Council of the European Union

Brussels, 16 March 2026
(OR. en)

7349/26

HYBRID 36	**POLMIL 123**
DISINFO 26	**COEST 208**
COPS 149	**ELARG 36**
CYBER 121	**AG 47**
JAI 355	**POLMAR 22**
RELEX 363	**TRANS 155**
CFSP/PESC 394	**ESPACE 46**
AVIATION 47	**EU-GNSS 11**
CIVCOM 62	**COMPET 330**

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
Subject:	Council conclusions on advancing the European Union's capacity to counter hybrid threats

Delegations will find in annex the Council Conclusions on advancing the European Union's capacity to counter hybrid threats, approved by the Council at its 4162nd meeting on 16 March 2026.

ANNEX

COUNCIL CONCLUSIONS

on advancing the European Union's capacity to counter hybrid threats

THE COUNCIL OF THE EUROPEAN UNION:

1. RECALLS the European Council[1] and the Council[2] conclusions concerning countering hybrid threats.

2. CONDEMNS persistent hybrid threats by state and non-state actors aimed at undermining the security and stability of the European Union, its Member States, and its partners through coordinated and deliberate campaigns. STRESSES that the Union remains prepared and will act on such threats irrespective of their origin, scale and intensity.

3. In this regard, STRONGLY DENOUNCES sabotage, including against critical infrastructure, malicious cyber activities, foreign information manipulation and interference (FIMI), election interference, and the instrumentalisation of migration.

4. STRONGLY CONDEMNS and HOLDS ACCOUNTABLE the Russian Federation and its proxies for their persistent, coordinated, and long-standing hybrid campaigns aimed at threatening and undermining the security, resilience and democratic foundations of the EU, its Member States and its partners, as well as undermining support to Ukraine and its ability to defend itself. STRESSES that the Union will continue to act with determination through a strategic approach to counter the Russian Federation's hybrid threats and campaigns, which

---

1 In particular, EUCO 24/25(December 2025); EUCO 18/25 (October 2025); EUCO 12/25 (June 2025); EUCO 50/24 (December 2024); EUCO 25/24 (Oct 2024); EUCO 15/24 (June 2024).

2 In particular, Council Conclusions on democratic resilience: safeguarding electoral processes from foreign interference (ST 10119/24); Council conclusions on Foreign Information Manipulation and Interference (FIMI).
(ST 11429/22); Council conclusions on a Framework for a coordinated EU response to hybrid campaigns (ST 10016/22); Council conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic (ST 14064/20).

ensures a proactive, coherent and sustained response, including through asymmetric and proportionate measures in line with international law.

5. REAFFIRMS its determination to use all available tools to prevent, deter and respond to hybrid campaigns and RECALLS that decisions on a coordinated EU response should be aligned with the EU Hybrid Toolbox.[3] STRESSES that any measures and initiatives coordinated or proposed at the EU level must be framed and implemented in full respect of Member States' exclusive competences.

6. STRESSES the importance of coherence and alignment across security-related EU-level initiatives and strategies. REITERATES that the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP ERCHT) must remain duly informed of and actively involved in all actions and policies related to countering hybrid threats, including sectoral and geographic initiatives where appropriate, to fulfil its central coordinating role and ensure fast and efficient decision-making.

7. WELCOMES the progress made and the ongoing implementation of a range of EU measures and initiatives supporting the detection, prevention, resilience, deterrence and response to hybrid threats, as well as support to partners in countering these threats, and cooperation with international organisations and like-minded partners. RECOGNISES the importance of proactive action as deemed appropriate.

8. REAFFIRMS the need to further strengthen the Union's capacity to assess and analyse hybrid threats. RECALLS that the Single Intelligence Analysis Capacity (SIAC) constitutes the EU's integrated intelligence analysis mechanism and serves as the single point of entry for intelligence contributions at EU level for the purposes of situational awareness, early warning, threat analysis and strategic foresight. EMPHASISES, in this context, the central role of SIAC's Hybrid Fusion Cell as designated provider of intelligence for EU-level assessments and analyses of hybrid threats, to support EU decision-making. STRESSES the need to further strengthen SIAC, including the Hybrid Fusion Cell, through reinforcement of resources and capacities as mandated by the Strategic Compass and in accordance with the Joint Paper by

[3] Framework for a Coordinated EU Response to Hybrid Campaigns (ST 10016/22) and its Implementing Guidelines (ST 15880/22).

the High Representative and Member States[4]. UNDERLINES the role of the EU Satellite Centre in enhancing situational awareness in this regard.

9. STRESSES the importance of continued contributions by the Member States' intelligence services to SIAC. ENCOURAGES Member States, relevant EU institutions, bodies and agencies, as well as EU Delegations, and where appropriate and at the request of the Council, CSDP Missions, Initiatives and Operations to contribute to the EU's comprehensive 360° situational awareness of hybrid threats.

10. UNDERLINES the need to further enhance the protection of Member States' critical infrastructure and strengthen their resilience against hybrid threats. CALLS ON Member States to ensure the effective implementation of relevant Union legal acts, in particular the Network and Information Security (NIS2)[5] and the Critical Entities Resilience (CER) Directives[6]. STRESSES that the implementation of the Cyber Blueprint[7] is crucial for the EU's rapid and collective response to large-scale cyber incidents. TAKES STOCK OF ongoing initiatives, including the Preparedness Union Strategy, the European Internal Security Strategy (ProtectEU) and the EU Action Plan on Cable Security, which could contribute further to enhancing the Member States' resilience against hybrid threats.

11. RECALLS that the integrity and resilience of electoral processes are at the core of the EU's democratic foundations and constitute a key target of hybrid campaigns. UNDERLINES that FIMI, along with other hybrid activities, tends to intensify during elections. REITERATES that, in view of upcoming elections across the Union and in partner countries, including candidate countries and potential candidates, continued vigilance, preparedness, and coordination are vital to safeguarding electoral integrity.

---

4 ST 6781/1/24 (R-UE/EU-R).

5 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022.

6 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333, 27.12.2022.

7 Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management, OJ C, C/2025/3445, 20.6.2025.

12. STRESSES that malicious cyber activities often constitute a key component of broader hybrid campaigns targeting the European Union, its Member States and its partners, including activities conducted by non-state actors, acting as proxies on behalf of states; REITERATES the importance of making full use of the Cyber Diplomacy Toolbox to prevent, deter and respond to cyber threats and malicious cyber activities.

13. STRESSES the need to uphold maritime security and REITERATES its full commitment to international law, including international law of the sea as reflected in the United Nations Convention on the Law of the Sea. UNDERLINES the need for the EU to strengthen its collective resilience and preparedness against hybrid threats in the maritime domain, as set forth by the EU Maritime Security Strategy, including by enhancing situational awareness, protecting critical maritime and underwater infrastructure, and ensuring the ability to react rapidly with coordinated civilian and military capabilities.

14. REITERATES[8] its determination to continue and intensify coordinated actions aimed at countering the shadow fleet and its role in sanction circumvention and potentially as a platform for hybrid actions. UNDERLINES the significant risks the shadow fleet poses to maritime safety and security, critical maritime infrastructure and the marine environment.

15. INVITES the Member States to further develop and strengthen joint efforts, in a coordinated manner, and with the support of the High Representative and the Commission, to counter hybrid threats and risks to safety in the air domain, including violation of Member States' Flight Information Region (FIR) and national airspace, as well as disruption of airport operations, through the use of unmanned aircraft systems and other airborne devices, radiofrequency interference, including intentional jamming and spoofing of the Global Navigation Satellite Services (GNSS), cyber-attacks and drone-enabled espionage.

16. NOTES that the affected Member States have raised, in relevant international fora, including the International Civil Aviation Organization (ICAO), the International Maritime Organisation (IMO), and the International Telecommunication Union (ITU), concerns related

---

[8] Declaration of the European Union and its Member States on making full use of the international law of the sea framework relating to threats from the "shadow fleet" and to the protection of critical undersea infrastructure (ST 16829/25).

to airspace and navigation interference, including violations of Member States' flight information regions (FIRs) and ENCOURAGES them to continue doing so in the future.

17. RECOGNISES the value of further EU exercises related to hybrid threats in enhancing Member States' preparedness and the Union's capacity to respond, in line with the EU exercise policy framework. REITERATES, in line with the Strategic Compass, the need to further invest in our mutual assistance under Article 42(7) of the Treaty on European Union and mutual solidarity under Article 222 of the Treaty on the Functioning of the European Union, in particular through frequent exercises.

18. WELCOMES the establishment, operationalisation and successful deployments of the EU Hybrid Rapid Response Teams and RECOGNISES their added value in supporting Member States, partners and CSDP missions and operations at their request, in countering hybrid threats.

19. INVITES the High Representative and the Commission, in close cooperation with Member States and on a case-by-case basis, to present further actor-specific strategic approaches based on intelligence-backed assessments provided by SIAC and in line with the EU Hybrid Toolbox.

20. REITERATES the Union's determination to steadily increase the costs of hybrid activity for those responsible, including those who act as proxies on behalf of state actors, by making full use of existing and dedicated tools, including the EU's frameworks of restrictive measures in response to Russia's destabilising activities and against cyber-attacks threatening the Union or its Member States.[9]

21. INVITES the EEAS and the Commission services, in coordination with Member States in the relevant Council preparatory bodies, to identify and discuss potential gaps and options to further strengthen the EU's restrictive measures in response to hybrid threats, including the possible establishment of a horizontal EU restrictive measures framework.

22. INVITES the Commission to discuss with Member States the improvement of the Hybrid Risk Survey, including by ensuring that the results are taken into account when preparing

---

[9] Restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 129I 17.5.2019 p.1; OJ L 129I 17.5.2019, p. 13); Restrictive measures in view of Russia's destabilising activities (OJ L 2642 9.10.2024, p. 1; OJ L 2643 9.10.2024, p. 1).

future Union legislative and non-legislative activities, proposals and strategies countering vulnerabilities to hybrid threats.

23. UNDERLINES the increasing and potential future malign use of critical and emerging technologies including artificial intelligence, quantum technologies and distributed ledger technologies for hybrid campaigns. ACKNOWLEDGES that these technologies also provide opportunities for countering and mitigating hybrid threats, including for early-detection and analysis.

24. CONDEMNS the use of online platforms by malicious actors for hybrid activities, including FIMI campaigns as well as the planning, coordination, recruitment for and execution of hybrid attacks. INVITES the Commission and the High Representative, where applicable, to make the full use of the relevant Union instruments, including through the full implementation and enforcement of the Digital Services Act, to address these activities, and to share relevant developments with the Council. In this context, CALLS ON online platforms to enhance cooperation with the EU and the Member States and implement ambitious and robust measures to counter such activities.

25. WELCOMES the work done by the EEAS in monitoring, detecting and responding to FIMI campaigns and coordinating with international partners in this regard. UNDERLINES the relevance of the Rapid Alert System and the need to further strengthen it and increase its impact, including through close cooperation with HWP ERCHT.

26 WELCOMES the presentation of the Joint Communication "European Democracy Shield: Empowering Strong and Resilient Democracies".[10] TAKES NOTE of the establishment of the European Centre for Democratic Resilience and UNDERLINES its commitment to work together with the Commission and the EEAS to enhance the Union's democratic resilience.

27. INVITES the High Representative and the Commission to put forward options for the consideration of the Council concerning the announced Blueprint for Countering FIMI and enhancing the EEAS' capabilities to counter FIMI campaigns against the EU and its Member States in view of the rapidly changing threat landscape and the expanded set of threat actors targeting the EU and its Member States based on a mapping of existing EU efforts to avoid

---

10 JOIN(2025) 791 final.

duplications. RECALLS that the Framework for a coordinated response to hybrid campaigns, as outlined in the Council conclusions of 21 June 2022,[11] should also be used to address FIMI.

28 INVITES the High Representative and the Commission, in close cooperation with Member States, to continue developing and deploying proactive and tailored strategic communication campaigns to be implemented in a coordinated manner by EU institutions and Member States to highlight and counter FIMI targeting the EU and its Member States, and promote and defend EU democratic values in third countries, in particular candidate countries and potential candidates, and in the information space of hybrid actors.

29. WELCOMES that all CSDP missions and operations have been equipped with FIMI monitoring tools, and STRESSES that they should continue to be regularly trained on detection and receive operational and analytical support to build their resilience and address FIMI threats more effectively on the ground.[12] ACKNOWLEDGES the EU Cyber Defence Coordination Centre (EU CDCC) as a key initiative to support CSDP missions and operations on cyber situational awareness.

30. UNDERLINES the role of Member States and relevant EU institutions in raising public awareness within Member States on hybrid threats to enhance societal preparedness and resilience.

31. REITERATES the need to further strengthen cooperation and synergies with the private sector, academia and civil society, with a view to strengthening resilience, deterrence, detection, analysis, and response to hybrid threats, in full respect of applicable law and national competences.

32. EMPHASISES the importance of continued action by Member States and relevant EU institutions to strengthen public resilience to FIMI, including through measures to foster a well-informed and critically engaged public, improve media literacy and digital skills, and promote fact-checking initiatives, in full respect of human rights and fundamental freedoms and with continued strong emphasis on promoting freedom of expression, independent media, and the protection and safety of journalists and human rights defenders.

---

11 ST 10016/22.

12 In line with the Strategic Compass for Security and Defence tasking.

33. REITERATES the importance of close cooperation with international partners and organisations, to enhance situational awareness and to prevent, deter and better respond to hybrid threats, including through coordinated messaging, diplomatic action and imposition of restrictive measures. RECOGNISES the importance of continuing and reinforcing support to partners, in particular candidate countries and potential candidates, affected by hybrid threats. ACKNOWLEDGES the value of deepening bilateral sectoral dialogues and consultations with like-minded partners on relevant topics related to hybrid threats, especially within the framework of Security and Defence Partnerships, while keeping Member States duly involved in the preparation of these dialogues and informed of their outcome.

34. UNDERLINES the importance of ensuring coherence and further strengthening the mutually beneficial cooperation in countering hybrid threats between the EU and NATO - recalling that NATO remains the foundation of collective defence for its members.-REAFFIRMS the significance of the EU-NATO Parallel and Coordinated Exercises (PACE) framework in this regard. EU-NATO cooperation will be taken forward within the framework of the three Joint Declarations,[13] in full respect of the agreed guiding principles of reciprocity, transparency, inclusiveness and of both organisations' decision-making autonomy and procedures.

35. WELCOMES the contribution of CSDP Missions, Initiatives and Operations to enhancing hosting countries' resilience and response to hybrid threats, including FIMI. WELCOMES the work of the European Union Partnership Mission (EUPM) in Moldova in strengthening Moldova's resilience against hybrid threats and INVITES the High Representative to draw lessons from the experiences of EUPM Moldova, and explore how these can be implemented in other CSDP theatres and in assistance of other partners where relevant. CALLS for further cooperation and exchange of lessons learned with like-minded partners including Moldova and Ukraine.

36 EXPECTS candidate countries and potential candidates to fully align with the EU Common Foreign and Security Policy (CFSP), including restrictive measures, which is a key aspect of the EU integration process.

37. STRESSES the importance of further coordination with G7 and other like-minded partners on restrictive measures, and of further reinforcing anti-circumvention measures.

---

13 EU-NATO Joint Declarations of 10 January 2023, 10 July 2018 and 8 July 2016.

38. INVITES the EU institutions, bodies and agencies, supported by Member States, as well as EU Delegations and CSDP Missions, Initiatives and Operations to enhance their preparedness and resilience to hybrid threats by strengthening and regularly adapting training and capacity- building, and by continuing to enhance security measures relating to personnel, rapid and classified communications, information systems and counter- intelligence, in line with existing EU security and resilience frameworks and respective mandates.

39. RECOGNISES the efforts of the European Union Institute for Security Studies (EUISS), the European Security and Defence College (ESDC), and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in providing training related to hybrid threats and sharing of knowledge and best practices.

40. UNDERLINES the importance of reviewing the implementation of these conclusions on a regular basis.