Council of the
European Union

Brussels, 15 December 2020
(OR. en)

14064/20

HYBRID 47	**EDUC 444**
DISINFO 48	**AUDIO 63**
AG 70	**DIGIT 153**
PE 106	**INF 223**
DATAPROTECT 152	**COSI 251**
JAI 1112	**CSDP/PSDC 643**
CYBER 279	**COPS 480**
JAIEX 120	**POLMIL 199**
FREMP 147	**IPCR 50**
RELEX 1010	**PROCIV 97**
CULT 89	**CSC 362**

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	13626/20
Subject:	Council conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic

Delegations will find in the Annex the abovementioned Council conclusions approved by the Council by written procedure on 15 December 2020.

ANNEX

Draft Council conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic

1. The Council recalls the relevant conclusions of the European Council[1] and the Council[2], and acknowledges that the COVID-19 pandemic highlights the need for intensified efforts and ongoing initiatives to protect the European Union, its Member States and their societies and the EU Institutions from hybrid threats and the harmful effects thereof. Without prejudice to Member States' sole responsibility in matters of national security, the Council notes that:
   - hybrid threats constitute a growing challenge to the EU`s security, stability and common values and principles;
   - hostile state and non-state actors aim to deploy and use less conventional tools in order to disrupt, undermine or delegitimise democracies and democratic institutions, to interfere in electoral processes, to divide populations or to extend their covert influence in general;
   - new technologies and crises such as the ongoing pandemic offer opportunities for hostile actors to expand their interference activities, representing an additional challenge to the Member States and the EU Institutions besides the crisis itself.

2. We must protect our democratic societies and institutions from hybrid threats originating from hostile state and non-state actors. Addressing such threats, including malicious cyber activities, disinformation and threats to economic security requires a comprehensive approach with well-functioning cooperation and coordination.

[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 14972/19, ST 10048/19, ST 6573/1/19 REV1, ST 10255/19, ST 12836/19, ST 7928/16.

At EU level this should include an autonomous analysis capacity, enhanced technological capacities, and the prioritisation of the focus on and redistribution of financial and human resources. The Council acknowledges the progress made on the implementation of the Joint Framework on Countering Hybrid Threats and the Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats as well as on the Action Plan against Disinformation, the Joint Communication on COVID-19 Disinformation and the Free and Fair European Elections Package in line with the relevant Council and European Council conclusions. The Council invites all stakeholders involved to further increase their efforts and support the implementation of the goals defined in the abovementioned documents.

3. The Council acknowledges that the COVID-19 pandemic makes the EU and its Member States more vulnerable to hybrid threats, including via the intensified spread of disinformation and manipulative interference. The attempts are becoming more sophisticated and are increasing in volume. The Council acknowledges that the EU approach to addressing disinformation is multidisciplinary and multi-stakeholder. The Council invites the Commission and the High Representative to:
   - further enhance responses at the EU level, taking into account the economic and societal damage, as well as the possible damage to public health, caused by disinformation and the malign use of newly emerging technologies, including but not limited to artificial intelligence;
   - develop a holistic, systematic and proactive approach to address the phenomena, in particular recognising that, within the context of hybrid threats, foreign interference represents a cross-sectoral challenge, which should be reflected in the efforts of the EU and Member States to address it, ranging from preventive measures, detection, qualification and identification of source, to adequate and effective policy responses that could impose costs on hostile foreign state and non-state actors by building societal resilience, protecting the integrity of public debate and other means.

To this end, the Council stresses the importance of allocating sufficient resources to the relevant EU Institutions and urges the Commission and the High Representative, together with Member States, to continue further strengthening the EEAS Strategic Communication Division Task Forces and developing the Rapid Alert System with a view to developing a comprehensive platform for Member States and EU Institutions. In addition to this and in line with its conclusions of December 2019, the Council invites the High Representative to assess needs and possibilities as regards the reinforcement of its strategic communication activities in all other geographical areas in a balanced way as well as to take into account new emerging hybrid actors, who engage in activities whose aim is to threaten the security of the EU and/or its Member States, while maintaining the necessary capability to carry out the existing strategic communication tasks.

4. The Council welcomes the Assessment of the Implementation and Effectiveness of the Code of Practice on Disinformation.[3] It acknowledges the progress made and underlines the importance of addressing the shortcomings of the Code of Practice identified in the assessment. It considers that the way forward in addressing disinformation at national and EU level could involve a range of approaches, including the possibility of having a regulatory or co-regulatory framework and the means necessary for independent auditing, both by regulators and civil society, notably in terms of data access. On this basis, the Council invites the Commission to develop and eventually implement further transparency requirements for online platforms. The aim of such requirements would be to foster a well-functioning digital public sphere, greater accountability and improved transparency in addressing disinformation. These measures should be based on the primacy of fundamental rights, especially the freedom of expression, as well as democratic public discourse. The Council welcomes the setting in motion last June 2020 of the European Digital Media Observatory and underlines the need for further measures in support of media and digital literacy for all age groups, as well as for media pluralism, media independence and fact checking, with the aim of empowering our societies to counter disinformation and other risks enabled and amplified by new technologies.

[3] Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement, 10 September 2020.

5. The Council takes note of the Commission's European Democracy Action Plan and will examine its content attentively and revert to the issue in the coming months.

6. Dealing with hybrid threats requires comprehensive situational awareness (including the ability to detect, identify and analyse these threats including their source), the strengthening of resilience and measures to counter these threats. This will require actions at national, EU and international level in cooperation with partners, including the private sector and owners and operators of critical infrastructure and services.

   The Council takes note of the work of the Commission together with the European Centre of Excellence for Countering Hybrid Threats on 'The Landscape of Hybrid Threats: A Conceptual Model'[4]. It acknowledges that the conceptualisation of hybrid threats and related terminology is important for their identification with a view to improving coherence between European and national measures to enhance resilience and to counter hybrid threats in a more effective and streamlined manner. The Council invites the Commission and the High Representative to continue their work and to develop the Conceptual Model, informed by the Strategic Compass, and in accordance with the update of Action 1 of the 2016 Joint Framework, with the aim of making it a framework for responses, resilience measures and related resilience indicators, supported by case studies.

   Furthermore, this model could be considered as a guiding tool for the development of future initiatives regarding hybrid threats at European level and taken into account by the Member States when developing their national structures and initiatives. This work could also contribute to the analysis of comprehensive and coordinated responses to hybrid actions, where appropriate, at national and EU level, taking into account the whole possible range of tools.

[4] Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, European Commission, Ispra, 2020, PUBSY No. 117280.

7. The Council takes note of the Commission's 2020 EU Security Union Strategy, which envisages the development of a new, more proactive approach to countering hybrid threats. The Council notes the ongoing efforts as regards the creation of a restricted online platform for Member States' reference on counter-hybrid tools and measures at EU level. The Council agrees with the focus on mainstreaming hybrid considerations into policy-making, further emphasising the need to follow whole-of-government and whole-of-society approaches at national and EU level. Against this background, the Council invites the Commission and the High Representative to play an active role in addressing pan-European vulnerabilities, including the security and resilience of supply chains as part of economic security, and to come forward with initiatives to increase resilience and improve responses as appropriate with due consideration of emerging technologies.

8. The Council recalls that, building on the threat analysis and other possible thematic inputs, the Strategic Compass will define policy orientations and specific goals and objectives in the area of security and defence, including on strengthening resilience and countering hybrid threats.

9. The Council takes note of the fact that the EU Security Union Strategy recognises the Hybrid Fusion Cell of the EU Intelligence and Situation Centre (INTCEN) as the focal point for hybrid threat assessments. The Council invites the High Representative together with the Commission to prepare initiatives on how the Hybrid Fusion Cell, within its mandate, could contribute to streamlining information flows, improving the EU's autonomous analysis capacity and enhancing situational awareness in all domains related to hybrid threats. This includes the voluntary input from Member States and the input from the EU Institutions, agencies and bodies covering hybrid threats. The Council reiterates its position[5] on further enhancing the work of the Hybrid Fusion Cell and calls for it to be provided with additional human resources and funding without prejudice to the needs in other areas of work of INTCEN.

[5] Council conclusions on Complementary efforts to enhance resilience and counter hybrid threats (ST 14972/19)

Further, it calls for the development of a forward-looking hybrid trend analysis capability to analyse hybrid threats, with a strong focus on existing threats, while taking into account emerging hybrid actors and their malicious activities, including those targeting critical infrastructure and employing new technologies.

10. Every ongoing crisis underlines the necessity for safe and resilient information infrastructures between and within the European Institutions, bodies and agencies, including secure communications for Member States within the Council and swift electronic exchange of classified information. The Council calls on the EU Institutions, bodies and agencies to further enhance their security and resilience. In line with previous Council conclusions and in accordance with the mandate given by the European Council of June 2019, the Council strongly encourages them to work together on further strengthening their security culture and the protection of EU personnel, information, communication networks, and decision making processes, with Member States supporting EU Institutions, bodies and agencies in their efforts.

11. In addition to enhancing resilience, which remains one of the most important tasks and is at the heart of European efforts to counter hybrid threats, diplomatic engagement and measures are another effective European tool. The Council will further examine in the coming months possible responses in the field of hybrid threats, which may cover preventive measures as well as the imposition of costs on hostile state and non-state actors.

12. The Council notes that malicious cyber activities are often a key element of hybrid threats and acknowledges the continued implementation of the EU Cyber Diplomacy Toolbox as an important step to prevent, discourage, deter and respond to malicious cyber activities, including those malicious cyber activities that are part of a hybrid campaign.

13. The Council underlines the need to assist the EU Neighbourhood and the Western Balkans[6] in building resilience against disinformation and foreign interference.

14. The Council emphasises the need for cooperation, where appropriate, with like-minded partners who share European values and principles in order to further develop effective measures to address foreign interference and disinformation.

15. The Council also underlines the importance of the effective implementation of the two Joint Declarations on EU-NATO cooperation and the common set of proposals, in full respect of the principles of transparency, reciprocity, inclusiveness and decision-making autonomy and procedures of both organisations, and reiterates, in this framework, the need for enhanced, mutually-reinforcing and beneficial cooperation, including on countering hybrid threats and disinformation. The Council calls for a swift endorsement and implementation of the PACE plan for 2022-2023 and, in this context, reiterates the need for a more ambitious approach in order to strengthen resilience and reinforce synergies between the two organisations as a further step towards their closer interaction in real crisis situations. It also welcomes valuable contributions of the European Centre of Excellence for Countering Hybrid Threats in Helsinki and encourages its cooperation with relevant NATO Centres of Excellence.

16. The Council also stresses the importance of the ongoing contribution that CSDP missions and operations provide, in line with their mandates, in countering hybrid threats, including disinformation, and underlines the value of continued reflection on how CSDP missions and operations could address hybrid threats, including by strengthening their own resilience, as well as by providing support to the host states in this area, where and as appropriate.

---

[6] Zagreb Declaration from 6 May 2020: https://www.consilium.europa.eu/media/43776/zagreb-declaration-en-06052020.pdf