this context, the Energy and Environment Programme of the European Defence Agency continued its work through the Smart Blue Water Camps research project to investigate the scope for sustainable water management technological interventions in 'at home' military camps and through the Smart Camps Technical Demonstrator research contract, which investigates the feasibility of integrating a broader range or energy and environmental technologies on a larger scale in a military environment to address energy, water and waste considerations while improving the cost and military effectiveness of CSDP missions.

***Action 7:*** ***Transport and supply chain security***

For all areas of transport, namely civil aviation, maritime transport and land transport, the Commission has intensified discussions with the Member States, industry and other stakeholders on emerging security threats of a hybrid nature, to gain knowledge and learn from experiences.

In the context of the implementing activities and revision of the EU Maritime Security Strategy Action Plan, the Commission is analysing trends in maritime security - covering also piracy and maritime disputes - that could disrupt shipping and trade routes and that could affect the EU's interests. In view of the fact that EU Member States and those in the EEA control over 40% of the world's merchant fleet and that the EU is a major trading block, hybrid attacks on the maritime trade routes would have significant disruptive effects on the value and supply chains in Europe. Risk analysis and the monitoring of emerging threats in the maritime domain could lead to proposals to update the specific transport legislation, where appropriate. It is also the basis for continuous work on improving maritime awareness, including under the Common Information Sharing Environment (CISE) development context, where a new call for proposals supporting Member States to enhance IT interoperability between national maritime authorities has recently awarded three new projects (beginning of 2018).

With the adoption of the Border and Coastguard package[8] in September 2016, the European Parliament and the Council introduced a common article in the founding regulations of the European Border and Coast Guard Agency, the European Fisheries Control Agency (EFCA) and the European Maritime Safety Agency (EMSA) tasking them to strengthen their cooperation, each within their mandate, both with each other and with the national authorities carrying out coast guard functions[9], in order to increase maritime situational awareness and to support coherent and cost-efficient action. On this topic, a study identifying commonalities and ways to enhance interoperability and cooperation in the field of risk assessment among authorities performing coastguard functions was published in 201710.

Transport-related topics and emerging threats - including but not limited to ports - are cyber threats to aviation security, GPS jamming and spoofing, threats to satellites, or problems in the High North and Arctic. The Centre of Excellence for Countering Hybrid Threats in Helsinki also contributes to the analysis of these transport-related hybrid threats, and has recently taken up analysis for harbour protection.

EU customs holds a key role in ensuring external border and supply chain security and thus contributes to the security of the European Union. The Commission is significantly upgrading the advance cargo information and customs risk management system to ensure that customs in the EU obtain all necessary information, share this information more effectively between Member States, apply common and Member State-specific risk rules and target risky consignments more effectively. A key priority of the EU Chemical, Biological, Radiological and Nuclear (CBRN) Action plan[11] is to ensure border security and detection capacity against the illicit entry of CBRN materials. Adapting cargo information systems is essential to strengthen monitoring and risk-based controls of international supply chains in order that CBRN material is not illicitly entering into the EU. The Fifteenth report on progress towards an effective and genuine Security Union provides more details on the EU measures to enhance prepardeness against CBRN risks, and in particular the actions taken at EU level in the framework of the Commission Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks.

In order to remove obstacles for military mobility in the EU, the High Representative and the Commission presented an Action Plan on 28 March 2018 to explore the possibilities for civilian-military use of the Trans-European network, to simplify customs formalities for military transport and to address regulatory and procedural issues for the transport of dangerous goods for military purposes. The Commission proposed a budget of €6.5 billion under the Multi-Annual Financial Framework cluster "Defence" which would be implemented through the Connecting Europe Facility to support transport infrastructure in order to adapt it to military mobility requirements. The purpose is to enable a civilian-military dual-use of the transport infrastructure.

### ***Action 8:*** ***Building resilience in space assets***

The Commission proposal for a Space Programme of the Union[12] integrates security aspects, including in Copernicus, Government Satellite Communications and Space Surveillance and

---

8 Regulation (EU) 2016/1624 on the European Border and Coast Guard

9 Coast guard functions are: 1) Maritime safety and vessel traffic management; 2) Ship casualty and maritime assistance service; 3) Fisheries inspection and control; 4) Maritime border control; 5) Maritime environmental protection; 6) Prevention and suppression of trafficking and smuggling and related maritime law enforcement; 7) Maritime search and rescue; 8) Maritime monitoring and surveillance; 9) Maritime customs activities; 10) Maritime accident and disaster response and 11) Maritime, ship and port security

10 https://publications.europa.eu/en/publication-detail/-/publication/217db2fc-15d6-11e7-808e-01aa75ed71a1/language-en

11 COM(2017)610 final, 18.10.207

12 COM 2018(447) final, 6.6.2018

Tracking Support Framework, which would cover resilience aspects against hybrid threats, in addition to measures already in place for Galileo and EGNOS.

The Space Surveillance and Tracking[13] aims to support long-term availability of European and national space infrastructure, facilities and services. It began delivering initial services for collision avoidance, fragmentation and uncontrolled re-entry of space objects in July 2016. The Space Surveillance and Tracking national operations centres and the EU Satellite Center have data security measures in place which take account of the Council's recommendations on security aspects of the Space Situational Awareness data policy[14].

In terms of Galileo, the Commission is taking new steps to ensure better protection of the provision of data which are key to the proper functioning of critical infrastructures that depend on satellite navigation for timing and synchronisation. The use of Galileo is considered for delivering services in critical infrastructures, such as energy grids, telecommunication networks and financial market places. In this context, the Commission proposal for a Regulation establishing a framework for screening of foreign direct investments indicates the European Global Navigation Satellite Systems (GNSS) programmes Galileo and EGNOS as examples of projects or programmes of Union interest which may be relevant for the screening of foreign direct investments under the proposed Regulation.[15]

The EU Governmental Satellite Communication initiative will provide guaranteed and secured access to satellite communications to Union and Member State missions, operations and key infrastructures. This is an important tool to counter hybrid threats to a range of infrastructures, including space, transport, and energy infrastructures.

***Action 9:*** ***Adapt defence capabilities and development of EU relevance***

The European Defence Fund launched on 7 June 2017 represents a major step forward to incentivise Member States efforts to increase and sustain defence collaboration in Europe, so as to respond effectively to the strategic challenges. Under the Fund’s capability window the EU will in particular complement national financing for collaborative defence development projects. To that aim the Commission proposed in June 2017 a Regulation establishing a European Defence Industrial Development Programme with a budget of EUR 500 million for 2019-2020. A provisional agreement on the draft Regulation was reached on 22 May 2018 by the European Parliament and the Council. For the next EU Multiannual Financial Framework, the Commission proposed an integrated European Defence Fund with an ambitious budget of EUR 13 billion foreseeing more than EUR 8.90 billion for collaborative defence capability development projects.The potential impact of countering hybrid threats on capability development will be integrated in the revised Capability Development Plan, to be agreed by the Member States in June 2018.

***Action 10:*** ***Health preparedness and coordination mechanisms***

Health prepardness is a very important component of the overall preparedness against CBRN risks. This is why the Commission has taken steps, under the Commission Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, In particular, efforts have been put into initiatives to effectively share expertise.

The Commission therefore set up Chimera, an exercise for the health, civil protection and security sectors throughout the EU and third countries to test preparedness and response planning to serious cross-border threats. The fictitous scenario of the exercise included the deliberate release of a communicable disease combined with cyber-attacks on critical

13 Decision No 541/2014/EU of European Parliament and Council of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support Framework

14 Space Situational Awareness Data Policy (14698/12), 9.10.2012

15 See Annex in COM(2017)487 final.

infrastructures including hospitals to test the existing mechanisms and systems and communication tools at national and EU level in response to a hybrid threat. The EU-wide exercise took place on 30-31 January 2018 in Luxembourg. It contributed to supporting cross-sectoral capacity building and improving interoperability and coordination between health, civil protection and security sectors at EU and Member States level and collaboration with international partners. The exercise also helped identify the current responsibilities and roles of all stakeholders in crisis management of hybrid threats. The Early Warning Response System (EWRS), the Commission's cross-sectoral warning system (ARGUS), the Common Emergency Communication and Information System (CECIS), and the Council Integrated Political Crisis Response arrangements (IPCR) were tested on how they interacted. The Fifteenth report on progress towards an effective and genuine Security Union provides more details on the EU measures to enhance prepardeness against CBRN risks.

In April 2018, the Commission published a Communication and submitted a proposal for a Council Recommendation to strengthen the EU cooperation against vaccine-preventable diseases with the aim of seeing it adopted before the end of 2018. It aims to tackle vaccine hesitancy, enhance sustainability of vaccination programmes, and strengthen effectiveness of vaccine research and development

From a European Medical Corps perspective, the Norwegian Emergency Medical Team was classified by the World Health Organization (WHO), implying its adherence to minimum quality standards. In April 2018, the first regional meeting of the WHO European region emergency medical teams took place; this meeting was co-hosted by the Commission, World Health Organisation and the Belgian health authorities, as chair of the regional group.

Currently, preparations in close collaboration with the European Burns Association and the Member States are ongoing to develop a mechanism for the management of mass burn casualty disasters. Early October 2018, the Commission and Member States will meet in a workshop to finalise the work.

***Action 11:*** ***CSIRTs (Cyber Security Incident Response Teams) network and the CERT-EU and the NIS Directive***

The CERT-EUreleases cyber-threat assessment products related to critical sectors on a periodic and an ad-hoc basis. 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 Directive on security of network and information systems (NIS directive).

In September 2017, the European Defence Agency and the Estonian Presidency of the Council of the EU organised a strategic table-top cyber exercise for EU Ministers of Defence, named CYBRID17 to raise awareness of cybersecurity incident coordination at political level and of the potential effects of offensive cyber-campaigns. It focused on situational awareness, crisis response mechanisms and strategic communication. The European Defence Agency will migrate the elements of this exercise into the Education, Training, Evaluation and Exercise Platform of the European Security and Defence Collegeto be established in September 2018,. Similar high-level exercises by EU Presidencies are under consideration for the future.

***Action 12:*** ***Contractual Public Private Partnership for cybersecurity***

The Commission signed a public-private partnership on cybersecurity with the European Cybersecurity Organisation (ECSO) to stimulate the competitiveness and innovation capacities of the digital security and privacy industry in Europe. The EU will invest up to €450 million in this partnership to protect users and infrastructures from cyber attacks. The cPPP is expected to trigger €1.8 billion of investment by 2020.

On cybersecurity, the September 2017 *Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity in Europe*[16] sets out measures to provide a major boost to EU cybersecurity structures and capabilities, as set out in the Joint Communication. However effective cybersecuirty in the EU is hindered by insufficient investment and coordination. The EU is seeking to address this as set out in the Joint Communication.

***Action 13:*** ***Energy Sector Resilience***

In June 2018, the Commission will establish an energy sectoral work stream under the NIS Cooperation Group to address the particularities of the energy sector and to provide guidance to Member States on the implementation of the Directive on security of network and information systems (NIS Directive) for this sector. In parallel, the Commission is working on specific cybersecurity guidance which goes beyond the NIS Directive to identify good cybersecurity practice in the energy sector and addresses operators that are not covered by the NIS directive. The Commission will continue to initiate information sharing events about cybersecurity issues in the energy sector to raise awareness, share best practice, enhance cooperation (beyond borders and between transmission system operators and distribution system operators), address physical measures, new risks as well as education and skills.

In the long term, the Commission will establish a Network Code for sector-specific rules on cyber security as proposed in the Recast of the Electricity Regulation Recast [17] currently in the legislative process.

***Action 14:*** ***Financial sector's resilience: information-sharing platforms and networks***

The Commission's Fintech Action Plan addresses the potential barriers that limit information sharing on cyber threats among financial market players, and identify potential solutions to remedy these barriers. The CERT-EU furthermore plays a role in sharing information on incidents.

***Action 15:*** ***Resilience against cyber-attacks in the transport sector***

Protecting transport modes from cybersecurity attacks is a high priority for the Commission. In civil aviation, progress is well advanced from a cyber-security point of view, but vulnerability of the systems from a technical failure or from cyber-security threat can never discarded, as the recent IT incident in EUROCONTROL affecting half of Europe's flights showed. The Commission cooperates closely with the European Aviation Safety Agency in this transport area. CERT-EU has signed a Service Level Agreement with EUROCONTROL and a Memorandum of Cooperation with the European Aviation Safety Agency to help these entities and their stake-holders to deal with cyber-threats.

In maritime transport, the shipping industry issued cyber-security guidelines, subsequently discussed and adopted at the level of the International Maritime Organisation, in a mainly global perspective and approach. Cyber-security in European ports and port facilities remains a high policy priority, considered and regularly discussed with the Member States, industry and stakeholders in the context of the deployment and follow-up of the Network Information Security Directive.

The Commission intends to develop a holistic and interactive cyber-security knowledge toolkit with recommended good practices to support security managers and professionals in the transport sector to better identify, assess and mitigate cyber security risks.

---

16 JOIN (2017) 450 final

17 Proposal for a Regulation of the European Parliament and of the Council on the internal market for electricity (recast) - COM/2016/0861 final

***Action 16:*** ***Countering terrorist financing***

In the last year, the Commission has made significant efforts to counter-terrorist financing as reported in the regular Security Union reports. Most recently, in its security package of April 2018[18], the Commission took further measures to step up the cooperation between the authorities responsible for combating serious crime and terrorism and enhance their access to and use of financial information, with a proposal for a Directive[19] to facilitate the use of financial and other information for the prevention, detection, investigation or prosecution of serious criminal offences. Further details on the recent work done at EU level to counter terrorist financing are set out in the Fifteenth progress report towards an effective and genuine Security Union.

In order to harmonise sanctions for money-laundering criminal offences, the Commission proposed legislation with a view to adoption in mid-2018. Moreover, the 5th Anti-Money Laundering Directive was adopted in May this year to strengthen a number of measures such as enhanced checks of high-risk third countries, checks of virtual currency exchange platforms, transparency measures applicable to prepaid instruments, new powers of Financial Intelligence Units and swift access to information on the holders of bank and payment accounts, through centralised registers or electronic data retrieval systems for Financial Intelligence Units.

***Action 17:*** ***Actions against radicalisation and analysis of the need to reinforce procedures for removing illegal content***

The prevention of violent radicalisation, both off-line and on-line, has been a priority for the Commission in the last years. To step-up the work at EU level, the Commission set up a High-Level Expert Group on Radicalisation to provide recommendations on the coordination, outreach and impact of EU prevention policies. The High-Level Expert Group on Radicalisation delivered its final report on 18 May 2018, which includes a recommendation to establish an EU cooperation mechanism.

With regard to tackling illegal content online, following the adoption of the Commission's Recommendation of 1 March 2018, attention is being focussed on reducing the accessibility to such content online. The Commission has launched an impact assessment to determine whether current efforts are sufficient or whether additional measures are needed, in order to ensure the swift and proactive detection and removal of illegal content online, including possible legislative measures to complement the existing regulatory framework. The Commission work carried out in this area is set out in further details in the fifteenth progress report towards an effective and genuine Security Union.

The Code of Conduct for countering illegal hate speech online with Facebook, Twitter, Google (YouTube) and Microsoft is bringing quick and positive results. The Code of Conduct ensured that the companies made significant progress on the swift review and take down of deemed illegal hate speech which is notified to them. The 3rd monitoring exercise of the Commission on the implementation of the Code, published in January 2018, showed that on average 70% of hate speech content is removed and hate speech reviews happen within the 24 hours, as prescribed by the Code of Conduct. The Code has become an industry standard and the recent decision of Instagram and Google+ to join the Code is encouraging. In March 2018, the Commission also proposed additional measures for online platforms such as automated detection, transparency and feedback to users, and safeguards to protect freedom of speech[20].

---

18 COM(2018) 211 final.

19 COM(2018) 213 final

20 COM(2018) 1177 final

Beyond the the actions already taken against radicalisation and hate-speech on-line, steps should be taken to prevent and mitigate cyber-enabled threats to elections.

***Action 18:*** ***Increasing cooperation with neighbourhood regions and third countries***

The European Union has increased its focus on building capacities and resilience in partner countries in the security sector, inter alia, by developing the security dimension of the revised European Neighbourhood Policy. With the goal of enhancing Partners' capacities to counter hybrid threats dedicated Hybrid Risk Surveys are being launched to identify their critical vulnerabilities and provide targeted support.The EEAS, in coordination with the Commission, has conducted a survey with the Republic of Moldova. In 2018, Jordan and Georgia have officially requested the EU to undergo vulnerability surveys, the first step being to tailor the questionnaire to their specific needs. Complementary work on cybersecurity capacity building particularly for critical infrastructures has been undertaken in Ukraine through technical assistance missions, while the Commission also launched in early 2018 a comprehensive new programme designed to enhance the cyber resilience of third countries particularly in Africa and Asia.

The EU continues to discuss nuclear security capacity building plans and programs with the International Atomic Energy Agency and the U.S. government in the Border Monitoring Working Group. The European nuclear security training centre (EUSECTRA) provides training on prevention and detection in nuclear security and responding to nuclear incident modules. The Commission’s Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks has specific actions on cooperation with key international partners, including in the context of counter-terrorism and security dialogues with relevant third countries.

The EU-funded CBRN Centres of Excellence Initiative, covering nearly all Neighbourhood partners[21], continues to work on increasing national and regional capabilities of partner countries in prevention, preparedness and response to these threats, including those involving "hard security" structures.

In the Eastern and Southern neighbourhood, Civil Protection training and exercises are organised under the regional programmes of Prevention, Preparedness and Response to natural and man-made disasters (PPRD). The PPRD South third phase started in 2018, while the second phase of the PPRD East will finish in November 2018, with a possible time extension. Close links with the regional CBRN Centres of Excellences and PPRD programmes South and East shall be ensured.

## PREVENTING, RESPONDING TO CRISIS AND RECOVERING

While consequences can be mitigated through long-term policies at national and EU level, in the short-term it remains essential to strengthen the ability of Member States and the Union to prevent, respond and recover from hybrid threats in a swift and coordinated manner. A rapid response to events triggered by hybrid threats is essential. Much progress has been achieved in this area in the last year, with an operational protocol now in place in the EU laying out the crisis management process in the event of a hybrid attack. Regular monitoring and exercising will go forward.

***Action 19:*** ***A common operational protocol and exercises to improve strategic decision-making capacity in response to complex hybrid threats***

The EU Operational Protocol was established by joint staff working document in June 2016. It provided the bedrock guidance for pan-Institutional crisis response. During EUPACE17 the

[21] With regional CBRN Centres of Excellence in Rabat, Algiers, Amman and Tbilisi

protocol was tested against a hybrid scenario and proved invaluable as a tool to ease the interconnection between services. Moreover, it provided the touch points for interaction between the various levels of response: political strategic, operational and technical, as well as between the three main EU response mechanisms of Crisis Response (for external crises), ARGUS (the Commission internal IT based platform for information sharing) and the Council's Intergrated Political Crisis Response platform. The protocol also proved its worth during the parallel exercising with NATO at CMX'17. The next in the series of PACE'18 exercise will be run in November 2018 and, taking account of any future lessons identified, consideration will be given to updating the protocol.

In September and October 2017, the EU held the first parallel and coordinated exercise with NATO (PACE17), testing preparedness and interaction between the two organisations in case of a large scale hybrid crisis. In the preparatory phase, intensive staff exchanges took place across all four areas of the Hybrid Playbooks: Early Warning/Situational Awareness; Strategic Communications; Cyber defence; Crisis Prevention and Response. The scale of interaction between EU and NATO staffs during EUPACE17 is without precedent. It was also the first time that NATO participated at a Presidency-chaired Integrated Political Crisis Response round-table; senior EU officials participated in the discussions of the North Atlantic Council. The lessons-learned process focused on several aspects including the interaction between the EU and NATO crisis response mechanisms and the challenges related to the exchange of classified information between the two staffs, including the need for secure communications, notably with the aim to ensure, in the future, swift and secure exchange, in full respect of the need for originator's control.

Planning for the 2018 parallel and coordinated exercise for which the EU will be the leading organisation is on-going.

***Action 20:*** ***Examine the applicability and practical implications of Articles 222 TFEU and Article 42(7) TEU in case a wide-ranging and serious hybrid attack occurs***

The applicability of EU's solidarity clause and its mutual assitance mechanism as well as their interplay with one another and NATO's response mechanisms including Article 5 collective defence are being further discussed and tested in hybrid exercise scenarios. The Helsinki Centre of Excellence for Countering Hybrid Threats is interested and ready to take work forward both in terms of research and exercising and thus help develop a shared understanding between Member States and Allies.

***Action 21:*** ***Integrate, exploit and coordinate the capabilities of military action in countering hybrid threats within the Common Security and Defence Policy***

In response to tasking to integrate military capabilities in support of the Common Foreign and Security Policy/Common Security and Defence Policy, and following a seminar with military experts in December 2016, and guidance from the European Union Military Committee working group in May 2017, the military advice on "the EU military contribution to countering hybrid threats within the Common Security and Defence Policy" was finalised in July 2017. This work is being taken forward through the Concept Development Implementation Plan. In consultation with the European Centre of Excellence for Countering Hybrid Threats, the EU Military Staff is developing a concept on how the military can contribute to countering hybrid threats, including through Common Security and Defence Policy missions and operations.

In addition, on a daily basis the EU Military Staff and Member States are enabling the enhancement of early warning by providing military intelligence support to the EU Hybrid Fusion Cell. The Single Analytical Intelligence Capability supports EEAS Stratcom Task Forces by contributing military advice to help counter misinformation campaigns targeted at the EU and individual Member States.

Military capabilities to counter hybrid threats will be exercised during the 2018 Parallel and Coordinated Exercise with NATO (PACE18). Based on the PACE18 hybrid scenario, EU Military Staff and NATO International Military Staff will have EU-NATO Scenario Based informal discussions to ensure complementarity in countering hybrid threats, where the requirements overlap, based on the principle of inclusiveness, while respecting each organisation's decision-making autonomy and data protection rules.

## EU-NATO COOPERATION

***Action 22:*** ***EU-NATO cooperation on situational awareness, strategic communications, cybersecurity and "crisis prevention and response"***

Countering hybrid threats remains a key area of EU-NATO interaction It is based on the realisation that, in the event of a hybrid threat, the resources and capabilities that the two organisations can mobilise are complementary and enhance Member States' and Allies' ability to prevent, deter and respond to such threats. The PACE17 exercise has tested the two organisations' 'Playbooks' and, through that, their capacity to work together swiftly and effectively in support of their stricken members. In light of the experience gained the two 'Playbooks' will be revised and updated. In the field of strategic communication, consultations have taken place support for Ukraine, Bosnia and Herzegovina, the Republic of Moldova and Georgia.

In September 2017, an EU-NATO Resilience Workshop brought together experts in critical strategic sectors to exchange information on respective activities and explore proposals for further work, particularly in the area of critical infrastructure protection.

In 2018, Military Mobility is a project to facilitate the movement of military material and staff, which could take account of the likely challenges posed by hybrid threats specifically designed to slow-down Member States' and Allies' reaction times – this is an area for future parallel exercising and will be considered in the EUPACE19/20 series.

Coordinating cyber training efforts represents an important area for closer interaction. NATO was also participating as an observer at ENISA's CyberEurope tabletop exercise in June 2018.

## CONCLUSION

Improving situational awareness and building resilience against evolving hybrid threats from various sources remains challenging and requires a constant effort from the EU. The Joint Framework holds a vast set of actions ranging from improving information fusion and exchange, to strengthening protection of critical infrastructure and cybersecurity, to building resilient societies against radicalisation and violent extremism. The EU framework for countering hybrid threats has allowed for support to be given to Member States through a variety of measures aimed at bolstering the capacity of the EU and the Member States to withstand stress, to respond in a coordinated way to harmful attacks and, finally, to recover.

The EU response to hybrid threats has also been successfully tested and exercised jointly with NATO in a number exercises and the plan is to continue along these lines. Close cooperation

between all relevant actors within the EU and with NATO is key of the resilience building efforts. In addition, supporting neighbouring partner countries in identifying their vulnerabilities and strengthening capacity building against hybrid threats contributes to improved understanding of the nature of external threats and thereby, results in enhanced security for the EU neighbourhood.