Council of the European Union

Brussels, 7 April 2016
(OR. en)

7688/16

COPS 102	**PROCIV 21**
CSDP/PSDC 193	**CYBER 31**
CFSP/PESC 282	**EF 75**
JAI 263	**ECOFIN 272**
POLMIL 33	**ENER 100**
EUMC 39	**POLMAR 1**
CIVCOM 60	**TRANS 97**
COEST 86	**ESPACE 20**
COAFR 97	**SAN 121**
COTER 33	**CSC 88**

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	7 April 2016
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	JOIN(2016) 18 final
Subject:	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Joint Framework on countering hybrid threats: a European Union response

Delegations will find attached document JOIN(2016) 18 final.

Encl.: JOIN(2016) 18 final

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 6.4.2016
JOIN(2016) 18 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Joint Framework on countering hybrid threats

a European Union response

1. INTRODUCTION

In recent years, the European Union's security environment has changed dramatically. Key challenges to peace and stability in the EU's eastern and southern neighbourhood continue to underscore the need for the Union to adapt and increase its capacities as a security provider, with a strong focus on the close relationship between external and internal security. Many of the current challenges to peace, security and prosperity originate from instability in the EU's immediate neighbourhood and changing forms of threats. In his 2014 Political Guidelines, the European Commission President Jean-Claude Juncker stressed the need 'to work on a stronger Europe when it comes to security and defence' and to combine European and national instruments in a more effective way than in the past. Further to this, following the invitation from the Foreign Affairs Council of 18 May 2015, the High Representative in close cooperation with Commission services and the European Defence Agency (EDA), and in consultation with the EU Member States, undertook work to present this joint framework with actionable proposals to help counter hybrid threats and foster the resilience of the EU and Member States, as well as partners.[1] In June 2015 the European Council recalled the need to mobilise EU instruments to help counter hybrid threats.[2]

While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats.

Insofar as countering hybrid threats relates to national security and defence and the maintenance of law and order, the primary responsibility lies with Member States, as most national vulnerabilities are country-specific. However, many EU Member States face common threats, which can also target cross-border networks or infrastructures. Such threats can be addressed more effectively with a coordinated response at EU level by using EU policies and instruments, to build on European solidarity, mutual assistance and the full potential of the Lisbon Treaty. EU policies and instruments can and, to a significant degree already do, play a key value-adding role in building awareness. This is helping to improve the resilience of Member States to respond to common threats. The Union's external action proposed under this framework is guided by the principles set out in Article 21 of the Treaty on European Union (TEU), which include democracy, the rule

[1] Council Conclusions on Common Defence and Security Policy (CSDP), May 2015 [Consilium 8971/15]
[2] European Council Conclusions, June 2015 [EUCO 22/15].

of law, the universality and indivisibility of human rights and respect for the principles of the United Nations Charter and international law[3].

This Joint Communication aims to facilitate a holistic approach that will enable the EU, in coordination with Member States, to specifically counter threats of a hybrid nature by creating synergies between all relevant instruments and fostering close cooperation between all relevant actors.[4] The actions build on existing strategies and sectoral policies that contribute to achieving greater security. In particular, the European Agenda on Security[5], the upcoming European Union Global Strategy for foreign and security policy and European Defence Action Plan[6], the EU Cybersecurity Strategy,[7] the Energy Security Strategy,[8] the European Union Maritime Security Strategy[9] are tools that may also contribute to countering hybrid threats.

As NATO is also working to counter hybrid threats and the Foreign Affairs Council proposed stepping up cooperation and coordination in this area, some of the proposals aim to enhance EU–NATO cooperation on countering hybrid threats.

The proposed response focuses on the following elements: improving awareness, building resilience, preventing, responding to crisis and recovering.

2. RECOGNISING THE HYBRID NATURE OF A THREAT

Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties. As a first step, the High Representative and the Commission will work together with Member States to enhance situational awareness by monitoring and assessing the risks that may target EU vulnerabilities. The Commission is developing security risk assessment methodologies to help inform decision makers and promote risk-based policy formulation in areas ranging from aviation security to terrorist financing and money laundering. In addition, a survey by Member States identifying areas vulnerable to hybrid threats would be pertinent. The aim would be to identify indicators of hybrid threats, incorporate these into early warning and existing risk assessment mechanisms and share them as appropriate.

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.

[3] The Charter of Fundamental Rights of the EU is binding on the institutions and on the Member States when they implement Union law.
[4] Possible legislative proposals will be subject to Commission better regulation requirements, in line with Commission's Better Regulation Guidelines, SWD(2015) 111.
[5] COM(2015) 185 final.
[6] To be presented in 2016.
[7] EU Cyber Defence Policy Framework [Consilium 15585/14] and Joint Communication on 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', February 2013 [JOIN(2013)1].
[8] Joint Communication on 'European Energy Security Strategy', May 2014 [SWD(2014) 330].
[9] Joint communication 'For an open and secure global maritime domain: elements for a European Union maritime security strategy — JOIN(2014) 9 final — 06/03/2014.

3. ORGANISING THE EU RESPONSE: IMPROVING AWARENESS

3.1. EU Hybrid Fusion Cell

It is essential that the EU, in coordination with its Member States, has a sufficient level of situational awareness to identify any change in the security environment related to hybrid activity caused by State and/or non-state actors. To effectively counter hybrid threats, it is important to improve information exchange and promote relevant intelligence-sharing across sectors and between the European Union, its Member States and partners.

An EU Hybrid Fusion Cell will offer a single focus for the analysis of hybrid threats, established within the EU Intelligence and Situation Centre (EU INTCEN) of the European External Action Service (EEAS). This Fusion Cell would receive, analyse and share classified and open source information specifically relating to indicators and warnings concerning hybrid threats from different stakeholders within the EEAS (including EU Delegations), the Commission (with EU agencies[10]), and Member States. In liaison with existing similar bodies at EU[11] and at national level, the Fusion Cell would analyse external aspects of hybrid threats, affecting the EU and its neighbourhood, in order to rapidly analyse relevant incidents and inform the EU's strategic decision-making processes, including by providing inputs to the security risk assessments carried out at EU level. The Fusion Cell's analytical output would be processed and handled in accordance with the European Union classified information and data protection rules.[12] The Cell should liaise with existing bodies at EU and national level. Member States should establish National Contact Points connected to the EU Hybrid Fusion Cell. Staff inside and outside the EU (including those deployed to EU delegations, operations and missions) and in Member States should also be trained to recognise early signs of hybrid threats.

Action 2: Creation of an EU Hybrid Fusion Cell within the existing EU INTCEN 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.

3.2. Strategic communication

Perpetrators of hybrid threats can systematically spread disinformation, including through targeted social media campaigns, thereby seeking to radicalise individuals, destabilise society and control the political narrative. The ability to respond to hybrid threats by employing a sound **strategic communication** strategy is essential. Providing swift

[10] In accordance with their mandates.
[11] For example, Europol's European Cybercrime Centre and Counter Terrorism Centre, Frontex, EU Computer Emergency Response Team (CERT)-EU).
[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

factual responses and raising public awareness about hybrid threats are major factors for building societal resilience.

Strategic communication should make full use of social media tools, as well as the traditional visual, audio and web-based media. The EEAS, building on the activities of the East and Arab Stratcom Task Forces, should optimise the use of linguists fluent in relevant non-EU languages and social media specialists, who can monitor non-EU information and ensure targeted communication to react to disinformation. Furthermore, Member States should develop coordinated strategic communication mechanisms to support attribution and counter disinformation in order to expose hybrid threats.

***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.**

3.3. Centre of Excellence for 'countering hybrid threats'

Building on the experience of some Member States and partner organisations[13], one or a network of multinational institutes could act as a Centre of Excellence addressing hybrid threats. Such a Centre could focus on researching how hybrid strategies have been applied, and could encourage the development of new concepts and technologies within the private sector and industry to help Member States build resilience. The research could contribute to aligning EU and national policies, doctrines and concepts, and to ensuring that decision-making can take account of the complexities and ambiguities associated with hybrid threats. Such a Centre should design programmes to advance research and exercises to find practical solutions to existing challenges posed by hybrid threats. The strength of such a Centre would rely on the expertise developed by its multinational and cross-sector participants from the civilian and military, private and academic sectors.

Such a Centre could work closely with existing EU[14] and NATO[15] centres of excellence in order to benefit from insights into hybrid threats that have been gained from cyber defence, strategic communication, civilian military cooperation, energy and crisis response.

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

4. ORGANISING THE EU RESPONSE: BUILDING RESILIENCE

Resilience is the capacity to withstand stress and recover, strengthened from challenges. To effectively counter hybrid threats, the potential vulnerabilities of key infrastructures,

[13] NATO Centres of Excellence.
[14] E.g. EU Institute for Security Studies (EU ISS), thematic EU Centres of Excellence on CBRN issues.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.

supply chains and society must be addressed. By drawing on the EU instruments and policies, infrastructure at the EU level can become more resilient.

4.1. Protecting critical infrastructure

It is important to protect critical infrastructures (e.g. energy supply chains, transport), since an unconventional attack by perpetrators of hybrid threats on any 'soft target' could lead to serious economic or societal disruption. To ensure protection of critical infrastructure, the European Programme for Critical Infrastructure Protection[16] (EPCIP) provides an all-hazard cross-sectoral systems approach, looking at interdependencies, based on the implementation of activities under the prevention, preparedness and response work streams. The Directive on European Critical Infrastructures[17] establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection. In particular, work should be re-launched under the Directive to reinforce the resilience of critical infrastructures relating to transport (e.g. EU's main airports and merchant ports). The Commission will assess whether to develop common tools, including indicators, for improving resilience of critical infrastructure against hybrid threats in all relevant sectors.

***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.**

4.1.1. Energy Networks

Undisturbed production and distribution of power is of vital importance to the EU and significant power failures could be damaging. An essential element for countering hybrid threats is to further diversify EU's energy sources, suppliers and routes, in order to provide more secure and resilient energy supplies. The Commission is also carrying out risk and safety assessments ("stress tests") on EU power plants. To ensure energy diversification, work in the context of the Energy Union Strategy is being intensified: for example, the Southern Gas Corridor can enable gas from the Caspian region to reach Europe and in Northern Europe the establishment of liquid gas hubs with multiple suppliers. This example should be followed in Central and Eastern Europe and in the Mediterranean, where a gas hub is under development.[18] The developing market for liquefied natural gas will also contribute positively to this objective.

Concerning nuclear material and facilities, the Commission supports the development and adoption of the highest standards in safety thereby reinforcing resilience. The Commission is encouraging consistent transposition and implementation of the Nuclear

[16] Communication from the Commission on a European Programme for Critical Infrastructure Protection, 12.12.2006, COM(2006) 786 final.
[17] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345 of 23.12.2008.
[18] On the progress achieved so far, see the State of the Energy Union 2015 (COM(2015) 572 final.

Safety Directive[19] that sets rules on prevention of accidents and mitigation of accident consequences and of the provisions of the Basic Safety Standards Directive[20] on international cooperation on emergency preparedness and response, particularly between neighbouring Member States and with neighbouring countries.

***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**

4.1.2 Transport and supply chain security

Transport is essential for the functioning of the Union. Hybrid attacks on transport infrastructure (such as airports, road infrastructures, ports and railways) can have serious consequences, leading to disruptions to travel and supply chains. In implementing aviation and maritime security legislation[21], the Commission carries out regular inspections[22] and, through its work on land transport security, aims to address emerging hybrid threats. In this context, an EU framework is being discussed under the revised Aviation Safety Regulation[23], as part of the Aviation Strategy for Europe[24]. Furthermore, threats to maritime security are being addressed in the European Union Maritime Security Strategy and its Action Plan[25]. The latter enables the EU and its Member States to comprehensively tackle maritime security challenges, including countering hybrid threats, through cross-sectoral cooperation between civilian and military actors to protect maritime critical infrastructure, the global supply chain, maritime trade and maritime

[19] Council Directive 2009/71/Euratom of 25 June 2009 establishing a Community framework for the nuclear safety of nuclear installations, as amended by Council Directive 2014/87/Euratom of 8 July 2014.
[20] Council Directive 2013/59/Euratom of 5 December 2013 laying down basic safety standards for the protection against the dangers arising from exposure to ionising radiation and repealing Directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom and 2003/122/Euratom.
[21] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002; Commission Implementing Regulation (EU) No 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security; Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security; Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security.
[22] Under EU law, the Commission is required to carry out inspections to ensure Member States' correct implementation of aviation and maritime security requirements. This includes inspections of the appropriate authority in the Member State, as well as inspections at airports, ports, air carriers, ships and entities implementing security measures. The Commission inspections aim to ensure that EU standards are fully implemented by Member States.
[23] Commission Regulation (EU) 2016/4 of 5 January 2016 amending Regulation (EC) No 216/2008 of the European Parliament and of the Council as regards essential requirements for environmental protection; Regulation (EC) No 216/2008 of 20/02/2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency.
[24] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: An Aviation Strategy for Europe, COM/2015/0598 final, 7.12.2015
[25] In December 2014, the Council adopted an Action Plan to implement the European Union Maritime Security Strategy; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf

natural and energy resources. The security of the international supply chain is also addressed in the European Union Customs Risk Management Strategy and Action Plan[26].

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 Action Plan, the Commission and the High Representative (within their respective compentences), in coordination with Member States, will examine how to respond to hybrid threats, in particular those concerning transport critical infrastructure.

4.1.3 Space

Hybrid threats could target space infrastructures with multi-sectoral consequences. The EU has designed the Space Surveillance and Tracking support Framework[27] to network such assets owned by Member States in order to deliver Space Surveillance and Tracking services[28] to identified users (Member States, EU institutions, spacecraft owners and operators and civil protection authorities). In the context of the upcoming Space Strategy for Europe, the Commission will explore its further development, to monitor hybrid threats to space infrastructures.

Satellite communications (SatComs) are key assets for crisis management, disaster response, police, border and coastal surveillance. They are the backbone of large-scale infrastructures, such as transport, space or remotely piloted aircraft systems. In line with the European Council call to prepare the next generation of Governmental SatCom (GovSatCom), the Commission, in cooperation with the European Defence Agency, is assessing ways to pool demand, in the context of the upcoming Space Strategy and European Defence Action Plan.

Many critical infrastructures rely on exact timing information to synchronise their networks (e.g. energy and telecommunication) or timestamp transactions (e.g. financial markets). The dependency on a single Global Navigation Satellite System time synchronisation signal does not offer the resilience required to counter hybrid threats. Galileo, the European global navigation satellite system, would offer a second reliable timing source.

Action 8: Within the context of the upcoming 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

[26] Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the EU Strategy and Action Plan for customs risk management: Tackling risks, strengthening supply chain security and facilitating trade, COM (2014) 527 final.
[27] See Decision 541/2014 of the European Parliament and of the Council.
[28] Such as in-orbit collision avoidance warning, alerts regarding breakup or collision and risky re-entries of space objects into the Earth's atmosphere.

next generation of GovSatCom at European level and the introduction of Galileo in critical infrastructures dependant on time synchronisation.

4.2. Defence capabilities

Defence capabilities need to be strengthened in order to enhance the EU's resilience to hybrid threats. It is important to identify the relevant key capability areas, e.g. surveillance and reconnaissance capabilities. The European Defence Agency could be a catalyst for a military capability development (for example, by shortening defence capability development cycles, investing in technology, systems and prototypes, opening defence business to innovative commercial technologies) related to hybrid threats,. Possible actions could be examined under the upcoming European Defence Action Plan.

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.

4.3. Protecting public health and food security

The population's health could be jeopardised by the manipulation of communicable diseases or the contamination of food, soil, air and drinking water by chemical, biological, radiological and nuclear (CBRN) agents. In addition, the intentional spreading of animal or plant diseases may seriously affect the food security of the Union and have major economic and social effects on crucial areas of the EU food chain. Existing EU structures for health security, environmental protection and for food safety can be used to respond to hybrid threats using these methods.

Under EU law on cross-border health threats[29], existing mechanisms coordinate preparedness for serious cross-border threats to health, linking Member States, EU agencies and Scientific Committees[30] through the Early Warning and Response System. The Health Security Committee, which coordinates Member States' response to threats, may act as a focal point on vulnerabilities in public health,[31] to enshrine hybrid threats (in particular bioterrorism) in crisis communication guidelines and in (crisis simulation) capacity-building exercises with Member States. In the area of food safety, through the Rapid Alert System for Food and Feed (RASFF) and the Common Risk Management System (CRMS) for customs, competent authorities exchange risk analysis information in order to monitor health risks posed by contaminated food. For animal and plant health,

[29] Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC, OJ L 293/1, 05.11.2013.
[30] Commission Decision C(2015) 5383 of 7.8.2015 on establishment of Scientific Committees in the field of public health, consumer safety and the environment.
[31] in line with Decision 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC, OJ L 293/1.

the review of the EU legal framework[32] will add new elements to the existing "toolbox" [33], to be better prepared also for 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.

4.4. Cybersecurity

The EU greatly benefits from its interconnected and digitised society. Cyberattacks could disrupt digital services across the EU and such attacks could be used by perpetrators of hybrid threats. Improving the resilience of communication and information systems in Europe is important to support the Digital Single Market. The EU Cybersecurity Strategy and the European Agenda on Security provide the overall strategic framework for EU initiatives on cybersecurity and cybercrime. The EU has been active in developing awareness, cooperation mechanisms and responses under the Cybersecurity Strategy deliverables. In particular, the proposed Network and Information Security (NIS) Directive[34], addresses cybersecurity risks for a broad range of essential service providers in the fields of energy, transport, finance and health. These providers, as well as providers of key digital services (e.g. cloud computing) should take appropriate security measures and report serious incidents to national authorities, noting any hybrid characteristics. When adopted by the co-legislators, the effective transposition and implementation of the Directive would foster cybersecurity capabilities across Member States, reinforcing their cooperation on cybersecurity through information exchange and best practices on countering hybrid threats. In particular, the Directive provides for the establishment of a network of 28 national CSIRTs (Computer Security Incidents Response Teams) and CERT-EU[35] to pursue operational cooperation on a voluntary basis.

To encourage public-private cooperation and EU-wide approaches to cybersecurity, the Commission established the NIS Platform, which issues best practice guidance on risk management. While Member States determine security requirements and modalities to notify national incidents, the Commission encourages a high degree of convergence in risk management approaches, drawing in particular on the European Union Network and Information Security Agency (ENISA).

---

[32] Regulation 2016/429 of the European Parliament and of the Council on transmissible animal diseases and amending and repealing certain acts in the area of animal health ("Animal Health Law"), OJ L84), 31/3/2016. Concerning the Regulation of the European Parliament and of the Council on Protective measures against pests ("Plant Health Law"), a political agreement on the text has been reached by the European Parliament and the Council on 16 December 2015.

[33] E.g. EU vaccine banks, sophisticated electronic animal disease information system, increased obligation for measures by labs and other entities dealing with pathogens.

[34] Commission proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union COM(2013) 48 final - 7/2/2013. Political agreement has been reached by the Council of the EU and the European Parliament on this proposed Directive and the Directive should be formally adopted soon.

[35] Computer Emergency Response Team (CERT-EU) for the EU institutions.

<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 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.

4.4.1. Industry

Increased reliance on cloud computing and big data has increased vulnerability to hybrid threats. The Digital Single Market Strategy provides for a contractual Public-Private Partnership on cybersecurity[36], which will focus on research and innovation and will help the Union to retain a high degree of technological capacity in this area. The contractual Public-Private Partnership will build trust among different market players and develop synergies between the demand and supply side. While the contractual Public-Private Partnership and accompanying measures will primarily focus on civilian cybersecurity products and services, the outcome of these initiatives should allow technology users to be better protected also against hybrid threats.

<u>Action 12</u>: 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.

4.4.2. Energy

The emergence of smart homes and appliances and the development of the smart grid, increasing digitalisation of the energy system also results in an increased vulnerability to cyberattacks. The European Energy Security Strategy[37] and the Energy Union Strategy[38] support an all-hazard approach, in which resilience to hybrid threats is integrated. The Thematic Network on Critical Energy Infrastructure Protection fosters collaboration among operators in the energy sector (oil, gas, electricity). The Commission launched a web-based platform to analyse and share information on threats and incidents.[39] It is also developing, together with stakeholders[40], a comprehensive energy-sector strategy on cybersecurity in smart grid operations to reduce vulnerabilities. Whilst electricity markets are increasingly integrated, rules and procedures for how to deal with crisis situations are still national. We need to ensure that governments co-operate with each other in preparing for and preventing and mitigating risks and that all relevant players act on the basis of a common set of rules.

[36] To be launched in mid-2016.
[37] Communication from the Commission to the European Parliament and the Council: European Energy Security Strategy - COM/2014/0330 final.
[38] Communication on 'A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy - COM/2015/080 final.
[39] Incident and Threat Information Sharing EU Centre – ITIS.
[40] In the form of the Energy Expert CyberSecurity Platform (EECSP).

<u>Action 13</u>: 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.

4.4.3. Ensuring sound financial systems

The EU's economy needs a secure financial and payment system to function. Protecting the financial system and its infrastructure from cyber-attacks, irrespective of the motive or nature of the attacker, is essential. To deal with hybrid threats against EU financial services the industry needs to understand the threat, to have tested its defences and to have the necessary technology to protect the industry from attack. Accordingly, sharing information on threats among financial market participants and with relevant authorities and key service providers or customers is crucial but needs also to be secure and meet data protection requirements. In line with work in international fora, including the G7's work in this sector, the Commission will seek to identify factors that hinder the appropriate sharing of information on threats and propose solutions. It is important to ensure regular testing and refinement of protocols to protect business and relevant infrastructures, including continuous upgrading of security enhancing technologies.

<u>Action 14</u>: The Commission, in cooperation with ENISA[41], 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.

4.4.4. Transport

Modern transport systems (rail, road, air, maritime) rely on information systems that are vulnerable cyber-attacks. Given the cross-border dimension, there is a particular role for the EU to play. The Commission, in coordination with Member States, will continue analysing cyber-threats and risks related to unlawful interferences with transport systems. The Commission is developing a Roadmap on cybersecurity for aviation in cooperation with the European Aviation safety Agency (EASA) [42]. Cyber threats to maritime security are also addressed in the European Union Maritime Security Strategy and its Action Plan

<u>Action 15</u>: 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.

[41] European Union Network and Information Security Agency

[42] The new EASA regulation is currently under discussion between the European Parliament and the Council following the Commission's proposal on December 2015. Proposal for a regulation of the European Parliament and of the Council on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and repealing Regulation (EC) No 216/2008 of the European Parliament and of the Council- COM(2015) 613 final, 2015/0277 (COD).

4.5. Targeting hybrid threat financing

Perpetrators of hybrid threats need financing to maintain their activities. Financing can be used to support terrorist groups or more subtle forms of destabilisation, such as supporting pressure groups and fringe political parties. The EU stepped up efforts against crime and terrorist financing, as set out in the European Agenda on Security, in particular with the Action Plan.[43] In this context, namely, the revised European anti-money laundering framework reinforces the fight against terrorist financing and money laundering, facilitates the work of national Financial Intelligence Units (FIUs) to identify and follow suspicious money transfers and information exchanges, while ensuring traceability of funds transfers in the European Union. It could therefore also contribute to countering hybrid threats. In the context of CFSP instruments, tailored and effective restrictive measures could be explored to counter hybrid threats.

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

4.6. Building resilience against radicalisation and violent extremism

Although terrorist acts and violent extremism are not *per se* of a hybrid nature, perpetrators of hybrid threats can target and recruit vulnerable members of society, radicalising them through modern channels of communication (including internet social media and proxy groups) and propaganda.

In order to tackle extremist content on the Internet, the Commission is – within the context of the Digital Single Market strategy – analysing the need for potential new measures, with due regard for their impact on the fundamental rights of freedom of expression and information. This could include rigorous procedures for removing illegal content, while avoiding the take down of legal content ('notice and action') and greater responsibility and due diligence by intermediaries in the management of their networks and systems. This would complement the existing voluntary approach, where internet and social media companies (in particular under the umbrella of the EU Internet Forum) and in cooperation with Europol's EU Internet Referral Unit, swiftly remove terrorist propaganda.

Within the context of the European Security Agenda, radicalisation is being countered by exchanging experiences and developing best practices, including cooperation in third countries. The Syria Strategic Communication Advisory Team aims to reinforce the development and dissemination of alternative messages to counter terrorist propaganda. The Radicalisation Awareness Network supports Member States and practitioners, who need to interact with radicalised individuals (including foreign terrorist fighters) or with those deemed vulnerable to radicalisation. The Radicalisation Awareness Network provides training activities and advice and will offer support to priority third countries, where there is willingness to engage. In addition, the Commission is fostering judicial

[43] Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing - (COM(2016) 50 final)

cooperation between criminal justice actors, including Eurojust, to counter terrorism and radicalisation across Member States, including handling foreign terrorist fighters and returnees.

Complementing the above approaches in its **external action**, the EU contributes to countering violent extremism, including through external engagement and outreach, prevention (countering radicalisation and terrorist financing), as well as through measures to address underlying economic, political and societal factors that provide opportunities for terrorist groups to flourish.

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.***

4.7. Increasing cooperation with third countries

As underlined in the European Agenda on Security, the EU has increased its focus on building capacities in ***partner countries*** in the security sector, *inter alia,* by building on the nexus between security and development and developing the security dimension of the revised European Neighbourhood Policy[44]. These actions can also promote partners' resilience to hybrid activities.

The Commission intends to further intensify the exchange of operational and strategic information with enlargement countries and within the Eastern Partnership and Southern Neighbourhood as appropriate to help combat organised crime, terrorism, irregular migration and trafficking of small arms. On counter-terrorism, the EU is stepping up cooperation with third countries by establishing upgraded security dialogues and Action Plans.

EU external financing instruments aim at building functioning and accountable institutions in third countries[45] which are a prerequisite for responding effectively to security threats and for enhancing resilience. In this context, security sector reform and capacity building in support of security and development[46] are key tools. Under the Instrument contributing to Stability and Peace[47], the Commission has developed actions to enhance cyber-resilience and partners' abilities to detect and respond to cyber-attacks

[44] Joint Communication to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions, Review of the European Neighbourhood Policy, 18.11.2015, JOIN(2015) 50 final.

[45] Idem; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU Enlargement Strategy, 10.11.2015, COM(2015) 611 final; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Increasing the impact of EU Development Policy: an Agenda for Change, 13.10.2011, COM(2011) 637 final.

[46] Joint Communication 'Capacity-building in support of security and development-enabling partners to prevent and manage crises (JOIN(2015)17final).

[47] Regulation (EU) No 230/2014 of the European Parliament and of the Council of 11 March 2014 establishing an instrument contributing to stability and peace, OJ L 77/1, 15.3.2014.

and cybercrime, which can counter hybrid threats in third countries. The EU is funding capacity building activities in partner countries to mitigate security risks linked to CBRN issues[48].

Finally, in the spirit of the comprehensive approach to crisis management, Member States could deploy Common Security and Defence Policy (CSDP) tools and missions, independently or to complement deployed EU instruments, in order to assist partners in enhancing their capacities. The following actions could be considered: (i) support for strategic communication, (ii) advisory support for key ministries exposed to hybrid threats; (iii) additional support for border management in case of emergency. Further synergies could be explored between CSDP instruments and security, customs and justice actors, including the relevant EU agencies[49], INTERPOL and the European Gendarmerie Force, in accordance with their mandates.

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.

5. PREVENTING, RESPONDING TO CRISIS AND RECOVERING

As outlined in Section 3.1, the proposed EU Hybrid Fusion Cell aims to analyse relevant indicators to prevent and respond to hybrid threats and inform EU decision-makers. While liabilities 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. In this respect, the facilitation of national civil protection actions and capacities by the European Emergency Response Coordination Centre[50] could be an effective response mechanism for aspects of hybrid threats requiring a civil protection response. This could be achieved in coordination with other EU response mechanisms and early warning systems, in particular with the EEAS Situation Room on external security dimensions and the Strategic Analysis and Response centre on internal security.

[48] Areas covered include border monitoring, crisis management, first response, illicit trafficking export control of dual-use items, disease surveillance and control, nuclear forensics, post incident recovery and protection of high-risk facilities. Best practices derived from tools developed within the EU CBRN Action Plan, such as the European nuclear security training centre and the EU's participation in International Border Monitoring Working Group, can be shared with third countries.

[49] EUROPOL, FRONTEX, CEPOL, EUROJUST

[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.

The solidarity clause (Article 222 of the TFEU) allows for Union action, as well as action between Member States, if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. Action by the Union to assist the Member State is implemented by applying Council Decision 2014/415/EU.[51] Arrangements for coordination within the Council should rely on the EU Integrated Political Crisis Response.[52] Under these arrangements, the Commission and the High Representative (in their respective areas of competence), identify relevant Union instruments and submits proposals to the Council for decisions on exceptional measures.

Article 222 TFEU also addresses situations that involve direct assistance by one or several Member States to a Member State that has experienced a terrorist attack or disaster. In this respect, Council Decision 2014/415/EU does not apply. Given the ambiguity associated with hybrid activities, the possible last resort applicability of the Solidarity Clause should be assessed by the Commission and the High Representative (in their respective areas of competence), in case an EU Member State is subject to significant hybrid threats.

By contrast to Article 222 TFEU, if multiple serious hybrid threats constitute armed aggression against an EU Member State, Article 42 (7) TEU could be invoked to provide an appropriate and timely response. A wide-ranging and serious manifestation of hybrid threats may also require increased cooperation and coordination with NATO.

When preparing their forces, Member States are encouraged to take potential hybrid threats into account. To be prepared to take decisions swiftly and effectively in case of a hybrid attack, Member States need to hold regular exercises, at working and political level, to test national and multinational decision-making ability. The objective would be to have a common operational protocol between Member States, the Commission and the High Representative, outlining effective procedures to follow in case of a hybrid threat, from the initial identification phase to the final phase of attack, and mapping the role of each Union institution and actor in the process.

As an important component of the CSDP, engagement could provide (a) civilian and military training, (b) mentoring and advisory missions to improve a threatened state's security and defence capacity, (c) contingency planning to identify signals of hybrid threats and strengthen early warning capabilities, (d) support to border control management, in case of emergency, (e) support in specialised areas, such as CBRN risk mitigation and non-combatant evacuation.

***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**

[51] Council Decision 2014/415/EU on the arrangements for the implementation by the Union of the solidarity clause, OJ L 192, 1.7.2014, p. 53.
[52] http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/

threats building on the Crisis Management and Integrated Political Crisis Response procedures.

<u>Action 20</u>: 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.

<u>Action 21</u>: 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.

6. INCREASING COOPERATION WITH NATO

Hybrid threats represent a challenge not only for the EU but also for other major partner organisations including the United Nations (UN), the Organisation for Security and Cooperation in Europe (OSCE) and particularly NATO. An effective response calls for dialogue and coordination both at political and operational level between organisations. Closer interaction between the EU and NATO would make both organisations better able to prepare and respond to hybrid threats effectively in a complementary and mutually supporting manner based on the principle of inclusiveness, while respecting each organisation's decision-making autonomy and data protection rules.

The two organisations share values and face similar challenges. EU Member States and NATO Allies alike expect their respective organisations to support them, acting swiftly, decisively and in a coordinated manner in the event of a crisis, or ideally to prevent the crisis from happening. A number of areas for closer EU–NATO cooperation and coordination have been identified, including situational awareness, strategic communications cybersecurity and crisis prevention and response. The ongoing informal EU–NATO dialogue on hybrid threats should be strengthened in order to synchronise the two organisations' activities in this area.

In order to develop complementary EU/NATO responses, it is important that both share the same situational awareness picture before and during crisis. This could be done through regular sharing of analyses and lessons identified, but also through direct liaison between the EU Hybrid Fusion Cell and NATO's hybrid cell. It is equally important to build mutual awareness of each other's respective crisis management procedures to ensure swift and effective reactions. Resilience could be enhanced by ensuring complementarity in setting benchmarks for critical parts of their infrastructures, as well as close collaboration in strategic communication and cyber defence. Fully inclusive joint exercises both at political and technical levels would enhance the effectiveness of the two organisations' respective decision-making capacity. Exploring further options in training activities would help develop a comparable level of expertise in critical areas.

<u>Action 22</u>: 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.

7. CONCLUSIONS

This Joint Communication outlines actions designed to help counter hybrid threats and foster the resilience at the EU and national level, as well as partners. As the focus is on **improving awareness**, it is proposed to establish dedicated mechanisms to exchange information with Member States and to coordinate the EU's capacity to deliver strategic communications. Actions have been outlined 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. In each of these areas, implementation of agreed strategies by the EU and the Member States, as well as Member States' full implementation of existing legislation will be a key first step, while some more concrete actions have been put forward to further reinforce these efforts.

As regards **preventing, responding to and recovering from hybrid threats**, it is proposed to examine the feasibility of applying the Solidarity Clause Article 222 TFEU (as specified in the relevant Decision) and Art. 42(7) TEU, in case a wide-ranging and serious hybrid attack occurs. Strategic decision making capacity could be enhanced by establishing a common operational protocol.

Finally, it is proposed to **step up cooperation** and **coordination between the EU and NATO** in common efforts to counter hybrid threats.

In implementing this Joint Framework, the High Representative and the Commission are committed in mobilising relevant EU instruments at their respective disposal. It is important for the EU, together with the Member States, to work to reduce risks associated with exposure to potential hybrid threats from state and non-state actors.