027142/EU XXVI. GP
Eingelangt am 19/06/18

Council of the European Union

Brussels, 18 June 2018
(OR. en)

10242/18

HYBRID 11	**ENER 242**
COPS 223	**EUMC 106**
PROCIV 40	**CIVCOM 120**
CSDP/PSDC 346	**TRANS 271**
CYBER 147	**COEST 126**
CFSP/PESC 583	**ESPACE 32**
JAI 668	**COTER 80**
ECOFIN 632	**CSC 200**
POLMIL 89	**IPCR 15**

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	JOIN(2018) 16 final
Subject:	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Increasing resilience and bolstering capabilities to address hybrid threats

Delegations will find attached document JOIN(2018) 16 final.

Encl.: JOIN(2018) 16 final

www.parlament.gv.at

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 13.6.2018
JOIN(2018) 16 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL

Increasing resilience and bolstering capabilities to address hybrid threats

www.parlament.gv.at

1. INTRODUCTION

Hybrid activities by State and non-state actors continue to pose a serious and acute threat to the EU and its Member States. Efforts to destabilise countries by undermining public trust in government institutions and by challenging the core values of societies have become more common. Our societies face a serious challenge from those who seek to damage the EU and its Member States, from cyber-attacks disrupting the economy and public services, through targeted disinformation campaigns to hostile military actions.

Hybrid campaigns are multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic, and technological) to destabilise the adversary. They are designed to be difficult to detect or attribute, and can be used by both state and non-state actors. The nerve agent attack in Salisbury last March[1] further underlined the versatility of hybrid threats and the multitude of tactics now available. In response, the European Council[2] highlighted the need to step up the capacity of the EU and its Member States to detect, prevent and respond to hybrid threats in areas such as cyber, strategic communication and counter-intelligence. It also drew particular attention to the need for resilience in the face of Chemical, Biological, Radiological and Nuclear-related threats.

The threats posed by non-conventional weapons fall in a category of their own because of the potential scale of the damage they can cause. As well as being difficult to detect and attribute, they are complex to remedy. Chemical, Biological, Radiological and Nuclear-related threats, going beyond hybrid threats and covering also terrorist threats, are also a general concern of the international community[3], particularly the evolving risk of proliferation both geographically and to non-State actors.

Strengthening resilience to these threats and bolstering capabilities are predominantly Member State responsibilities. However, the EU institutions have already taken a number of actions to help to reinforce national efforts. This has included working in close collaboration with other international actors, including in particular the North Atlantic Treaty Organisation (NATO)[4], and such work could deepen further into support to Member States in areas like rapid response[5].

This Joint Communication responds to the European Council's invitation to take this work forward. It is part of a broader package which also includes the latest Security Union progress report[6], which takes stock and presents next steps in implementing the Chemical, Biological, Radiological and Nuclear Action Plan of October 2017[7], as well as the Second

---

1 As regards the Salisbury attack, the European Council on 22 March 2018 "agreed with the United Kingdom government's assessment that it is highly likely that the Russian Federation is responsible and that there is no plausible alternative explanation."

2 European Council conclusions of March 2018.

3 Including by the United Nations Security Council, Resolution S/RES/2325 (2016), 14 December 2016.

4 Countering hybrid threats is one of the seven areas of cooperation with the North Atlantic Treaty Organisation outlined in the Joint Declaration signed in Warsaw in July 2016 by the President of the European Council, the President of the European Commission, and the Secretary General of the North-Atlantic Treaty Organisation.

5 The G7, meeting at a summit in Charlevoix in June 2018, also agreed to develop a G7 Rapid Response Mechanism to address threats to democracies: https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/

6 Fifteenth Progress Report towards an effective and genuine Security Union, COM(2018) 470.

7 COM(2017) 610 final.

www.parlament.gv.at

progress report[8] on the implementation of the 22 actions of the Joint Framework on countering Hybrid Threats – a European Union response[9].

2. THE EU RESPONSE

The Commission and the High Representative have invested consistent efforts to build up the EU's capabilities and effectively support Member States to counter hybrid and Chemical, Biological, Radiological and Nuclear-related threats. Tangible results have already been achieved in areas such as strategic communications, situational awareness, strengthening preparedness and resilience, and reinforcing crisis response capacities.

The East Stratcom Task Force, established after the March 2015 European Council, has spearheaded work on forecasting, tracking and tackling disinformation originating from foreign sources. Its expert analyses and public products[10] have significantly raised awareness about the impact of Russian disinformation. Over the past two years, it has uncovered over 4000 individual disinformation cases, many of which deliberately targeting Europe. The work of the East Stratcom Task Force has also focused on the improved delivery of positive communications, with increased outreach in the Eastern Neighbourhood. Following this success, two other taskforces have been created with different geographic focus - a Task Force for the Western Balkans and a dedicated Task Force South for the Arab-speaking world.

Important steps have been taken to build up structures needed to improve situational awareness and support decision-making. The Hybrid Fusion Cell was established within the EU Intelligence and Situation Centre of the European External Action Service in 2016. The Fusion Cell receives and analyses classified and open source information from different stakeholders concerning hybrid threats. Over 100 assessments and briefings have been produced to date, shared within the EU and amongst Member States to inform EU decision-making. The Hybrid Fusion Cell has a close working relationship with the European Centre of Excellence for Countering Hybrid Threats in Helsinki. Set up in April 2017 to encourage strategic dialogue and carry out research and analysis on hybrid threats, the Centre of Excellence has now expanded its membership to 16 countries[11] and receives sustained support from the EU.

There have also been important steps in bolstering preparedness and resilience, in particular against Chemical, Biological, Radiological and Nuclear-related threats. The past six months have seen major steps in identifying gaps in preparedness for Chemical, Biological, Radiological and Nuclear-related security incidents, notably in terms of detection capacity to help prevent Chemical, Biological, Radiological and Nuclear-attacks. At the Commission's initiative, a consortium of national experts carried out an analysis of the gaps in the detection equipment for different types of Chemical, Biological, Radiological and Nuclear-related scenarios. The gap analysis report has been shared with Member States, allowing them to make informed decisions on detection strategies and take operational measures to address the identified gaps.

---

8 Joint Report on the implementation of the Joint Framework on countering hybrid threats (July 2017-July 2018), JOIN(2018) 14.

9 JOIN(2016) 18 final.

10 See www.euvsdisinfo.eu

11 Of the current 16 members 14 are EU Member States: the Czech Republic, Denmark, Estonia, Finland, France, Italy, Germany, Latvia, Lithuania, the Netherlands, Poland, Spain, Sweden, the United Kingdom. The initiative for its creation comes from the Joint Framework on Countering Hybrid Threats. The Centre has been also actively supported by the EU and the North Atlantic Treaty Organisation in the framework of their cooperation.

This work has been backed up through exercises testing out the degree of progress. The 2017 Parallel and Coordinated Exercise (PACE17) with the North Atlantic Treaty Organisation has allowed a detailed testing of the EU's response capacities to large-scale hybrid crisis. Unprecedented in terms of scope, it put to test not only the "EU Hybrid Playbook", the different EU response mechanisms and their ability to interact efficiently with each other, but also how the EU's response to hybrid threats interacted with North Atlantic Treaty Organisation's action. An Exercise for 2018 is in its planning phase, with the ambition not only to establish it as an annual practice, but also to help Member States to reinforce their hybrid crisis response capacities.

These concrete steps illustrate how the policy frameworks put in place by the EU are bearing fruit: the past two years have seen a series of frameworks to help guide and focus the EU's work.

The April 2016 *Joint Framework on countering hybrid threats – a European Union response*[12] encouraged a whole-of-government approach, with 22 areas for action, to help counter **hybrid threats** and foster the resilience of the EU and the Member States, as well as that of international partners. Most actions defined in the Joint Framework focus on improving situational awareness and building resilience, with better capacity to respond. They range from bolstering EU's intelligence analysis capacity to strengthening protection of critical infrastructure and cybersecurity to fighting radicalisation and violent extremism. Cyber-related threats and cyber-attacks are also at the core of the Joint Framework. The second progress report on the implementation of the Joint Framework, adopted in parallel to this Joint Communication, demonstrates tangible progress on these actions and confirms the strengthening and deepening of EU efforts to counter hybrid threats[13].

On **cyber-security**, 9 May 2018 was an important landmark as the deadline for all EU Member States to transpose the first EU-wide legally binding set of rules on cybersecurity, the Directive on Security of Networks and Information Systems. This is an important part of the broader approach set out in the September 2017 *Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity in Europe*,[14] with wide-ranging concrete measures to provide a major boost to EU's cybersecurity structures and capabilities. This centred on building EU's resilience to cyber-attacks and stepping up the EU's cybersecurity capacity; creating an effective criminal law response; and strengthening global stability through international cooperation. It was accompanied by a proposal for a Cybersecurity Act, to strengthen support at EU level[15] and has been backed up with a series of proposals which need to be carried through to implementation (see below).

Disinformation harms our democracies by hampering the ability of citizens to take informed decisions and to participate in the democratic process. The internet has vastly increased the volume and variety of news available to citizens. However, new technologies can be used to disseminate disinformation at unprecedented scale and speed, targeting with precision to sow distrust and create societal tensions. The Commission *Communication on tackling online disinformation: a European Approach*[16] set out a European approach in response to the problem of disinformation by calling on different stakeholders, in particular online platforms but also media companies, to take action. These actions cover a broad range of relevant fields, including increased transparency; trustworthiness and accountability of online platforms; more secure and resilient election

---

13 For the first Implementation report (July 2017): JOIN(2017) 30 final.
14 JOIN(2017) 450 final.
15 COM (2017) 477, see below.
16 COM (2018) 236 final.

www.parlament.gv.at

processes; fostering education and media literacy; supporting quality journalism; and countering disinformation through strategic communication. First concrete steps include a Code of Practice on Disinformation, to be developed by a Multi-Stakeholder Forum on Disinformation and a network of fact-checkers to be in place before the summer. A first meeting of the Multi-Stakeholder Forum on Disinformation was held on 29 May 2018, agreeing the steps needed to adopt the code in July 2018. The Commission will assess by the end of 2018 the progress made in tackling the problem and decide whether an additional intervention in this field is needed. The activities foreseen will be coherent with and complementary to those of the East Stratcom Task Force.

As regards **Chemical, Biological, Radiological and Nuclear** risks, the Commission's October 2017 *Action Plan*[17] proposed 23 practical actions and measures aimed at better protection of citizens and infrastructures against these threats, including through closer cooperation between the EU and its Member States, as well as with the North-Atlantic Treaty Organisation. As part of the measures in the Security Union to improve protection and resilience against terrorism, it followed a preventive approach based on the rationale that Chemical, Biological, Radiological and Nuclear-related risks were with low probability but high and lasting impact in case of an attack. In the meantime, the attack in Salisbury, as well as an increasing concern about terrorist interest and a capability to use Chemical, Biological, Radiological and Nuclear materials both inside and outside the EU[18] show that the threat posed by Chemical, Biological, Radiological and Nuclear substances is real. This further reinforces the urgent need to fully implement the Action Plan. It follows an all-hazards approach, and focuses on four objectives: reducing the accessibility of Chemical, Biological, Radiological and Nuclear materials; ensuring a more robust preparedness for and response to Chemical, Biological, Radiological and Nuclear security incidents; building stronger internal-external links in Chemical, Biological, Radiological and Nuclear security with key regional and international EU partners; and enhancing knowledge of Chemical, Biological, Radiological and Nuclear risks. Detailed reporting on the tangible progress in implementing the Action Plan is provided in the latest Security Union progress report, adopted in parallel to this Joint Communication.

Finally, to increase the effectiveness of efforts to counter hybrid threats and reinforce the message of unity among EU Members States and North-Atlantic Treaty Organisation (NATO) Allies, cooperation against hybrid threats has been defined as a key area of **EU-NATO cooperation**, as outlined in the July 2016 *Warsaw Joint Declaration*[19]. Nearly one third of all the current common proposals for cooperation are focused on hybrid threats[20]. The exercises and the "EU Playbook"[21] described above are being built on with deepened cooperation this year.

3. STEPPING UP THE RESPONSE TO THE EVOLVING THREATS

3.1. Situational awareness – improved capacity to detect hybrid threats

Efforts to counter and respond to hybrid threats have to be underpinned by a capacity to detect early malicious hybrid activities and sources, internal and external, and to

17 COM(2017) 610 final.

18 Europol, Terrorism Situation and Trend report (TE-SAT) 2017, p. 16, available at: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. See also the statements by the Director-General of the OPCW: www.globaltimes.cn/content/1044644.shtml.

19 The declaration signed by President Juncker, President Tusk, and NATO Secretary General Stoltenberg constitutes the current basis for EU-NATO cooperation.

20 15283/16 and 14802/17.

21 SWD(2016) 227 final.

www.parlament.gv.at

understand the possible links between often seemingly unconnected events. To that end, it is essential to make use of all available data streams, including open source intelligence.

The Hybrid Fusion Cell established within the European External Action Service as a single EU point of focus for Hybrid Threat Analysis is an important asset, but it needs the necessary expertise to address the full spectrum of hybrid threats, including in the field of Chemical, Biological, Radiological and Nuclear, as well as Counter Intelligence. Broadening the expertise would increase the support to any future EU crisis response by offering more complete civil and military intelligence products in these specific domains. This could be backed up by Member State action to increase the intelligence contributions of their national services to the Hybrid Fusion Cell and to further enhance the ability of the established network of national Points of Contact to the Hybrid Fusion Cell to provide and process time-critical information. Another step would be for Member States to look at increasing the intelligence contributions of their national services to the EU Intelligence and Situation Centre (INTCEN), to permit deeper analysis of potential threats.

Future Steps

- The High Representative will expand the EU Hybrid Fusion Cell with specialised Chemical, Biological, Radiological and Nuclear, Counter Intelligence as well as Cyber analytical components. Member States are invited to step up intelligence contributions to the Hybrid Fusion Cell for the analysis of existing and emerging hybrid threats.

- The Commission, in coordination with the High Representative, will finalise work on vulnerability indicators to allow Member States to better assess the potential of hybrid threats in different sectors. This work will also support EU's analysis of hybrid trends.

3.2. **Reinforced actions against Chemical, Biological, Radiological and Nuclear threats**

The October 2017 Action Plan against Chemical, Biological, Radiological and Nuclear security risks provides the framework for action to strengthen preparedness, resilience and coordination at EU level. The actions it sets out cover a range of measures to support Member States by pooling expertise and joint capacity building, exchanging knowledge and best practice, and stepping up operational cooperation. Member States and the Commission need to work together to fully implement the Action Plan as a matter of urgency. In addition, building on the progress already made in terms of gap analysis on detection capacities and in the exchange of best practice in the newly created Chemical, Biological, Radiological and Nuclear Security Advisory Group, the Union should now take further measures to address developing and evolving threats. This applies in particular to chemical threats. Following the example of the work to restrict the access to explosives precursors[22], the EU needs to take swift operational measures to better control access to high-risk chemical materials, and optimise the ability to detect such materials at the earliest stage possible. Member States also should consider carrying out further gap analysis and mapping exercises at EU level, for instance on Chemical, Biological,

[22] As part of the work in the Security Union to close down the space in which terrorists and criminals operate, the Commission has taken firm action to reduce the access to explosives precursors that can be misused to make homemade explosives. In October 2017, the Commission presented a Recommendation setting out immediate actions to prevent misuse of explosive precursors based on existing rules (Recommendation C(2017) 6950 final). Building on that, the Commission adopted in April 2018 a proposal to revise and strengthen the existing Regulation 98/2013 on the marketing and use of explosives precursors (COM(2018) 209 final).

www.parlament.gv.at

Radiological and Nuclear resilience and decontamination assets and approaches. Preparing and managing the consequences of a Chemical, Biological, Radiological and Nuclear-related attack requires strengthened cooperation and coordination amongst Member States, including civil protection authorities. The Union's Civil Protection Mechanism can play a key part in this process with the aim of strengthening Europe's collective capacity to prepare and respond.

International cooperation is also an important element in this work, and the EU can build on links with the regional Chemical, Biological, Radiological and Nuclear Centres of Excellences, including seeking synergies with the North-Atlantic Treaty Organisation, and the Prevention, Preparedness and Response to natural and man-made disasters programmes for the South and East[23].

Future Steps

- The EU should explore measures to uphold respect for international rules and standards against the use of Chemical Weapons, including through a possible specific EU sanctions regime on Chemical Weapons.

- To take forward the Chemical, Biological, Radiological and Nuclear Action Plan, the Commission will work with Member States to complete the following steps by the end of 2018:
  - develop a list of chemical substances posing a particular threat, as a basis for operational action to reduce their accessibility;
  - set up a dialogue with private actors in the supply chain to work together towards addressing evolving threats from chemicals that can be used as precursors;
  - accelerate a review of threat scenarios and an analysis of existing detection methods to improve the detection of chemical threats, with the aim of developing operational guidance for Member States to step up their detection capabilities.

- Member States should establish inventories of stockpiles of essential medical countermeasures, laboratory, treatment and other capacities. The Commission will work with Member States to regularly map the availability of these stockpiles across the EU to increase their access and rapid deployment in case of attacks

3.3. **Strategic communication – coherent dissemination of information**

An important challenge with respect to hybrid threats is to raise awareness and educate the general public to discern information from disinformation. Building on the experience of the East Stratcom Task Force, the EU Hybrid Fusion Cell and the European Centre of Excellence for Countering Hybrid Threats, as well as other efforts by the Commission[24], the Commission and the High Representative will further develop and professionalise EU strategic communications capabilities, by ensuring systematic interaction and coherence between the existing structures. This will be further extended to other EU institutions and

[23] In the Eastern and Southern neighbourhood, Civil Protection training and exercises are organised under the regional programmes of Prevention, Preparedness and Response to natural and man-made disasters.

[24] Commission Representations, for example, are also active in the area of fact-checking and myth-busting. Several have developed locally adapted tools, like *Les Décodeurs de l'Europe* in France, UE Vero Falso in Italy, a public EU Myth-busters cartoon competition in Austria, a similar cartoon series. in Romania and the UK Representation's Euromyths A-Z. More such projects are in the making.

Member States, including by using the announced secure online platform on disinformation.

Improved coordination and cooperation on strategic communication across the EU institutions, with the Member States and with partners and international organisations, will be essential and requires preparation and practice before reacting to real-time crises.

Election periods have proven to be a particularly strategic and sensitive target for cyber-enabled attacks and online circumvention of conventional ("off-line") safeguards and rules such as silence periods, transparent funding rules, and equal treatment of candidates. This has included attacks against electoral infrastructures and campaign IT systems, as well as politically-motivated mass online disinformation campaigns and cyber-attacks by third countries with the aim to discredit and delegitimise democratic elections. Several work strands are being carried forward at EU level to raise awareness in Member States in preparing and responding to these evolving threats. In the Council, the Member States' cybersecurity authorities[25] will issue voluntary guidelines and define common best practices to address cyber security of election technology through the election life cycle. This includes information systems and ICT solutions used to register voters and candidates, gather and count votes and broadcast results, as well auxiliary systems directly linked to the legitimacy of election results.

There is also a need to ensure quick, reliable and consistent information to the general public in case of hybrid attacks. Any Chemical, Biological, Radiological and Nuclear incident or similar impact event causes public outcry as citizens demand quick answers. Strategic messaging has a key role including between international organisations that may be separately enacting their response plans.

Future Steps

- The European External Action Service and the Commission will work together within their respective competences to establish more structured cooperation on Strategic Communications to address disinformation emanating from inside and outside the EU and to deter hostile disinformation production and hybrid interference by foreign governments.

- The Commission will hold high-level events in autumn with Member States and relevant stakeholders, including the Fundamental Rights Colloquium dedicated to democracy, to promote best practices and guidelines on how to prevent mitigate and respond to cyber-enabled and disinformation threats to elections.

- The High Representative and the Commission will look at ways of better supporting, in terms of tools and resources, the work carried out by the three Stratcom Task Forces in order to ensure EU efforts are sufficiently scaled to address the complexity of disinformation campaigns conducted by hostile actors.

3.4. **Building resilience and deterrence in the cybersecurity sector**

Cybersecurity is critical to both our prosperity and security. As our daily lives and economies become increasingly dependent on digital technologies, we become more and more exposed.

[25] Under the auspices of the Cooperation Group set up under the Directive on the Security of Networks and Information Systems.

www.parlament.gv.at

Effective cybersecurity in the EU today is hindered by insufficient investment and insufficient coordination. The EU is now seeking to address this by building up capacities through support measures, stronger coordination and new structures to advance technology and deployment in cybersecurity[26]. The Directive on the Security of Network and Information Systems[27] established a minimum level of security of network and information systems across the Union. Its full implementation by all Member States is essential to enhance cyber resilience: this is a key first step. The General Data Protection Regulation introduces an obligation to notify personal data breach to the competent supervisory authority. Other key measures include a stronger and modernised European Union Cybersecurity Agency and an EU certification framework for ICT products and services[28] to build consumer confidence. Work on assisting the network of Member States' competence centres to stimulate development and deployment of cybersecurity solutions and complement the capacity building efforts in this area at EU and national level is also ongoing. This will draw on the work of the Digital Europe Programme presented by the Commission on 6 June,[29] which gives a new priority to EU investment in cybersecurity.

At the same time, a Recommendation for Coordinated Response to Large Scale Cybersecurity Incidents and Crises (the "Blueprint")[30] set out how cooperation should work between Member States and various EU actors when responding to a large-scale cross-border cyber-attack. It highlighted the essential role of situational awareness for an effective coordination at technical, operational and strategic/political levels. The Cooperation Group set up under the Directive on the Security of Network and Information Systems is also working to enhance the exchange and sharing of information between relevant parties, developing a common taxonomy to describe an incident. This approach will be tested in upcoming exercises. Strategic analysis of current and emerging cyber threats, based on the contributions of Member States' intelligence services, is provided by the Hybrid Fusion Cell.

The Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the “cyber diplomacy toolbox”) was a major step forward in operational terms, setting out the measures under the Common Foreign and Security Policy, including restrictive measures that can be used to strengthen the EU's response to activities that harm its political, security and economic interests. The more this is used to the full by Member States, the more it will act as an effective deterrent. In April, the Foreign Affairs Council adopted conclusions on malicious cyber activities which firmly condemned the malicious use of information and communications technologies, including in the Wannacry and NotPetya attacks, which have caused significant damage and economic loss in the EU and beyond.

The EU and its Member States need to improve their capacity to attribute cyber-attacks, not the least through enhanced intelligence sharing. Attribution would deter potential aggressors and increase the chances that those responsible will be made properly accountable. Increasing deterrence is a key objective of the Commission's strategic approach towards enhancing cybersecurity. The recent Commission proposals aiming at improving the cross-border gathering of electronic evidence for criminal proceedings would also significantly enhance the ability of law enforcement to investigate and prosecute cybercrime.

---

26 In the framework of strengthening innovation in Europe’s regions, a new inter-regional pilot action gathering EU regions to scale up work in cybersecurity was launched in December 2017.

27 Directive 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.

28 COM (2017) 477.

29 Proposal for a Regulation establishing the Digital Europe programme for the period 2021-2027, COM(2018) 434.

30 C(2017) 6100.

Strong cyber resilience needs a collective and wide-ranging approach. This calls for more robust and effective structures to promote cybersecurity and to respond to cyber-attacks in the Member States also in the EU's own institutions, agencies, delegations, missions and operations: the lack of a joint secure communications network across the European institutions is an important shortcoming. Cyber security awareness in EU institutions and their staff should be increased by an improved security culture and intensified training.

Future Steps

- The European Parliament and the Council should accelerate the work to conclude negotiations on the cybersecurity proposals by agreement by the end of this year, and swiftly agree on the proposed legislation on gathering electronic evidence.

- The Commission and the High Representative will work closely with Member States to advance the cyber aspects of EU-wide crisis management and response mechanisms. Member States are invited to continue their work on attribution of cyber-attacks and the practical use of the cyber diplomacy toolbox to step up the political response to cyber-attacks.

- In response to the need to step up our cyber defence capabilities, a dedicated training and education platform is being set up to help coordinate cyber defence training opportunities offered by Member States. Synergies with similar North Atlantic Treaty Organisation's efforts will be sought.

3.5. **Building resilience to hostile intelligence activity**

Countering hostile intelligence activity requires first and foremost enhanced and effective coordination among Member States, in accordance with relevant EU and national rules and arrangements. It is, however, also imperative to increase the EU institutions' capabilities to counter the growing threat of such activity directed specifically at the institutions and to build a culture of security awareness, supported by improved training and physical security. The institutions could also work with Member States to build a more robust EU accreditation system. Such system would be based on proactive reporting, permitting improved awareness amongst Member States and institutions of possible hostile actors, most notably those already identified by Member States.

Coordination among Member States and between Member States and other relevant international organisations, the North Atlantic Treaty Organisation in particular, would help to leverage the counter-intelligence against hostile activity in the EU. An example of an area which would benefit from increased coordination between Member States is investment screening, on the basis of a Regulation[31] proposed in September 2017 by the Commission for screening of foreign direct investments by Member States on grounds of security or public order. Increased coordination between Member States would be equally important for scrutinising financial transactions, as the hostile intelligence services are increasingly funding their active measures against the EU through elaborate financial schemes.

[31] Proposal for a Regulation of the European Parliament and of the Council establishing a framework for screening of foreign direct investments into the European Union, COM(2017) 487.

Future Steps

- The European External Action Service and the Commission will put in place improved practical measures to sustain and develop the EU's ability to interact with Member States to counter hostile intelligence activity directed specifically at the institutions.
- The enhanced Hybrid Fusion Cell will be complemented by counter-intelligence expertise to provide detailed analyses and briefings on the nature of hostile intelligence activity likely against individuals and the institutions.
- The European Parliament and the Council should accelerate the work to conclude negotiations on the investment screening proposal by the end of the year.

4. CONCLUSION

Hybrid and Chemical, Biological, Radiological and Nuclear-related threats have been high on EU's radar screen. The March incident in the UK underlined the wide spectrum of hybrid warfare and the particular need for resilience in the face of Chemical, Biological, Radiological and Nuclear-related threats.

The Commission and the High Representative have adopted and proposed a number of initiatives to address the challenges posed by hybrid threats. The Commission is also accelerating the implementation of the 2017 Action Plan to enhance preparedness against Chemical, Biological, Radiological and Nuclear security risks.

This Joint Communication serves to inform the European Council of the work already under way and to identify areas where action should be intensified in order to further deepen and strengthen the EU's essential contribution to addressing these threats. It is now up to the Member States, the Commission and the High Representative to ensure swift follow-up.