Council of the European Union

Brussels, 28 July 2017
(OR. en)

11539/17

HYBRID 3	ENER 336
COPS 260	EUMC 104
PROCIV 68	CIVCOM 146
CSDP/PSDC 451	TRANS 331
CYBER 117	COEST 211
CFSP/PESC 718	ESPACE 37
JAI 722	COTER 82
ECOFIN 671	CSC 187
POLMIL 91	IPCR 9

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	20 July 2017
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	JOIN(2017) 30 final
Subject:	JOINT REPORT TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of the Joint Framework on countering hybrid threats - a European Union response

Delegations will find attached document JOIN(2017) 30 final.

Encl.: JOIN(2017) 30 final

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 19.7.2017
JOIN(2017) 30 final

JOINT REPORT TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the implementation of the Joint Framework on countering hybrid threats - a European Union response

1. INTRODUCTION

The EU is facing one of the greatest security challenges in its history. Threats are increasingly taking non-conventional forms, some physical such as new forms of terrorism, some using the digital space with complex cyber-attacks. Others are more subtle and are aimed at the coercive application of pressure including misinformation campaigns, and media manipulation. They seek to undermine core European values, such as human dignity, freedom and democracy. Recent coordinated cyber-attacks across the globe, for which attribution has proved challenging, have demonstrated the vulnerabilities of our societies and institutions.

In April 2016, the European Commission and the High Representative adopted a Joint Communication on countering hybrid threats[1] (Joint Framework). Recognising the trans-boundary and complex nature of hybrid threats this Framework proposes a whole-of-government approach to strengthening the overall resilience of our societies. The Council[2] welcomed the initiative and the proposed actions, and invited the Commission and the High Representative to report on progress in July 2017. While the EU can assist Member States to build their resilience against hybrid threats, the primary responsibility lies with Member States, insofar as countering hybrid threats relates to national security and defence.

This Joint Framework for Countering Hybrid Threats forms an important part of the EU's overall more integrated approach to security and defence. It contributes to the creation of a Europe that protects, as called for by President Juncker in the State of the Union speech of September 2016. In 2016, the European Union also laid the foundations for a stronger European defence policy to address citizens' expectations for more protection. The EU Global Strategy for EU Foreign and Security policy[3] elaborated the need for an integrated approach to link internal resilience with EU's external actions, and called for synergies between defence policy and policies covering the internal market, industry, law enforcement and intelligence services. Following the adoption in November 2016 of the European Defence Action Plan, the Commission put forward concrete initiatives which will contribute to strengthening the EU's capacity to respond to hybrid threats by fostering resilience in the defence supply chains and reinforcing the single market for defence. In particular, on 7 June 2017, the Commission launched the European Defence Fund with proposed funding of €600m up to 2020 and €1.5bn annually post 2020. The Security Union Communication[4] recognised the need to counter hybrid threats and the importance of ensuring greater coherence between internal and external actions in the field of security.

EU leaders have placed security and defence at centre-stage in the debate about the future of Europe.[5] This was acknowledged in the Rome Declaration of 25 March 2017 which set out a vision of a safe and secure Union committed to strengthening its common security and defence. The Presidents of the European Council, the European Commission and the

[1] Joint Communication to the European Parliament and the Council *Joint Framework on countering hybrid threats – a European Union response*, JOIN (2016) 18 final.
[2] *Council conclusions on countering hybrid threats*, Press Release 196/16, 19 April 2016.
[3] Presented by the High Representative to the European Council on 28 June 2016.
[4] COM(2016) 230 final, 20.4.2016.
[5] The Bratislava Roadmap of the European Council from 16 September 2016 and The Rome Declaration of the leaders of 27 member states and of the European Council, the European Parliament and the European Commission from 25 March 2017.

Secretary-General of NATO signed a Joint Declaration in Warsaw on 8 July 2016 with a view to giving new impetus and new substance to the EU-NATO strategic partnership. The Joint Declaration outlined seven concrete areas, including countering hybrid threats, where cooperation between the two organisations should be enhanced. A common set of 42 proposals for implementation was subsequently endorsed by both the EU and NATO Councils and a first report, showing substantial progress, was issued in June 2017[6].

The Commission's reflection paper on the future of European Defence[7] presented in June 2017 outlines different scenarios on how to address the growing security and defence threats facing Europe and enhance Europe's own abilities in defence by 2025. In all three scenarios security and defence are considered as integral elements of the European project, in order to protect and promote our interests at home and abroad. Europe must become a security provider and ensure progressively its own security. No single Member State can face the challenges ahead on its own, in particular that of countering hybrid threats. Cooperation on defence and security is therefore not an option; it is a necessity to deliver on a Europe that protects.

The aim of this Report is to give an account of progress and next implementing steps on the actions in the four areas proposed in the Joint Framework: improving situational awareness; building resilience; strengthening the ability of Member States and the Union to prevent and respond to crisis, and for coordinated recovery; and enhance cooperation with NATO to ensure complementarity of measures. It should be read in conjunction with the monthly progress reports towards an effective and genuine Security Union.

2. RECOGNISING THE HYBRID NATURE OF A THREAT

Hybrid activities are becoming a frequent feature of the European security environment. The intensity of these activities is increasing with growing concerns over elections being interfered with, disinformation campaigns, malicious cyber activities and perpetrators of hybrid acts trying to radicalise vulnerable members of society as their proxy actors. Vulnerabilities to hybrid threats are not limited to national boundaries. Hybrid threats need a coordinated response also at EU and NATO levels. Developments since April 2016 show that even though threats are often still assessed in isolation, there is a growing recognition and understanding within the Union of the hybrid nature of some of the activities observed and the need for coordinated action. The EU will continue its efforts to improve situational awareness and cooperation.

Action 1: Member States, supported as appropriate by the Commission and the High Representative, are invited to launch a hybrid risk survey to identify key vulnerabilities, including specific hybrid related indicators, potentially affecting national and pan-European structures and networks.

The Council has established a "Friends of the Presidency" group bringing together experts from Member States to build a generic survey that would enable them to better identify key indicators of hybrid threats, incorporate these into early warning and existing risk assessment

[6] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation
[7] Reflection paper on the future of European defence, 7.6.2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf

mechanisms and share them as appropriate. Terms of Reference have been agreed and work has already started. The generic survey should be ready by the end of 2017 with the actual surveys commencing thereafter. Protection against hybrid threats should be mutually reinforcing. Member States are therefore encouraged to carry out these surveys as rapidly as possible as they will provide valuable information on the extent of vulnerability and preparedness across Europe.

a. IMPROVING AWARENESS

The sharing of intelligence analysis and assessment work is a key tool reducing uncertainty and enhancing situational awareness. Significant progress has been made over the past year. The EU Hybrid Fusion Cell has been established and is now fully operational, the East Stratcom Task Force is in place and Finland has launched the European Centre for Countering Hybrid Threats. Much work has been focussed on analysing the tools and levers in disinformation or propaganda, with good cooperation existing between the EU StratCom Task Force East, the Hybrid Fusion Cell and NATO. This forms a good basis to continue building a more deeply-engrained culture of analysing and assessing threats to our internal and external security through a hybrid lens.

Hybrid Fusion Cell

Action 2: Creation of an EU Hybrid Fusion Cell within the existing EU Intelligence and Situation Centre structure, capable of receiving and analysing classified and open source information on hybrid threats. Member States are invited to establish National Contact Points on hybrid threats to ensure cooperation and secure communication with the EU Hybrid Fusion Cell.

The EU Hybrid Fusion Cell has been established within the EU Intelligence and Situation Centre to receive and analyse classified and open source information from different stakeholders concerning hybrid threats. Analysis is then shared within the EU and amongst Member States and in turn informs the EU decision-making processes, including inputs to the security risk assessments carried out at EU level. The EU Military Staff Intelligence Directorate contributes to the Fusion Cell work with military analysis. To date, over 50 assessments and briefings on hybrid topics have been produced. Since January 2017, the Cell has produced a periodical "Hybrid Bulletin", analysing current threats and hybrid issues, shared directly within the EU institutions and bodies and national points of contact[8]. The Cell's Full Operating Capacity has been achieved, as planned, in May 2017. Finally, staff-to-staff engagement with NATO's nascent Hybrid Analysis Branch is ongoing, both in regard to sharing lessons learnt in the creation of the Fusion Cell and in sharing information (carried out in full respect of the EU rules on classified information exchange). The EU Hybrid Fusion Cell is currently identifying further initiatives to enhance future cooperation and will play a key role in the EU-NATO parallel exercises planned for autumn 2017 where the responsiveness of the EU Hybrid Fusion Cell will be tested and lessons identified will be incorporated.

[8] To date, 21 Member States have nominated national points of contact. These are individuals working in Member States capitals in a policy / resilience role.

Strategic communication

Action 3: The High Representative will explore with Member States ways to update and coordinate capacities to deliver proactive strategic communications and optimise use of media monitoring and linguistic specialists.

In recent months, increased disinformation campaigns and systematic spreading of fake news in social media is among a spectrum of measures used to undermine adversaries. Where social media is the preferred platform, information that appears reliable and legitimate can change public opinion for the benefit some individuals, organisations or governments. These hybrid tactics have a broader goal of creating confusion in our societies and discrediting democratic governments and our structures, institutions and elections. Fake news is often spread through online platforms (see also action 17). The Commission and the High Representative welcome recent steps taken by online platforms and news media publishers to tackle misinformation. The Commission will continue to encourage such voluntary measures.

The High Representative has put in place the East Stratcom Task Force which forecasts and responds to disinformation cases and campaigns. This is significantly improving communication on Union policies in the Eastern Neighbourhood while also strengthening the media environment in these countries. The Task Force has over the past two years uncovered over 3,000 individual disinformation cases in 18 languages. The upcoming launch of a new website: *"#EUvsdisinformation*" with an online search facility will significantly improve user access. However, research and analytical work show that the number of disinformation channels and messages spread on a daily basis is significantly higher. The EU-STRAT project, funded by Horizon 2020, analyses policy and media in the Eastern Partnership countries.

The High Representative invites Member States to support the work of the StratCom Task Forces in order to counter more effectively the rise of hybrid threats. This will help the Task Force South to improve communication and outreach to the Arab World including in Arabic, myth-busting and establishing the facts about the European Union and its policies. Interaction with local journalists will help ensure the news products are culturally in tune. Both Task Forces, supported by the EU Hybrid Fusion Cell aim to support and complement Member States' related efforts. In addition, the Commission co-funds the European Strategic Communications Network, a collaborative network of 26 Member States that shares analysis, good practice and ideas on the use of strategic communications in Countering Violent Extremism, including on disinformation.

Centre of Excellence for 'countering hybrid threats'

Action 4: Member States are invited to consider establishing a Centre of Excellence for 'countering hybrid threats'.

Responding to the call to establish a Centre of Excellence, in April 2017, Finland launched the European Centre for Countering Hybrid Threats. Ten EU Member States[9], Norway and the USA are members, while both the European Union and NATO have been invited to support the steering board.[10] The Centre's mission is to encourage strategic dialogue as well

[9] Finland, France, Germany, Latvia, Lithuania, Poland, Sweden, United Kingdom, Estonia, Spain.
[10] The Centre is open for other EU Members States and NATO Allies to join.

as, conduct research and analysis working with communities of interest to improve resilience and ability to respond, in order to help counter hybrid threats. The Centre is expected to serve also as a venue for future hybrid exercises. The Centre has already established close contact with the EU Hybrid Fusion Cell and the work of the two organisations should complement each other. The EU is currently assessing ways in which it can provide concrete support to the Centre.

b. BUILDING RESILIENCE

The Joint Framework places resilience (e.g. of transport, communications, energy, finance, or regional security infrastructures) at the heart of the EU action in order to resist propaganda and information campaigns, attempts to undermine business, societies and economic flows, as well as attacks on information technology and cyber-related infrastructure. It considers strengthening resilience as a preventive and deterrent action to solidify societies and avoid escalation of crises both within and outside the EU. The EU's added value lies in assisting Member States and partners to build their resilience, relying on a wide range of existing instruments and programmes. Significant progress has been made in actions to build resilience, in areas such as cybersecurity, critical infrastructure, protecting the financial system from illicit use and efforts to counter violent extremism and radicalisation.

Protecting critical infrastructure

Action 5: The Commission, in cooperation with Member States and stakeholders, will identify common tools, including indicators, with a view to improve protection and resilience of critical infrastructure against hybrid threats in relevant sectors.

In the context of the European Programme for Critical Infrastructure Protection (EPCIP), the Commission took forward the work to identify common tools, including vulnerability indicators, to improve resilience of critical infrastructure against hybrid threats in relevant sectors. In May 2017, the Commission organised a workshop on hybrid threats to critical infrastructure, in which participants included almost all Member States, operators of critical infrastructure, the EU Hybrid Fusion Cell and NATO as observer. A common roadmap and steps for the future work, based on a questionnaire sent to national authorities in the Member States was agreed. The Commission will further consult stakeholders in the autumn, with the aim of agreeing on indicators by the end of 2017.

The European Defence Agency is working to identify common capability and research shortfalls arising from the nexus of energy infrastructures and defence capabilities. The European Defence Agency will develop a conceptual paper in autumn 2017 as well as pilot actions for holistic methodologies.

Increasing the EU energy security of supply

Action 6: The Commission, in cooperation with Member States, will support efforts to diversify energy sources and promote safety and security standards to increase resilience of nuclear infrastructures.

The Commission made concrete proposals in the security of supply package in December 2016 and in April 2017, the Council and the European Parliament reached an agreement on the new security of gas supply regulation, which aims at preventing gas supply crises. The new rules will ensure a regionally coordinated and common approach to security of supply

measures among the Member States. This will put the EU in a better position to prepare for and manage gas shortages, in case of a crisis or a hybrid attack. For the first time, the solidarity principle will apply: Member States will be able to help neighbours in the event of a serious crisis or attack, so that European households and businesses do not suffer black-outs.

The EU has also made progress in developing key projects to diversify its routes and sources of energy supplies, in line with the Energy Union Framework Strategy and the European Energy Security Strategy. For example, on the Southern Gas Corridor, concrete construction works are ongoing on all major pipeline projects: expansion of the South Caucasus pipeline, Trans-Anatolian and Trans-Adriatic pipelines, the upstream Shah Deniz II, as well as the expansion of the Southern Gas Corridor to Central Asia, notably Turkmenistan. Imports of liquefied natural gas (LNG) into Europe are increasing and are coming from new sources, such as the US. The example of the terminal in Lithuania shows how diversification projects can reduce the dependence on a single supplier. Strengthening energy efforts and better using indigenous energy sources, in particular renewables, also contributes to the diversification of energy routes and sources.

In the area of nuclear safety, the Commission is actively supporting, notably through workshops with national authorities and regulators, a consistent and effective implementation of the two Directives on nuclear safety and basic safety standards, which Member States are required to transpose by end of 2017 and 2018 respectively. Furthermore, the Euratom Research and Training programme contributes to increasing nuclear safety.

Transport and supply chain security

Action 7: The Commission will monitor emerging threats across the transport sector and will update legislation where appropriate. In implementing the EU Maritime Security Strategy and the EU Customs Risk Management Strategy and their Action Plans, the Commission and the High Representative (within their respective competences), in coordination with Member States, will examine how to respond to hybrid threats, in particular those concerning transport critical infrastructure.

In line with the Security Union communication, the Commission is facilitating security risk assessments at EU level with Member States, EU Intelligence and Situation Centre and relevant Agencies to identify threats to transport security and to support the development of effective and proportionate mitigation measures. The downing of Malaysia Airlines flight MH17 over Eastern Ukraine in 2014 highlighted the risk posed by the overflight of conflict zones. In line with the recommendations of the European High Level Task Force on Conflict Zones[11], the Commission developed a methodology for "common EU risk assessment" with the support of national aviation and security experts and the EEAS, allowing for the exchange of classified information and the definition of a common risk picture. In March 2017, the European Aviation Safety Agency (EASA) issued the first "Conflict Zones Information Bulletin"[12] on the basis of the results of this common EU risk assessment. The Commission is considering the extension of risk assessment activities carried out in the field of aviation security to other transport modes (e.g. rail, maritime) and proposals will be made in 2018. In

[11] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

[12] https://ad.easa.europa.eu/czib-docs/page-1

June 2017, the Commission, EEAS, and Member States have launched a risk assessment exercise on railway security to identify gap and possible measures to mitigate the risks.

Considerable efforts on aviation security and Air Traffic Management (ATM) have also been made in the 7th Framework Programme and Horizon 2020 security research projects. In the field of civil aviation, the Commission, with the European Aviation Safety Agency and stakeholders, is developing two new initiatives to reinforce cyber-security, also tackling hybrid threats: the establishment of the Computer Emergency Response Team on Aviation, and the setting up of a Task Force on Cyber-security in Single European Sky Air Traffic Management Research (SESAR) Joint Undertaking, responsible for the Single European Sky Air Traffic Management. The European Defence Agency provides military inputs with regard to Aviation Cyber to SESAR Joint Undertaking, as well as to the European Aviation Safety Agency through the "European Strategic Coordination Platform on Cyber Security" which, at the request of Member States and industry, will help coordination at EU level of all activities in aviation. In line with the Roadmap on cybersecurity in aviation, in 2016 the European Aviation Safety Agency carried out gap analyses of existing rules and in particular the definition and establishment of the European Centre for Cybersecurity in Aviation; the latter is now operational and cooperates with the Computer Emergency Response Team-EU (CERT-EU) (Memorandum of Understanding signed in February 2017) producing threat analyses in aviation and with EUROCONTROL (a roadmap for cooperation adopted), while a website for distribution of open sources analyses was developed. By autumn 2017, a standardisation programme and a secured information exchange will be adopted.

Customs risk management

From a customs perspective, the Commission is focusing on significantly upgrading the advance cargo information and customs risk management system. This covers the full range of customs risks, including in relation to threats to the security and integrity of international supply chains and to relevant critical infrastructures (e.g. direct threats to sea-port facilities, airports or land borders posed by imports). The upgrading aims to ensure that customs in the EU obtain all necessary information from traders as regards the movement of goods; that they are able to share this information more effectively between Member States; that they apply common as well as Member State specific risk rules; and that they are able to target risky consignments more effectively by cooperating more intensively with other authorities in particular other law enforcement and security agencies. The IT development required to implement this upgrading by the Commission is currently in its inception phase and relevant investments at central level will be launched in the coming months.

Space

Action 8: Within the context of the Space Strategy and European Defence Action Plan, the Commission will propose to increase the resilience of space infrastructure against hybrid threats, in particular, through a possible extension of the Space Surveillance and Tracking scope to cover hybrid threats, the preparation for the next generation of GovSatCom at European level and the introduction of Galileo in critical infrastructures dependant on time synchronisation.

The Commission, when preparing the regulatory framework on Government Satellite Communications (GovSatCom) and Space Surveillance and Tracking in 2018, will integrate resilience aspects against hybrid threats in its assessment. In line with the Space Strategy, when preparing the evolution of Galileo and Copernicus, the Commission, will assess the potential of these services to help mitigate vulnerability of critical infrastructures. The

Evaluation report should be ready in autumn 2017 and the proposal on the next generation of Copernicus and Galileo in 2018. The European Defence Agency is working on collaborative capability development projects in the areas of space-based communications, military positioning, navigation and timing and earth observation. All projects will focus on resilience requirements in light of current and emerging hybrid threats.

Defence capabilities

Action 9: The High Representative, supported as appropriate by Member States, in liaison with the Commission, will propose projects on how to adapt defence capabilities and development of EU relevance, specifically to counter hybrid threats against a Member State or several Member States.

In 2016 and 2017, the European Defence Agency conducted three Table Top Exercises on hybrid threats scenarios, together with the Commission, EEAS and Member States' experts. Their findings will feed into the review of the Capability Development Plan, so that the resulting key capability developments required to counter hybrid threats will be integrated in the new EU capability development priorities. Work on the revision of the Requirements Catalogue 2005 will take account of the hybrid threat dimension. In April 2017, the European Defence Agency finalised an analysis report on military implications stemming from hybrid attacks directed against critical harbour infrastructure, which will be discussed in a workshop with maritime experts in October 2017. Another specific analysis of the military role in the context of countering mini-drones is scheduled for 2018. Furthermore, capabilities priorities to strengthen resilience against hybrid threats identified by Member States might also be eligible for support under the European Defence Fund as of 2019. The Commission calls on the co-legislators to ensure a swift adoption, and on Member States to submit proposals for capability projects to strengthen the EU resilience against hybrid threats.

Action 10: The Commission, in cooperation with Member States, will improve awareness of and resilience to hybrid threats within existing preparedness and coordination mechanisms, notably the Health Security Committee.

With a view to strengthening preparedness and resilience to hybrid threats, including capacity building within health and food systems, the Commission supports the Member States - through training, simulation exercises, and by facilitating exchange of experience guidelines and financing Joint Actions. This takes place notably under the EU health security framework on serious cross-border threats to health and under the Public Health Programme to implement the International Health Regulations, a legislative pillar, binding on 196 countries including the Member States, which aims to prevent and respond to acute public, cross-border health risks worldwide. To test cross-sectorial preparedness and response in the health sector, the Commission services will carry out an exercise on complex and multidimensional hybrid threats in the autumn of 2017. The Commission and the Member States are preparing a Joint Action on vaccination, including vaccine supply and demand forecasting and research on innovative vaccine manufacturing processes with a view to strengthening vaccine supply and improving health security at the EU level (2018-2020). The Commission also collaborates with the European Food Safety Authority and the European Centre for Disease Prevention and Control to adapt to advanced scientific investigation techniques, for a more precise identification and sourcing of health threats, and a resulting rapid management of food safety outbreaks. The Commission established a network of research funders -Global Research Collaboration for Infectious Disease Preparedness – for coordinated research response within 48 hours of any significant outbreak.

<u>Action 11</u>: The Commission encourages Member States as a matter of priority to establish and fully utilise a network between the 28 CSIRTs and the CERT-EU (Computer Emergency Response Team-EU) as well as a framework for strategic cooperation. The Commission, in coordination with Member States, should ensure that sectorial initiatives on cyber threats (e.g. aviation, energy, maritime) are consistent with cross-sectorial capabilities covered by the NIS Directive to pool information, expertise and rapid responses.

The recent global cyberattacks using ransomware and malware to disable thousands of computer systems have again highlighted the urgent need to step up cyber resilience and security actions within the EU. As announced in the Digital Single market mid-term review, the Commission and the High Representative are now reviewing the 2013 EU Cybersecurity Strategy, in particular through the adoption of a package planned for September 2017. The objective will be to provide a more effective cross-sector response to these threats, increasing trust in the digital society and economy. It will also review the mandate of ENISA the EU Agency for Network and Information Security, to define its role in the changed cybersecurity ecosystem. The European Council[13] welcomed the Commission's intention to review the Cybersecurity Strategy.

The adoption of the Network Information Services (NIS) Directive[14] in July 2016 was a key step towards building European level cybersecurity resilience. The Directive sets the first EU-wide rules on cybersecurity, improves cybersecurity capabilities and strengthens cooperation between Member States. It also requires companies in critical sectors to take appropriate security measures and to notify any serious cyber incidents to the relevant national authority. These sectors include energy, transport, water, healthcare, banking and financial market infrastructure. Online marketplaces, cloud computing services and search engines will have to take similar steps. Consistent implementation across different sectors, as well as across borders will be ensured by the Network Information Services Cooperation Group (established by the Commission in 2016), which is tasked with avoiding market fragmentation. In this context, the Network Information Services Directive is considered the reference framework for any sectorial initiatives in the area of cybersecurity. Furthermore, the Directive creates the Network of Computer Security Incident Response Teams (CSIRT), which gathers all relevant stakeholders. In parallel, the Commission and CERT-EU actively monitor the cyber threat landscape and exchange information with national authorities to ensure that the EU institutions Information Technology systems are secure and resilient to cyberattack. The May 2017 WannaCry ransomware incident presented the first opportunity for the Network to engage in operational information exchange and cooperation by means of dissemination of advice. The EU Computer Emergency Response Team was in close contact with the European Cybercrime Centre (EC3) at Europol, affected countries' Computer Security Incident Response Teams (CSIRTs), cybercrime units and key industry partners to mitigate the threat and assist victims. Exchanging national situational reports produced a common situational awareness across the EU. This experience allowed the Network to be better prepared for the next incidents (e.g. "NonPetya"). Several challenges were also identified and are being addressed.

[13] European Council conclusions of 22-23 June 2017.

[14] 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.

***Action 12*: The Commission, in coordination with Member States, will work together with industry within the context of a contractual Public Private Partnership for cybersecurity, to develop and test technologies to better protect users and infrastructures against cyber aspects of hybrid threats.**

In July 2016 the Commission, in coordination with Member States, signed with industry a contractual Public Private Partnership (cPPP) for cybersecurity, investing up to €450 million under the EU research and innovation programme Horizon 2020, to develop and test technologies to better protect users and infrastructures against cyber and hybrid threats. The Partnership delivered the first pan-European Strategic Research Agenda, which focused on enhancing the resilience of critical infrastructure, as well as citizens against cyber-attacks. The Partnership increased coordination between stakeholders, leading to efficiency and effectiveness gains in the cybersecurity funding under the Horizon 2020. The Partnership is working in parallel on issues related to Cybersecurity Certification of Information and Communications Technology as well as on how to tackle the acute shortage of cybersecurity skilled professionals in the market place. In view of the substantial needs for civil research and the high resilience required in defence, the European Defence Agency Cyber Research and Technology Group is contributing to the research areas identified by the European Cyber Security Organisation in their Strategic Research and Innovation Agenda.

***Action 13*: The Commission will issue guidance to smart grid asset owners to improve cybersecurity of their installations. In the context of the electricity market design initiative, the Commission will consider proposing 'risk preparedness plans' and procedural rules for sharing information and ensuring solidarity across Member States in times of crisis, including rules on how to prevent and mitigate cyber-attacks.**

In the energy sector, the Commission is preparing a sectoral strategy on cybersecurity with the setting-up of the Energy Expert Cyber Security Platform to reinforce the implementation of the NIS Directive. A study in February 2017 identified Best Available Techniques to enhance the level of cyber-security of smart metering systems, supporting this platform. The Commission created also a web-based platform "*Incident and Threat Information Sharing EU Centre*", which analyses and shares information on cyber threats and incidents in the energy sector.

Enhancing financial sector's hybrid threat resilience

***Action 14*: The Commission, in cooperation with ENISA[15], Member States, relevant international, European and national authorities and financial institutions, will promote and facilitate threat information-sharing platforms and networks and address factors that hinder the exchange of such information.**

Recognising that cyber threats are among the top risks to financial stability, the Commission reviewed the regulatory framework on payment services in the European Union, which is now subject to implementation. The revised Payment Services Directive[16] introduced new provisions to enhance security of payment instruments and strong customer authentication, with the aim of reducing fraud, especially in online payments. The new legislative framework will be applicable as of January 2018. Currently, the Commission, assisted by the European Banking Authority and in consultation with stakeholders, is developing regulatory technical

[15] European Union Network and Information Security Agency.
[16] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, OJ L 337, 23.12.2015, p. 35.

standards, expected to be published by the end of 2017, on strong customer authentication and on common and secure communication to operationalise security in payment transactions. Furthermore, on the international front, the Commission has worked closely with the respective G7 partners on the "G7 fundamental principles of cyber security in the financial sector", endorsed in October 2016 by the G7 Finance Ministers and Central Bank's Governors. The principles are designed for financial sector entities (private and public) and contribute to a co-ordinated cybersecurity approach within the financial sector to jointly tackle cyber threats, including increased and more sophisticated cyber threats.

Transport

Action 15: The Commission and the High Representative (within their respective areas of competence), in coordination with Member States, will examine how to respond to hybrid threats, in particular those concerning cyber-attacks across the transport sector.

The implementation of the EU Maritime Security Strategy Action Plan[17] will help break the silos mentality in information exchange and shared use of assets between civilian and military authorities. A whole of government approach has led to increased cooperation across various actors. A joint Commission and EEAS civil-military Strategic Research Agenda is planned to be completed by the end of 2017, with a final workshop on protection of critical maritime infrastructure. This work could in the future expand to cover the emerging threat to sub-marine piping, energy transfer, fibre optic and traditional communications cabling from interference outside national waters.

A recent study[18] evaluated risk assessment capacity of national authorities carrying out coast guard functions. It identified the most important barriers to collaboration and recommended practical ways to enhance cooperation between maritime authorities at EU and national level on this specific field. Risk assessment is essential in countering maritime threats and even more instrumental in the evaluation and prevention of hybrid threats, since they require additional and more complex considerations. The results of this study will be presented to different coast guard related fora so that the proposed recommendations can be assessed and implemented to increase cooperation in this field with preparedness and response to hybrid threats as the main objectives.

Countering terrorist financing

Action 16: The Commission will use the implementation of the Action Plan on Terrorist Financing to also contribute to countering hybrid threats.

Hybrid threats perpetrators and their supporters require funds to execute their plans. EU efforts against crime and terrorist financing under the European Agenda on Security and the Action Plan on terrorist financing can also contribute to countering hybrid threats. In December 2016, the Commission presented three legislative proposals, including on criminal sanctions of money laundering and illicit cash payments, as well as freezing and confiscation of assets [19].

[17] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf and the 2nd report on the implementation of the EUMSS AP presented to Member States on 21 June 2017.
[18] Study on "Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions", 2017, https://ec.europa.eu/maritimeaffairs/documentation/studies
[19] Third progress report towards an effective and genuine Security Union (COM(2016) 831 final)

All Member States needed to transpose by 26 June 2017 the 4th Anti-Money Laundering Directive[20], and in July 2016, the Commission submitted a targeted legislative proposal to complement and strengthen it with additional measures[21].

On 26 June 2017, the Commission issued the supranational risk assessment foreseen by the 4th Anti-Money Laundering Directive. It also put forward a proposal for a Regulation to prevent the importation and storage in the EU of cultural goods illicitly exported from third countries[22]. Later this year, the Commission will report on its ongoing assessment of the need for possible additional measures to track terrorist financing in the EU. The Commission is also reviewing legislation on combatting fraud and counterfeiting of non-cash means of payments.[23]

The Eighth report on progress towards an effective and genuine Security Union provides more details on the state of play of implementation of the Action Plan against Terrorist Financing.

Promoting EU common values and inclusive, open and resilient societies

Building resilience against radicalisation and violent extremism

Religious and ideological radicalisation, ethnic conflict and minority conflicts can be instigated by external actors through support to specific groups or through efforts to fuel conflicts among groups. Additional challenges have emerged, such as threats from lone actors, new pathways of radicalisation, including potentially in the context of the migratory crisis, as well as the rise of right wing extremism (including violence against migrants) and risks of polarisation. While work on radicalisation is taken forward within the Security Union context, it may be also indirectly relevant from the perspective of hybrid threats insofar as people vulnerable to radicalisation can be manipulated by hybrid threat perpetrators.

Action 17: ***The Commission is implementing the actions against radicalisation set out in the European Agenda on Security and is analysing the need to reinforce procedures for removing illegal content, calling on intermediaries' due diligence in managing networks and systems.***

Preventing radicalisation

The Commission continues to implement its multi-faceted response to radicalisation as set out in the June 2016 Communication on supporting the prevention of radicalisation leading to violent extremism[24], with key actions such as promotion of inclusive education and common values, tackling extremist propaganda online and radicalisation in prisons, strengthening cooperation with third countries and enhancing research to better understand the evolving

[20]Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance), OJ L 141, 5.6.2015, p. 73–117.

[21] For more details please see the Third progress report towards an effective and genuine Security Union (COM(2016) 831 final) and the Eighth progress report towards an effective and genuine Security Union (COM(2017) 354 final)

[22] COM(2017) 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final 0.

[23] Eighth progress report towards an effective and genuine Security Union (COM(2017) 354 final)

[24] http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf

nature of radicalisation and better inform policy responses. The Radicalisation Awareness Network (RAN) has been at the forefront of the Commission's work to support Member States in this area, working with local practitioners at community level. More details are provided in the Eighth progress report towards an effective and genuine Security Union[25].

Online radicalisation and hate speech

In line with the European Agenda on Security[26], the Commission has taken steps to reduce the availability of illegal content online, notably through the EU Internet Referral Unit at Europol, and the EU Internet Forum[27]. Significant progress has also been made under the Code of Conduct countering illegal hate speech online[28]. More details are provided in the Eighth progress report towards an effective and genuine Security Union[29]. These actions will be reinforced, also in light of the European Council conclusions[30], the G7 Summit[31] and the Hamburg G20 Summit[32].

On-line platforms have a key role in tackling illegal or potentially harmful content. Under the Digital Single Market Strategy, as set out in the mid-term review[33], the Commission will ensure better coordination of platform dialogues focusing on the mechanisms and technical solutions for removal of illegal content. Where applicable, the aim should be to underpin these mechanisms with guidance on aspects, such as the notification and removal of illegal content. The Commission will also provide guidance on liability rules.

Increasing cooperation with third countries

***Action 18:* The High Representative, in coordination with the Commission, will launch a hybrid risk survey in neighbourhood regions. The High Representative, the Commission and Member States will use the instruments at their respective disposal to build partners' capacities and strengthen their resilience to hybrid threats. CSDP missions could be deployed, independently or to complement EU instruments, to assist partners in enhancing their capacities.**

The European Union has increased its focus on building capacities and resilience in partner countries in the security sector, inter alia, by building on the nexus between security and development, developing the security dimension of the revised European Neighbourhood Policy and initiating counterterrorism and security dialogues with countries around the Mediterranean. To this extent a Pilot Project risk survey was launched with the cooperation of the Republic of Moldova. Its purpose is to help identify the country's key vulnerabilities and ensure that EU assistance targets specifically those areas. The results of the pilot showed that

[25] COM(2017) 354 final
[26] For more details please see the Eighth progress report towards an effective and genuine Security Union COM(2017) 354 final
[27] For more details please see the Eighth progress report towards an effective and genuine Security Union COM(2017) 354 final
[28] Code of Conduct on illegal online hate speech, 31 May 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
[29] For more details please see the Eighth progress report towards an effective and genuine Security Union COM(2017) 354 final
[30] Council Conclusions 22-23 June 2017.
[31] G7 summit in Taormina, Italy, 26-27/05/2017.
[32] G20 summit in Hamburg, Germany, 07-08/07/2017.
[33] Cf. above Communication from the Commission COM(2017) 228 final.

the survey in itself was deemed as useful. Building on the experience gained, the Commission and the EEAS will make recommendations to prioritise actions under the heading of building effectiveness, strategic communications, critical infrastructure protection and cyber security.

Looking ahead, additional neighbouring countries could benefit from the survey, building on this first experience; albeit with tailored adaptations to reflect the differing national local situations and specific threats and avoiding duplication with ongoing counterterrorism and security dialogues. More generally, on 7 June 2017 the Commission and the High Representative adopted a Joint Communication on "A Strategic Approach to Resilience in the EU's External Action".[34] The aim is to support partner countries in becoming more resilient to today's global challenges. It recognises the need to move from crisis containment to a more structural, long-term approach to vulnerabilities, with an emphasis on anticipation, prevention and preparedness.

Cyber Resilience for Development

The EU is supporting countries beyond Europe in order to strengthen the resilience of their information networks. The ever increasing digitalisation has an intrinsic security dimension which brings particular challenges to the resilience of information networks systems globally as cyber-attacks know no borders. The EU supports third countries to build up their ability to adequately prevent and respond to accidental failures and cyber-attacks. Following a pilot cybersecurity project in the former Yugoslav Republic of Macedonia, Kosovo[35] and Moldova, concluded in 2016, the Commission will launch a new programme to enhance the cyber resilience of third countries, mainly in Africa and Asia for the period 2017-2020, but also in Ukraine. It aims to increase the security and preparedness of critical information infrastructure and networks in third countries on the basis of a whole-of-government approach, while ensuring compliance with human rights and rule of law.

Aviation Security

Civil aviation remains a major and symbolic target for terrorists but could also be targeted as part of a hybrid campaign. While the EU has developed a robust aviation security framework, flights originating from third countries may be more vulnerable. In line with UN Security Council resolution 2309 (2016), the Commission is stepping up efforts to build capacities in third countries. In January 2017, the Commission launched a new integrated risk assessment to ensure the prioritisation and coordination of capacity building efforts carried out at EU and Member State levels, as well as with international partners. In 2016, the Commission launched a 4-year project on Civil Aviation Security in Africa and the Arabian Peninsula to counter the threat of terrorism against civil aviation. The project focuses on sharing of expertise between partner States and experts from European Civil Aviation Conference Member States, mentoring, training and coaching activities. The activities will be further scaled up during 2017.

[34]Joint Communication to the European Parliament and the Council: A Strategic Approach to Resilience in the EU's external action JOIN (2017) 21 final.

[35] This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence

c. 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 take place going forward.

Action 19: ***The High Representative and the Commission, in coordination with the Member States, will establish a common operational protocol and carry out regular exercises to improve strategic decision-making capacity in response to complex hybrid threats building on the Crisis Management and Integrated Political Crisis Response procedures.***

The Joint Framework recommended the establishment of rapid response mechanisms to events triggered by hybrid threats, to coordinate among the EU response mechanisms[36] and early warning systems. To this end, the Commission services and the EEAS issued the EU operational protocol for countering hybrid threats (EU Playbook)[37], which outlines the modalities for coordination, intelligence fusion and analysis, informing policy-making processes, exercises and training, and cooperation with partner organisations, notably NATO, in the event of a hybrid threat. Similarly, NATO developed a playbook for enhanced NATO-EU interaction in preventing and countering hybrid threats in the areas of cyber defence, strategic communications, situational awareness and crisis management. The EU Playbook will be tested through an exercise in autumn 2017, as part of the European Union Parallel and Coordinated Exercise, which includes interaction with NATO.

Action 20*:* ***The Commission and the High Representative, in their respective areas of competence, will 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.***

Article 42(7) TEU refers to armed aggression on a Member State's territory, while Article 222 TFEU (solidarity clause) refers to terrorist attack or natural or man-made disaster on a Member State's territory. The latter is more likely to be used in case of hybrid attacks, which are a mix of criminal/subversive actions. The invocation of the solidarity clause triggers coordination at Council level (Integrated Political Crisis Response arrangements, IPCR) and implication of relevant EU institutions, agencies and bodies, as well as EU assistance programs and mechanisms. Council Decision 2014/415/EU provides arrangements for the implementation by the Union of the solidarity clause. These modalities of application remain valid and there is no need to revise the Council decision. If a hybrid attack includes an armed aggression, Article 42(7) could also be invoked. In such a case, the aid and assistance shall be provided both by the Member States and by the EU. The Commission and the High Representative will continue to assess the most effective ways to address such attacks.

The adoption of the EU operational Protocol, mentioned above, directly supports this assessment and will be exercised as part of the EU Parallel and Coordinated Exercise (PACE)

[36] The Council's EU Integrated Political Crisis Response (IPCR) arrangements, the Commission's ARGUS system and the EEAS' CRM.
[37] Staff Working Document (2016) 227 adopted 7 July 2016.

in October 2017. This exercise will test the EU's various mechanisms and ability to interact with the goal of speeding decision making where ambiguity triggered by a hybrid threat detracts from clarity.

Action 21: ***The High Representative, in coordination with Member States, will 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 to support CFSP/CSDP, 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 CSDP" was finalised in July 2017 and will be taken forward through the Concept Development Implementation Plan.

d. EU-NATO COOPERATION

Action 22: ***The High Representative, in coordination with the Commission, will continue informal dialogue and enhance cooperation and coordination with NATO on situational awareness, strategic communications, cybersecurity and "crisis prevention and response" to counter hybrid threats, respecting the principles of inclusiveness and autonomy of each organisation's decision making process.***

On the basis of the Joint Declaration signed by the Presidents of the European Council and the European Commission, together with the Secretary General of NATO in Warsaw on 8 July 2016, the EU and NATO developed a common set of 42 proposals for implementation, which was subsequently endorsed in separate, parallel processes on 6 December 2016 by both the EU and NATO Councils[38]. In June 2017, the High Representative/Vice President and the Secretary General of NATO published a report on the overall progress made on the 42 actions of the Joint Declaration. Countering hybrid threats is one of the seven areas of cooperation identified in the Joint Declaration accounting for ten of the forty two actions. The report demonstrates that joint efforts undertaken over the past year have delivered substantial results. Many of the specific actions aimed at countering hybrid threats have already been mentioned, including the European Centre of Excellence for Countering Hybrid Threats, better situational awareness, establishment of the EU Hybrid Fusion Cell and its interaction with the newly created NATO Hybrid Analysis Branch and collaboration between strategic communications teams. For the first time, NATO and the EU staffs will exercise together their response to a hybrid scenario. This exercise is expected to test the implementation of over a third of the common proposals. The EU will carry out its own parallel and coordinated exercise this year and is preparing to take a leading role in 2018.

On resilience, both the EU and NATO staffs have engaged in cross-briefings, including on the EU mechanism for Integrated Political Crisis Response. Regular contacts between NATO and EU staffs, including through workshops and NATO or participation in the European Defence Agency's Steering Board, have allowed information exchanges on NATO's baseline requirements for national resilience. Further exchanges between the Commission and NATO on bolstering resilience are planned for the autumn. The next progress report on EU-NATO cooperation will suggest possibilities for expanding cooperation between the two organisations.

[38] http://www.consilium.europa.eu/en/press/press-releases/2016/12/06-eu-nato-joint-declaration/

3. CONCLUSION

The Joint Framework outlines actions designed to help counter hybrid threats and foster resilience at the EU and national level, as well as for partners. While the Commission and the High Representative are delivering in all areas in close cooperation with Member States and partners it is vital that this momentum is maintained in the face of ongoing and continuously evolving hybrid threats. Member States have the primary responsibility for countering hybrid threats related to national security and the maintenance of law and order. National resilience and collective efforts to protect against hybrid threats must be understood as mutually reinforcing elements of the same overall effort. Member States are therefore encouraged to carry out hybrid risk surveys as rapidly as possible as they will provide valuable information on the extent of vulnerability and preparedness across Europe. Building on the significant progress in improving awareness the potential of the EU Hybrid Fusion Cell should be maximised. The High Representative invites Member States to support the work of the StratCom Task Forces in order to counter more effectively the rise of hybrid threats. The EU will fully support the Finnish led European Centre for Countering Hybrid Threats.

The EU's unique strength lies in assisting Member States and partners to build their resilience, relying on a wide range of existing instruments and programmes. Significant progress has been made in actions to build resilience, in areas such as transport, energy, cybersecurity, critical infrastructure, protecting the financial system from illicit use and efforts to counter violent extremism and radicalisation. EU action in building resilience will continue, as the nature of hybrid threats evolves. In particular, the EU will develop indicators to improve protection and resilience of critical infrastructure against hybrid threats in relevant sectors.

The European Defence Fund may co-finance, together with Member States, capabilities priorities to strengthen resilience against hybrid threats. The upcoming Cybersecurity package, as well as cross-sectorial measures aimed at implementation of the Networks Information Security Directive, will provide for new platforms for countering hybrid threats across the EU.

The Commission and the High Representative call on Member States and stakeholders, where necessary, to reach swift agreement and to ensure rapid and effective implementation of the many measures aimed at bolstering resilience outlined in this Communication. The EU will build on and deepen its already fruitful cooperation with NATO.

The Union remains committed to mobilising all relevant EU instruments to address complex hybrid threats. Supporting Member States' efforts remains a priority for the Union, acting as a stronger and more responsive security provider, alongside its core partners.