Council of the European Union

Brussels, 10 December 2019
(OR. en)

14972/19

HYBRID 56	EDUC 478
DISINFO 18	AUDIO 118
AG 68	DIGIT 179
PE 257	INF 332
DATAPROTECT 300	COSI 252
JAI 1307	CSDP/PSDC 575
CYBER 328	COPS 360
JAIEX 177	POLMIL 129
FREMP 176	IPCR 23
RELEX 1147	PROCIV 100
CULT 141	CSC 294

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
Subject:	Complementary efforts to enhance resilience and counter hybrid threats - Council Conclusions (10 December 2019)

Delegations will find attached the Council conclusions on Complementary efforts to enhance resilience and counter hybrid threats adopted at the 3739th meeting of the Council on 10 December 2019.

ANNEX

Council Conclusions on complementary efforts to Enhance Resilience and Counter Hybrid Threats

1. The Council recalls the relevant Conclusions of the European Council[1] and the Council[2] and expresses its continued commitment to strengthening the Union's and its Member States' resilience to multi-faceted and ever-evolving hybrid threats and enhancing cooperation to detect, prevent and counter them.

2. The Council recognises the progress made on the implementation of the Joint Framework on Countering Hybrid Threats (2016) and the Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats (2018) as well as the Action Plan against Disinformation (2018), in line with the relevant Council Conclusions.

3. The primary responsibility for countering hybrid threats lies with the Member States. Efforts at EU level are complementary in nature and without prejudice to Member States' sole responsibility in matters of national security. A comprehensive, whole-of-government and whole-of-society approach to security is necessary to address hybrid threats, working across all relevant policy sectors in a more strategic, coordinated and coherent way. It is important that a whole-of-government approach is followed and applied also at the EU level.

4. In these Conclusions the Council sets out priorities concerning the protection of our societies, citizens and freedoms and the security of our Union against hybrid threats in the context of the implementation of the new Strategic Agenda for 2019-2024, by promoting a comprehensive approach to security with better coordination, resources and technological capacities, building on the important work already done in different policy sectors, including as part of EU security and defence cooperation.

---

1 In particular, the European Council Conclusions of June 2019, March 2019, December 2018, October 2018, June 2018, March 2018, June 2015 and March 2015

2 In particular, ST 10048/19, ST 6573/1/19 REV1, ST 10255/19, ST 12836/19, ST 7928/16

5. Efforts to protect our democratic institutions from hybrid threats must always respect fundamental rights, including the protection of personal data, freedom of expression and information and freedom of association, as enshrined in the Charter of Fundamental Rights.

6. The EU and its Member States should continue to develop, train and exercise capabilities to detect, analyse the sources and respond to hybrid activities and support enhancing the resilience of its Member States and of EU institutions, bodies and agencies to hybrid threats in the long term, taking full advantage of existing instruments suited to that end. The Council stresses the need for updating the EU operational protocol for countering hybrid threats based on lessons identified and learnt from previous exercises.

7. The Council underlines the continuing need to cooperate with international organisations such as the UN, the OSCE and the Council of Europe and formats such as the G7 in order to defend the rules-based global order, also in the context of countering hybrid threats, including through confidence-building and other relevant measures.

8. The Council emphasises the EU's commitment to continue close and mutually reinforcing cooperation with and support to all relevant partner countries, in particular in the EU neighbourhood, on enhancing resilience and countering hybrid threats.

9. The Council calls for continuous and sustained efforts to further progress in the implementation of all actions related to countering hybrid threats under the common set of proposals for the implementation of the Joint Declarations on EU-NATO cooperation, including in the areas of situational awareness, strategic communication, crisis prevention and response and bolstering resilience. In this context, it reiterates the need for further enhancing political dialogue on countering hybrid threats as well as for regular Parallel and Coordinated Exercises (PACE), with the participation of all EU Member States and NATO Allies, and calls for a timely finalisation of the new PACE plan. The Council stresses the need to take into account lessons identified and the importance of unimpeded exchange of information in an inclusive and non-discriminatory manner.

Furthermore, the Council highlights the valuable contributions of the European Centre of Excellence for Countering Hybrid Threats in Helsinki and encourages its cooperation with relevant NATO Centres of Excellence. It also welcomes the regular and structured staff-to-staff exchanges, including the cooperation between the Hybrid Fusion Cell of the EU Intelligence and Situation Centre (INTCEN) and the NATO Hybrid Analysis Branch.

10. The Council acknowledges the efforts of the Member States, in cooperation with the Commission and the European External Action Service (EEAS), in carrying out the Hybrid Risk Survey foreseen in Action 1 of the Joint Framework on Countering Hybrid Threats (2016) and calls for the continuation of the work and a possible revision of the Hybrid Risk Survey in order to better address vulnerabilities.

Working in a coherent way to enhance resilience and counter hybrid threats

11. When developing and using new and emerging technologies, including artificial intelligence and data-gathering techniques, new opportunities for enhancing resilience as well as the potential vulnerabilities and cascading effects in the context of countering hybrid threats, should be duly taken into account in order to reduce overall risks, also in the strategic planning process of the Framework Programme for Research and Innovation.

12. The Council notes that malicious cyber activities can be a part of hybrid threats and in this context underlines the relevance of the EU Cyber Diplomacy Toolbox.

13. The relation between hybrid threats and economic security is a relevant element which should be taken into account and which remains primarily a responsibility of the Member States.

14. New instruments such as the mechanism under the EU Foreign Direct Investment Screening Regulation should be used effectively to enhance resilience and counter hybrid threats by providing means to identify and address foreign direct investments likely to affect security or public order.

15. The Council invites the Commission to include resilience against hybrid threats in the impact assessment process for relevant future legislative proposals including future Framework Programmes for Research and Innovation.

16. The Council underlines the importance of regular exercises and scenario-based discussions on countering hybrid threats at ministerial and other levels, as well as the inclusion of hybrid elements in other relevant EU training and exercise activities at all different levels, with the support of its Member States and the relevant bodies, in particular the European Centre of Excellence for Countering Hybrid Threats, as appropriate.

17. In order to ensure the coherence of the next steps of EU cooperation on enhancing resilience and countering hybrid threats, the Council invites the Commission and the High Representative to produce a mapping that would take into account the measures taken so far and the relevant documents adopted in a comprehensive fashion, with a view to possible new initiatives.

Internal-external security nexus

18. Law enforcement, civil protection and other relevant authorities should continue to develop their preparedness to prevent and counter hybrid threats. Cooperation between relevant national authorities, as well as EU institutions, bodies and agencies across the internal-external security nexus, based on their respective mandates, needs to be continuously improved and mainstreamed while increasing synergies and avoiding duplication of efforts, including through horizontal working methods, voluntary information-exchange, and training and exercises cutting across sectors. To that end, the supporting roles and contributions of relevant EU mechanisms and EU agencies - within their respective mandates and respecting existing budgetary restraints - should be further assessed.

19. The use of relevant EU mechanisms and instruments to support Member States' responses to cross-sectoral and cross-border threats should be further elaborated by the EU institutions and bodies together with the Member States, including the Integrated Political Crisis Response arrangements (IPCR), the Union Civil Protection Mechanism (UCPM) and its Emergency Response Coordination Centre (ERCC).

20. The Council acknowledges the possibility for the Member States to invoke the Solidarity Clause (Article 222 TFEU) in addressing a severe crisis resulting from hybrid activity.

Situational awareness and intelligence analysis

21. EU cooperation on enhancing resilience and countering hybrid threats needs to be guided by a regularly updated threat assessment and a comprehensive situational awareness. These need to be developed by the EU INTCEN and its Hybrid Fusion Cell to enhance the EU's and its Member States' abilities to detect, prevent, disrupt and respond to hybrid activities while respecting the competence of the Member States. The Council considers that the work of the EU Hybrid Fusion Cell should be further enhanced, taking into account an appropriate level of resources including professional expertise.

22. The Council recalls its Conclusions on Countering Hybrid Threats of 19 April 2016 calling for mobilising EU instruments to prevent and counter hybrid threats to the Union and its Member States as well as partners. The Council underlines the need to further develop the Member States and EU's existing situational awareness functions, taking into account the sources of threats, and to make a better use of the intelligence analysis of the EU INTCEN and its Hybrid Fusion Cell, particularly in the EU policy-making and crisis management processes on countering hybrid threats.

23. The Council acknowledges the relevant contribution that CSDP missions and operations could provide, where and as appropriate, in identifying and analysing indicators of possible hybrid third party actions, including disinformation aiming at discrediting and hampering the action of the EU and its Member States, and recognises the value in further exploring the possibility of developing this contribution.

Critical Infrastructure Protection

24. Protecting national and European critical infrastructures as well as functions and services critical to the proper functioning of the State, the economy and society is a key priority including in the context of enhancing resilience to hybrid threats, requiring a whole-of-government-and-society approach. This work needs to take into account the strong interdependencies between different critical functions and services, including financial services, the key role of the private sector, the changing security environment and emerging risks, in both the physical and in the cyber domains.

25. Furthermore, in addition to EU and national legal, regulatory and supervisory requirements governing the operational resilience and business continuity, arrangements with private sector owners and operators of infrastructure and services should be promoted in order to guarantee the continuity of and access to critical services also beyond force majeure, by ensuring an acceptable level of preparedness to respond to all relevant threats as well as flexibility to address, mitigate and recover from high impact-low probability events.

26. The Council emphasises that while the responsibility for critical infrastructure protection is primarily a matter of national competence, the high degree of cross-border and cross-sectoral interdependencies require coordinated or, where necessary, harmonised efforts at the EU level, including in view of the uninterrupted functioning of the internal market.

27. Following the July 2019 evaluation on the implementation of the Directive (2008/114/EC) for the identification and designation of European critical infrastructures (ECIs), the Council invites the Commission to consult with Member States on a possible proposal for a revision of the Directive early in the new legislative cycle, including potential additional measures to enhance the protection and resilience of critical infrastructure in the EU, taking into account the strong interdependencies between critical functions and services.

28. The Council invites the Commission to continue engaging with Member States and, where appropriate, to develop non-binding cooperation arrangements between Member States sharing connected critical infrastructures.

29. The Council recognises the importance of the Directive on security of network and information systems (NIS Directive) for the development of a risk-management and security culture by the operators in critical sectors as well as for national capabilities and strategies ensuring a high level of security of network and information systems in their territory, including in the context of hybrid threats. The Council invites Member States, Commission and the European Union Agency for Cybersecurity (ENISA) to continue developing their cooperation based on the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (Blueprint) at all relevant levels.

Countering disinformation and securing free and fair elections

30. The Council welcomes the Report on the implementation of the Action Plan Against Disinformation and recognises that the Action Plan's continued implementation remains at the heart of the EU's efforts. The Council underlines the need to regularly review and when necessary update the Action Plan to ensure an efficient long-term approach.

31. The Council underlines that the work of the EEAS Strategic Communication Division and in particular the three Task Forces (East, Western Balkans, South) needs to be supported with sufficient resources allowing long-term planning, implementation and evaluation. Among their tasks, all three Task Forces should be able to continuously detect, analyse and challenge disinformation activities of foreign State actors and external non-state actors. The Task Forces should also continue to contribute to effective and fact-based positive communication and promotion of Union principles, values and policies in the EU Eastern and Southern neighbourhood and the Western Balkans and the strengthening of the overall media environment and civil society in their corresponding regions. The Council invites the EEAS to assess needs and the possibilities for reinforcing its strategic communication work in other geographical areas, such as sub-Saharan Africa, while maintaining the necessary capability to carry out the existing strategic communication tasks.

32. The Council recognises that a comprehensive approach at all levels is needed to address the challenges of disinformation, including interference seeking to undermine free and fair European elections, making best use of all available tools online and offline. This must include monitoring and analysis of disinformation and manipulative interference, enforcement of European data protection rules, application of electoral safeguards, efforts to enhance pluralistic media, professional journalism and media literacy as well as awareness among citizens. The Council recommends further consolidation of an active independent cross-European network of fact checkers and researchers against disinformation. The Council recognises the importance of and the role played by civil society, academia and the private sector in addressing disinformation and in building resilience.

33. The Council recognises the potential of the Rapid Alert System (RAS) regarding the fight against disinformation, in particular on election interference. It urges the Commission and the EEAS, together with the Member States, to further develop the RAS towards a comprehensive platform for Member States and EU institutions to enhance cooperation, coordination and information exchange, such as research and analytical insights, best practices, and communication products, to support addressing disinformation campaigns as part of a range of European and national efforts.

34. The Council recognises the usefulness of the measures and recommendations presented by the Commission on 12 September 2018 in its elections package for securing European elections. The Council encourages the Commission and the Member States to examine possibilities to continue the activities of European cooperation networks on elections to support the exchange of information and best practices. The Council welcomes efforts by the Commission to engage all relevant stakeholders and to support a broad range of measures such as the exercise on the cybersecurity of the European Elections (EU ELEx19), taking into account the national competences in this area.

35. The Council acknowledges the need to continue working with social media platforms to achieve higher standards of responsibility, transparency and accountability on addressing disinformation. In addition, unhindered access to anonymised data from social media platform providers for academic research should be granted to facilitate evidence-based policies. The Council invites the Commission to present initiatives on the way forward in addressing disinformation on online platforms. These initiatives should be based on an assessment of the implementation of the Code of Practice on Disinformation, which should take into account the analytical work and reports conducted by academia and civil society organisations, the monitoring report on the Code by the European Regulators Group for Audiovisual Media Services, and also the lessons learned from the European Parliament elections in May 2019. In this context, the Council invites the Commission to consider ways, including possible enforcement mechanisms for online platforms, to further enhance the implementation of the Code of Practice, notably by including an independent assessment of the signatories' compliance with their commitments.

Security of EU institutions, bodies and agencies

36. The security of EU personnel, institutions, bodies and agencies against hybrid threats, and other malicious activities, is an interest shared by the EU and its Member States. The Council calls on the EU institutions, bodies and agencies, supported by the Member States, to ensure the capacity of the Union to protect its integrity and to enhance the security of EU information and communication networks and decision-making processes from malicious activities of all kinds, on the basis of a comprehensive threat assessment. To this end, institutions, bodies and agencies, supported by Member States, should develop and implement a comprehensive set of measures to ensure their security, in accordance with the mandate of the European Council of June 2019. The Council underlines the importance of ensuring interoperability of EU IT infrastructure for the exchange of classified information between EU institutions, bodies, agencies, and Member States.