Council of the
European Union

Brussels, 21 June 2022
(OR. en)

10016/22

HYBRID 55	**JAIEX 67**
DISINFO 52	**AUDIO 55**
INST 221	**DIGIT 118**
AG 61	**INF 95**
PE 62	**COSI 160**
DATAPROTECT 185	**CSDP/PSDC 341**
JAI 847	**COPS 255**
CYBER 207	**POLMIL 136**
FREMP 122	**PROCIV 76**
RELEX 758	**IPCR 64**

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
Subject:	Council conclusions on a Framework for a coordinated EU response to hybrid campaigns

Delegations will find in the Annex the above-mentioned Council conclusions approved by the Council on 21 June 2022.

ANNEX

COUNCIL CONCLUSIONS

on a Framework for a coordinated EU response to hybrid campaigns

THE COUNCIL OF THE EUROPEAN UNION,

1. RECALLS the relevant conclusions of the European Council[1] and the Council[2], ACKNOWLEDGES that state and non-state actors are increasingly using hybrid tactics, posing a growing threat to the security of the EU, its Member States and its partners[3]. RECOGNISES that, for some actors applying such tactics, peacetime is a period for covert malign activities, when a conflict can continue or be prepared for in a less open form. EMPHASISES that state actors and non-state actors also use information manipulation and other tactics to interfere in democratic processes and to mislead and deceive citizens. NOTES that Russia's armed aggression against Ukraine is showing the readiness to use the highest level of military force, regardless of legal or humanitarian considerations, combined with hybrid tactics, cyberattacks, foreign information manipulation and interference, economic and energy coercion and an aggressive nuclear rhetoric, and ACKNOWLEDGES the related risks of potential spillover effects in EU neighbourhoods that could harm the interests of the EU.

[1] In particular, the European Council conclusions of December 2021, October 2021, June 2019, March 2019, December 2018, October 2018, June 2018, March 2018, June 2015 and March 2015.
[2] In particular, the conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic (ST 13626/20), the conclusions on complementary efforts to enhance resilience and counter hybrid threats (ST 14972/19), the conclusions on safeguarding a free and pluralistic media system (ST 13260/20), and the conclusions on the European Court of Auditors' Special Report No 09/2021: Disinformation affecting the EU: tackled but not tamed (ST 10968/21).
[3] In line with the Partner chapter of the Strategic Compass.

2. REITERATES that, in the face of the current geopolitical shifts, the strength of our Union lies in unity, solidarity and determination, by enhancing the EU's strategic autonomy and its ability to work with partners to safeguard its values and interests, and by swiftly implementing the Strategic Compass, including to counter hybrid threats and campaigns. UNDERLINES that a stronger and more capable EU in the field of security and defence will contribute positively to global and transatlantic security and is complementary to NATO, which remains the foundation of collective defence for its members. REAFFIRMS the EU's intention to intensify support for the rules-based international order, with the United Nations at its core.

3. RECALLS that the Strategic Compass, approved by the Council on 21 March 2022 and endorsed by the European Council on 24 and 25 March 2022, underlines the need to develop in 2022 an EU Hybrid Toolbox that should bring together existing and possible new instruments and provide a framework for a coordinated response to hybrid campaigns affecting the EU and its Member States, comprising for instance preventive, cooperative, stability, restrictive and recovery measures and strengthening solidarity and mutual assistance, as well as the need to develop in 2022 the Foreign Information Manipulation and Interference Toolbox ('FIMI toolbox'), which will strengthen our ability to detect, analyse and respond to the threat, including by imposing costs on perpetrators. STRESSES that hybrid campaigns will be detected and countered at their early stages using all necessary EU policies and instruments. Thus, for the development of this broad EU Hybrid Toolbox, INTRODUCES a Framework for a coordinated response to hybrid threats and campaigns affecting the EU, Member States and partners, and UNDERLINES that this Framework should also be used to address foreign information manipulation and interference in the information domain (FIMI).

4. NOTES that while definitions of hybrid threats and campaigns may vary, they need to remain flexible in order to allow for proper responses to the evolving nature of the threat. For the purpose of this Framework and to allow it to be used effectively, ACKNOWLEDGES the conceptualisation of 'hybrid threat' and 'hybrid threat campaign' – hereby referred to as 'hybrid campaign' – provided by the Commission and the European Centre of Excellence for Countering Hybrid Threats in 'The Landscape of Hybrid Threats: A Conceptual Model'[4]. UNDERLINES that the Hybrid Risk Survey plays a key role in developing a common understanding and analysis of hybrid threats and campaigns, as well as in identifying vulnerabilities potentially affecting national and pan-European structures and networks, as well as EU partners in neighbourhood regions.

5. EMPHASISES the importance of a strong coordinated response demonstrating EU solidarity in the event of hybrid attacks targeting the EU and its Member States, and STRESSES that the EU Hybrid Toolbox, as well as this Framework, should contribute to responses to hybrid attacks, as appropriate. UNDERLINES the relevance of existing EU crisis management mechanisms, including the Council's Integrated Political Crisis Response (IPCR) arrangements, in supporting coordinated action in response to major, complex crises.

6. UNDERLINES that, as the distinction between internal and external threats is becoming increasingly blurred by actors using hybrid tactics, a comprehensive response to hybrid threats and campaigns should mobilise all relevant internal and external EU policies and tools, as set out in the EU Security Union Strategy 2020-2025, and include all relevant civil and military tools and measures. EMPHASISES the increased need to prevent, detect, mitigate and respond to hybrid threats and activities and that the EU and its Member States should be able to mitigate and terminate the impact of a hybrid campaign at the earliest stage possible and prevent it from developing into a full-fledged crisis, using the full range of the EU's and its Member States' capacities, tools and instruments, in particular those measures that aim to boost the EU's and its Member States' capacity to build resilience, deny perpetrators the benefits of a hybrid campaign and increase the costs for them.

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

EMPHASISES that hybrid campaigns in third countries can also have an impact on EU security, values and interests and that it is therefore important that the EU and its Member States can respond to requests for assistance from partner countries, if appropriate, using this Framework. UNDERLINES that clearly signalling the likely consequences of a coordinated EU response to hybrid campaigns influences the behaviour of potential aggressors and could prevent them from achieving their goals, thus reinforcing the security of the EU and its Member States. STRESSES the importance for the EU and its Member States of developing an adequate posture in this area, based on the work of the relevant Council bodies.

7. UNDERLINES that when one or multiple incidents that could be part of a hybrid campaign have been detected or have been brought to the attention of Member States by the Commission or the High Representative, Member States may request that the relevant Council body examine the issue. EMPHASISES the need for a fast and efficient decision-making process, on a case-by-case basis, to define and approve coordinated EU responses to hybrid campaigns, including FIMI. UNDERLINES that in such cases there is a need for the Council to quickly receive proposals prepared jointly by the Commission and the High Representative and, where relevant, make swift decisions on their implementation based on the support that can be given by the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats to Coreper and, when activated, to the IPCR arrangements. NOTES that the Political and Security Committee (PSC) may deliberate on the measures decided on within this Framework that fall within its mandate.

8. REITERATES that primary responsibility for countering hybrid threats lies with Member States and STRESSES that decisions on a coordinated EU response to hybrid campaigns should be guided by the following main principles:

- serve to protect democratic values, processes and institutions, as well as the integrity and security of the EU, its Member States and their citizens, and its strategic interests, including the security of partners in our neighbourhood and beyond;
- respect international law and protect fundamental rights and freedoms, and support international peace and security;

- provide for the attainment of the objectives of the Union, in particular the Common Foreign and Security Policy (CFSP) objectives, as set out in the Treaty on European Union (TEU), and the objectives set out in Treaty on the Functioning of the European Union (TFEU), as well as the procedures required for their attainment;
- be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of each particular hybrid campaign;
- be based on a shared situational awareness among the Member States and correspond to the needs of the specific situation at hand;
- take into account the broader context of the EU's external relations with the state concerned by the response.

9. INVITES the High Representative – through the Single Intelligence Analysis Capacity (SIAC), in particular the Hybrid Fusion Cell – to continue to provide comprehensive assessments of hybrid threats affecting the EU and its Member States, based primarily on the Member States' contributions, including annual Hybrid Trends Analysis (HTA) reports, and CALLS on Member States and relevant institutions to enhance their participation and contributions to these reports.

10. ENCOURAGES the EU and its Member States to take further action to develop an efficient monitoring mechanism covering various hybrid domains and the variety of hybrid activities taking place in each of them, using new technologies – including artificial intelligence – and mobilising the necessary networks. TAKES NOTE in that regard of the proposal by the High Representative to create an appropriate mechanism to systematically collect data on FIMI incidents, facilitated by a dedicated Data Space. STRESSES the role of CSDP missions and operations in enhancing EU situational awareness by monitoring hybrid threats, in line with their mandate.

11. ENCOURAGES the EU and Member States to collect and decode relevant early signals, exchange information and constantly assess possible links between them in order to characterise a threat quickly; EMPHASISES that Member States and relevant EU institutions, bodies and agencies should enhance their contributions to building shared situational awareness by sharing relevant information through the SIAC – as a single entry point for strategic intelligence contributions from Member States' civilian and military intelligence and security services, through the Rapid Alerts System, by sharing relevant situational updates and by providing their national assessments as part of awareness-raising activities within the relevant Council working party; STRESSES that the SIAC, in particular the Hybrid Fusion Cell, will play a central role contributing to the decision-making process by providing strategic foresight and comprehensive situational awareness, notably to identify the origin and features of the hybrid campaign, provided they have the appropriate resources; and NOTES that this work can be complemented by other relevant EU institutions, bodies and agencies, as well as CSDP missions and operations, as appropriate and at the request of the Council.

12. REITERATES the need to enhance the EU's overall level of resilience to hybrid threats and campaigns, based on a whole-of-society and whole-of-government approach, through the adoption of the Directive on measures to achieve a high common level of cybersecurity across the Union (NIS 2 Directive) and the Directive on the resilience of critical entities (CER Directive), and in the light of the proposed Regulation on the transparency and targeting of political advertising, the Digital Services Act (DSA), the proposed Anti-Coercion Instrument (ACI), the revised Code of Practice on Disinformation, and the implementation of the EU foreign investment screening mechanism, and INVITES Member States, with the support of the Commission, to make the best use of the joint operational mechanism on electoral resilience. ENCOURAGES the Commission to make use of new instruments, including the Observatory of Critical Technologies, to identify dependencies and vulnerabilities that could be used in the framework of hybrid campaigns. INVITES the Commission and the High Representative to identify by the end of 2022, as part of the development of the EU Hybrid Toolbox, operational proposals to bolster societal and economic resilience to hybrid threats, based, where appropriate, on the EU's sectoral hybrid resilience baselines, the Hybrid Risk Survey and the EU Flagship report on resilience.

13. STRESSES that priority should be given to measures aiming to mitigate and terminate the impact of a detected campaign, as well as to prevent its further expansion and escalation, discourage its perpetrator from conducting further action and facilitate the quick recovery of the targeted Member State or EU institution, body or agency. In doing so, ENCOURAGES the Commission and the High Representative to mobilise all the EU's tools and instruments drawing from external and internal policies, in accordance with their respective rules and governance**.**

14. EMPHASISES that when the perpetrator of a hybrid campaign can be identified with a high degree of certainty, asymmetric and proportionate measures in line with international law may be taken – including forms of diplomatic, political, military, economic or strategic communication – to prevent or respond to a hybrid campaign, including in the event of malicious activities that are not classified as internationally unlawful acts but are considered unfriendly acts; AFFIRMS that measures within foreign, security and defence policy, including, if necessary, restrictive measures, are suitable for this Framework and should strengthen prevention, encourage cooperation, facilitate the mitigation of immediate and long-term threats, and influence the behaviour of potential aggressors in the long term; INVITES the Commission and the High Representative to develop options for well-defined measures that could be taken against FIMI actors when this is necessary to protect EU public order and security; and RECALLS that Member States may propose coordinated attribution of hybrid activities, recognising that attribution is a sovereign national prerogative.

15. NOTES that the measures falling within the foreign, security and defence policies can be inter alia preventive measures, including capacity and confidence building measures, exercises and training, including through CSDP missions and operations; cooperative measures, including dialogue, cooperation, coordination, sharing of best practices and training with partner countries and organisations; stability building measures, including public diplomacy and diplomatic engagement with the involved state actor, when and where appropriate in coordination with relevant international organisations and with like-minded partners and countries; restrictive measures (sanctions), including against those responsible for the campaign, according to the relevant provisions of the Treaties; measures to support Member States, upon their request, that choose to exercise their inherent right of individual or collective self-defence as recognised in Article 51 of the Charter of the United Nations and in accordance with international law.

NOTES that those measures include obligations stemming from the Treaty on European Union, such as support in response to the invocation of Article 42(7) of the Treaty on European Union, which stipulates that, if a Member State is a victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States. Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organization, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation.

16. UNDERLINES that the use of military force can be an integral component of some state actors' hybrid tactics and NOTES their readiness to use hybrid tactics combined with or in preparation for or as a substitute for armed aggression. STRESSES the need, in line with the Strategic Compass, to further invest in our mutual assistance under Article 42(7) of the Treaty on European Union as well as solidarity under Article 222 of the Treaty on the Functioning of the European Union, in particular through frequent exercises, to prevent, prepare against, and counter such actions.

17. UNDERLINES that attribution is defined as the practice of assigning responsibility for a malicious hybrid activity to a specific actor; ACKNOWLEDGES that attribution may contribute to building greater resilience, by preparing and educating the public about the threat, and may also help build support for possible further measures; RECALLS that attribution to a state or a non-state actor remains a sovereign political decision based on all-source intelligence and taken on a case-by-case basis; STRESSES that Member States may employ different methods and procedures to attribute malicious hybrid activities, and UNDERLINES that the SIAC plays a key role in supporting Member States in this regard.

18. NOTES that hybrid campaigns are often designed in such a way as to create ambiguity around their origins and to hinder decision-making processes. In that regard, STRESSES that not all measures forming part of a coordinated EU response to hybrid campaigns require responsibility to be assigned to a state or a non-state actor and that measures within the Framework can be tailored to the degree of certainty that can be established in any particular case; UNDERLINES that when coordinated attribution is not possible or public attribution is not in the best interest of the EU and its Member States, well-calibrated asymmetric actions responding to a hybrid campaign against the EU, its Member States or partners, according to this Framework and in accordance with international law, could also be envisaged on a case-by-case basis, upon due approval.

19. ACKNOWLEDGES that malicious cyber activities are often a key element of hybrid campaigns and the continued development of the EU cyber posture is an important step towards preventing, discouraging, deterring and responding to malicious cyber activities, including malicious cyber activities that form part of a hybrid campaign. UNDERLINES that the EU Cyber Diplomacy Toolbox counters cyber security threats and could contribute to the EU response to a hybrid campaign, in line with to its own rules and procedures; STRESSES the need for relevant Council bodies, the High Representative and the Commission to encourage cooperation and synergies in the implementation of measures and actions decided on under this Framework, in particular through the Hybrid Toolbox and FIMI Toolbox, as well as within the EU Cyber Diplomacy Toolbox when and where appropriate.

20. EMPHASISES the need for cooperation and coordinated responses, where appropriate, with like-minded partners when implementing this Framework. STRESSES the importance of further cooperating with relevant international organisations, such as NATO, and like-minded partners and countries, including in the UN and the G7, as well as with civil society and private sector in countering hybrid threats and in view of defining a leading role for the EU in international norm development for countering hybrid threats, including FIMI.

EMPHASIZES in particular the need to develop synergies and explore further avenues for counter-hybrid cooperation with NATO, inter alia by building on the Parallel and Coordinated Exercises organised by the EU and NATO to prepare for tackling complex hybrid attacks, taking into account the shifting geopolitical and technological trends currently underway, in full respect of the principles of transparency, reciprocity and inclusiveness, as well as the decision-making autonomy and procedures of both organisations.

21. STRESSES the need to further develop in 2022 both the EU Hybrid Toolbox and the FIMI Toolbox, in line with the guidance given by the Strategic Compass. INVITES the High Representative and the Commission to continue to identify measures to be implemented within this Framework based on a regular update of the existing mapping[5] and, before the end of 2022, to submit proposals on the creation of EU Hybrid Rapid Response Teams, in order for these to be approved by the Council. INVITES the Commission and the High Representative to conclude the review of the EU operational protocol for countering hybrid threats ('EU Playbook') and present its revised version by the end of 2022. CALLS on the Member States, the Commission and the High Representative to give full effect to the development of the Framework, putting in place implementing guidelines and testing its procedures through existing and new exercises, including exercises involving the activation of Article 222 TFEU and/or Article 42(7) TEU. The Council will TAKE STOCK of the implementation of these conclusions before the end of 2023 and, if necessary, will review the Framework in order to address the evolving threat landscape.

---

[5] JOINT STAFF WORKING DOCUMENT Mapping of measures related to enhancing resilience and countering hybrid threats, SWD(2020) 152 final