European Parliament
2024-2029

TEXTS ADOPTED

P10_TA(2026)0303

Hybrid warfare and the protection of the EU's territorial integrity and critical security and defence infrastructure

European Parliament resolution of 16 September 2026 on Hybrid warfare and the protection of the EU's territorial integrity and critical security and defence infrastructure (2026/2024(INI))

The European Parliament,

– having regard to the UN Charter and the fundamental principles of international law,

– having regard to Title V of the Treaty on European Union (TEU), in particular Chapter Two, Section Two thereof on provisions on the common security and defence policy,

– having regard to the Treaty on the Functioning of the European Union (TFEU),

– having regard to Articles 42(7) and 222 TEU,

– having regard to its previous resolutions on Ukraine, Russia and Belarus, in particular those adopted since Russia's annexation of the Crimean Peninsula in February 2014 and Russia's full-scale invasion of Ukraine in February 2022,

– having regard to the international legal framework for preventing and fighting terrorism, including UN Security Council Resolution 2341 on protection of critical infrastructure against terrorist acts, adopted on 13 February 2017,

– having regard to Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union[1],

– having regard to the 'Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests

[1] OJ L 79I 21.3.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/452/oj.

and contributes to international peace and security', approved by the Council on 21 March 2022 and endorsed by the European Council on 25 March 2022,

– having regard to the Council conclusions of 21 June 2022 on a framework for a coordinated EU response to hybrid campaigns,

– having regard to 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[2],

– having regard to the Final Assessment Report of 29 June 2023 by the NATO-EU Task Force on the Resilience of Critical Infrastructure,

– having regard to the report of 30 October 2024 by Sauli Niinistö entitled 'Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness' (Niinistö report),

– having regard to the Commission communication of 11 December 2024 on countering hybrid threats from the weaponisation of migration and strengthening security at the EU's external borders (COM(2024)0570),

– having regard to Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services[3],

– having regard to Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)[4],

– having regard to the joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 21 February 2025 entitled 'EU Action Plan on Cable Security' (JOIN(2025)0009),

– having regard to its resolution of 12 March 2025 on the white paper on the future of European defence[5],

– having regard to the joint white paper from the Commission and the High Representative of the Union for Foreign Affairs and Security

---

2 OJ L 333, 27.12.2022, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj.

3 OJ L, 2025/37, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/37/oj.

4 OJ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

5 OJ C, C/2025/3151, 20.6.2025, ELI: http://data.europa.eu/eli/C/2025/3151/oj.

Policy of 19 March 2025 entitled ‘Joint White Paper for European Defence Readiness 2030’ (JOIN(2025)0120),

– having regard to the joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 26 March 2025 on the European Preparedness Union Strategy (JOIN(2025)0130)),

– having regard to the Commission communication of 1 April 2025 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy (COM(2025)0148),

– having regard to the Declaration of the North Atlantic Council Summit in The Hague, adopted by the Heads of State and Government participating in the meeting of the North Atlantic Council on 25 June 2025,

– having regard to its resolution of 9 October 2025 on a united response to recent Russian violations of the EU Member States’ airspace and critical infrastructure[6],

– having regard to the non-paper of November 2025 by the Italian Minister of Defence entitled ‘Countering hybrid warfare: an active strategy’,

– having regard to the Commission proposal of 10 December 2025 for guidelines for trans-European energy infrastructure (COM(2025)1006),

– having regard to its resolution of 18 December 2025 on the continuous Belarusian hybrid attacks against Lithuania[7],

– having regard to the Commission communication of 18 February 2026 on the EU’s eastern regions bordering Russia, Belarus and Ukraine (COM(2026)0082),

– having regard to its resolution of 21 January 2026 on the implementation of the common security and defence policy – annual report 2025[8],

– having regard to the Council conclusions of 16 March 2026 on advancing the European Union’s capacity to counter hybrid threats,

– having regard to Rule 55 of its Rules of Procedure,

---

6 OJ C, C/2026/1530, 15.4.2026, ELI: http://data.europa.eu/eli/C/2026/1530/oj.

7 OJ C, C/2026/2161, 6.5.2026, ELI: http://data.europa.eu/eli/C/2026/2161/oj.

8 Texts adopted, P10_TA(2026)0013.

– having regard to the report of the Committee on Security and Defence (A10-0212/2026),

– having regard to the Declaration of the North Atlantic Council Summit adopted by the Heads of State and Government participating in the meeting of the North Atlantic Council in Ankara on 8 July 2026,

A. whereas the intensity and scope of hybrid attacks against the EU have escalated significantly since the start of Russia’s war of aggression against Ukraine, with incidents repeatedly linked to authoritarian states, notably Russia, Belarus, China, Iran and North Korea;

B. whereas Russia constitutes the primary and most significant security threat to the EU and its Member States; whereas Russia has persistently violated the principle of territorial integrity and political independence set forth in Article 2(4) of the UN Charter; whereas hybrid attacks represent a threat to democracy in the EU and its Member States;

C. whereas the severity of these attacks has increased drastically and constitute a blatant violation of Member States’ sovereignty, the EU’s territorial integrity and international law; whereas hybrid warfare has become a structural feature of the current geopolitical environment;

D. whereas recent hybrid attacks can include unauthorised drone incursions, ‘smuggling balloons’, airspace violations, clandestine tunnels for infiltration and smuggling, sabotage of and espionage targeting critical security and defence infrastructure, the sabotage of undersea cables and energy infrastructure, GPS jamming and navigation spoofing, cyberattacks, arson and assassination plots, the instrumentalisation of migration and organised crime, elite capture, covert foreign investment, economic coercion, data exfiltration and other acts of political subversion and economic penetration, foreign information manipulation and interference (FIMI), and interference in political and electoral processes;

E. whereas, in the summer of 2026, the EU witnessed an intensification of physical hybrid activities and attacks across EU territory; whereas this included an attempted explosive drone attack targeting Ukrainian cargo aircraft at Leipzig/Halle Airport in Germany, an attempted attack by an explosive-laden maritime drone against a Romanian offshore gas project, a foiled Russian-directed sabotage and espionage plot targeting military infrastructure and Ukrainian cargo aircraft in Romania, an arson attack targeting a defence contractor in Estonia, deliberate sabotage and arson attacks targeting defence and drone manufacturing facilities in Poland, a Russian cruise missile violating Polish airspace and crashing in the

Lublin region, and a foiled arson plot in Slovakia targeting a Ukrainian drone manufacturer; whereas the Leipzig/Halle Airport attack, the targeting of the Romanian offshore gas project and the sabotage plot targeting military infrastructure and Ukrainian cargo aircraft in Romania have been publicly attributed to Russia by the respective national authorities; whereas following the attack on Leipzig/Halle Airport, the German authorities closed the Russian consulate in Bonn and the Russian House in Berlin;

F. whereas the sovereignty and territorial integrity of all Member States are foundational principles of the EU; whereas hostile state actors, in particular Russia, target the EU's territorial integrity on two fronts: through direct physical attacks against Member States and through influence operations aimed at undermining the unity of the EU, by engineering Member States' withdrawal from the EU;

G. whereas hybrid threats increasingly affect the EU as a whole, including overseas countries and territories such as Greenland, but the EU's external border regions and the EU's maritime areas are particularly susceptible to attacks; whereas these attacks also target candidate countries and EU neighbours, notably Ukraine, Moldova, Armenia, Georgia and the Western Balkans; whereas the territorial integrity of the EU's neighbourhood is key to ensure peace, stability and security in Europe and the wider world;

H. whereas interference in Greenland by non-EU countries, notably inflammatory narratives and the conduct of hybrid actions on Greenland's territory, as well as the US Government's formulation of explicit threats against Greenland's sovereignty, have raised concerns regarding Greenland's sovereignty and territorial integrity;

I. whereas Georgia is an example of successful Russian hybrid interference resulting in Kremlin-aligned Georgian Dream-led authorities replicating Russia's playbook of hybrid operations against Georgia's own civil society and democratic institutions;

J. whereas sabotage activities by Russian intelligence are increasingly being carried out using intermediaries, vulnerable social groups, including underaged persons, proxies and 'disposable agents', thereby complicating attribution and response; whereas religious institutions, including the Russian Orthodox Church and networks linked to the Muslim Brotherhood, have been exploited to conduct interference operations in the EU, undermining democratic values, the rule of law and the EU's ability to defend itself;

K. whereas these attacks aim not only to create chaos and destabilise the EU Member States, but also to undermine democratic integrity, manipulate decision-making processes, deepen political divisions, weaken social cohesion, sow fear and public distrust among EU citizens, and weaken defence readiness and the EU's support for

Ukraine, generating cascade effects across the EU;

L. whereas the invocation of NATO Article 5 following the 9/11 terrorist attacks demonstrates that collective defence can be triggered following attacks not only by the actions of a state actor but also by attacks involving non-state actors and complex networks operating across national borders; whereas this precedent highlights the evolving nature of security threats and the need to adapt collective response mechanisms accordingly, including with improved common standards and procedures for attribution;

M. whereas there has been a drastic increase in cognitive warfare together with FIMI; whereas, according to the European External Action Service (EEAS) 4th Annual Report on FIMI Threats, Russian FIMI activity is expected to intensify in 2026, with the budget for state-controlled media projected to reach approximately EUR 1,56 billion, 7 % higher than in 2025, with the Baltic Sea and Arctic regions anticipated to be among the primary targets;

N. whereas FIMI operations use sophisticated cognitive-psychological methods, including reflexive control, a technique rooted in Soviet military theory that introduces specific informational inputs to limit a target’s perceived choices and steer decisions toward the influencer’s strategic goals;

O. whereas Russia’s 2015 and 2021 national security strategies frame the promotion of so-called traditional values and the ‘Russian World’ as instruments of its broader hybrid warfare strategy and geopolitical influence; whereas Russia has strategically deployed historical, religious, cultural and values-based narratives as part of its hybrid warfare strategy to influence public discourse, and ecclesiastical dynamics, weaken social cohesion, and undermine democratic resilience and Transatlantic integration;

P. whereas the transversal nature of the cognitive domain requires cognitive indicators to be fully integrated into the common operational picture used by cyber, intelligence, law enforcement, military and critical infrastructure structures;

Q. whereas the success of modern military operations and the effectiveness of public institutions increasingly depend on the control of cyberspace and on the strategic use of digital resources and information systems;

R. whereas internal security remains a responsibility of the Member States, although the cross-border, interconnected and multi-dimensional nature of those hybrid attacks requires strengthened cooperation, systematic information sharing and coordinated action at EU level, supported by adequate funding and complemented by long-term strategies to strengthen societal resilience and protect institutional integrity;

S. whereas EU Justice and Home Affairs (JHA) agencies have a key role to play in cooperation with national authorities, in establishing and maintaining common situational awareness of risks related to such threats and in assisting front-line Member States in crisis situations; whereas the Commission has included the strengthening of the European Border and Coast Guard Agency (Frontex) in its flagship initiatives for the 2024-2029 legislative terms, as well as a revision of the mandates of European Union Agency for Law Enforcement Cooperation (Europol) and European Union Agency for Criminal Justice Cooperation (Eurojust); whereas other initiatives such as the ‘Eastern Flank Watch’ may contribute to strengthening the protection of the external borders and increasing resilience against hybrid threats;

T. whereas the emergence of advanced AI systems represents a structural disruption to existing cybersecurity architectures, invalidating threat models and defensive assumptions developed over previous decades; whereas hostile state and non-state actors are already exploiting AI capabilities to increase the speed, scale and precision of hybrid operations, including cyber intrusions, AI poisoning, disinformation campaigns and critical infrastructure targeting; whereas the EU’s collective cyber resilience frameworks must be adapted to address these new vulnerabilities;

U. whereas despite the significant efforts undertaken by Member States, and the development of tools and mechanisms to counter hybrid threats, the EU’s response to hybrid attacks continues to suffer from legislative gaps, the lack of a harmonised approach among Member States, differing levels of awareness, and the absence of a dedicated structure or entity to monitor such attacks; whereas as a consequence, despite the urgency, EU Member States have yet to develop a fully coordinated and coherent response to hybrid warfare both individually, at European level and, where relevant, with NATO;

V. whereas national defence spending would benefit from increased coordination and pooling between Member States or further investment in European collaborative projects; whereas significant increases in Member States’ defence spending, in combination with the EU’s defence initiatives such as SAFE and other measures under the Defence Readiness 2030 framework, are beginning to address long-standing capability shortfalls, but a faster translation into concrete operational capabilities is needed to better protect the EU, its Member States and their citizens against hybrid threats; whereas in this area further potential remains for dual-use technologies; whereas further response is equally required in the area of internal security;

W. whereas responsibility for national security remains primarily with the Member States and any measures and initiatives coordinated or

proposed at EU level must be framed and implemented in full respect of Member States' exclusive competences and aligned with the EU Hybrid, FIMI and Cyber Diplomacy Toolboxes;

X. whereas the EU's dependence on foreign actors and foreign-made technologies in critical infrastructure and supply chains, including the sourcing of raw materials from third countries, is one of the EU's most significant vulnerabilities and a key challenge for European security and strategic autonomy;

Y. whereas the current security environment confronting the EU is characterised by neither peace nor open armed conflict, but phase zero warfare in which adversaries deploy hybrid instruments to exploit the gap between the EU's peacetime governance structures and the decisiveness required to deter and respond; whereas existing EU foreign and security policy frameworks, calibrated for consensus-based deliberation, generate structural latency that adversaries actively exploit; whereas this in-between state demands a fundamental reassessment of EU decision-making architecture in the security and defence domain;

Z. whereas the credibility of deterrence rests not only on the material capabilities and technological edge of the European and allied forces, but decisively on political will, strategic cohesion and a common understanding of the threat; whereas Russia's hybrid strategy is calibrated to erode precisely these qualities – through ambiguity, division and sub-threshold pressure – in order to degrade the credibility of collective defence commitments before any kinetic threshold is reached;

Hybrid warfare: between war and peace

1. Stresses that hybrid operations are deliberate, combined, intelligence-led and coordinated acts by states – including through non-state actors, intermediaries and proxies – spanning multiple domains simultaneously; stresses that they are designed to appear as isolated incidents and remain below the threshold of armed conflict, while having the potential to produce effects comparable to conventional aggression, thus making attribution and an effective response significantly harder; calls therefore on the EU and the Member States to recognise that hybrid acts can constitute a form of warfare regardless of whether conventional force is employed;

2. Underlines that the primary objective of hybrid warfare is to destabilise, divide and undermine the EU and its Member States by exploiting systemic vulnerabilities, and weakening their security, resilience and democratic foundations, and their defence readiness by disrupting the EU's defence industrial base and critical infrastructure undermining public and political support for EU defence, and by strengthening political forces favourable to the

perpetrators through systematic interference in democratic processes;

3. Affirms that Russia, acting directly or via multiple proxies such as Belarus, is the gravest hybrid-threat state actor targeting the EU and its Member States; notes that China, Iran, North Korea and others have been implementing hybrid campaigns aimed at undermining European democracies and eroding the EU's security interests; underlines that the EU must adopt a comprehensive approach to hybrid threats that addresses not only Russian and Belarusian activities but also the growing strategic role of China, Iran and North Korea in enabling and amplifying hostile actions against European interests and security; notes with concern that non-state actors – including terrorist groups, organised crime networks, oligarchic and kleptocratic networks, religious institutions and faith networks, private military companies, extremist movements and influence-for-hire operators – may also conduct or enable hybrid campaigns against European democracies;

4. Calls on the Commission and the Council to assess the adequacy of existing EU legal frameworks for addressing hybrid threats, close identified gaps, and treat sub-threshold hybrid operations that cannot be addressed through law enforcement alone as collective security matters, requiring a combined civil-military response;

Information warfare, cognitive security and societal resilience

5. Underlines that information warfare is one of the core elements of hybrid warfare; expresses concern at the growing scale of cognitive warfare together with FIMI, which aims to erode societal trust in democratic institutions, increase polarisation, undermine democratic decision-making and public support for European security and defence, including support for Ukraine;

6. Highlights that the above-mentioned objectives (see paragraph 5) are predominantly being pursued through sophisticated and coordinated operations spanning multiple domains of social life and employing strategic cognitive and psychological techniques designed to shape decision-making processes, individual and collective perceptions, identity formation, cultural norms, historical memory, moral frameworks and religious belief systems, while exploiting technological infrastructure, media ecosystems and economic and political vulnerabilities; notes with concern that FIMI operations employ sophisticated cognitive-psychological methods, including reflexive control, which are difficult to detect, attribute or counter through conventional responses; stresses therefore that the EU FIMI toolkit must explicitly integrate countermeasures against such advanced influence techniques in order to safeguard the integrity of EU decision-making;

7. Warns that individual kinetic incidents may either trigger or be deliberately engineered to provide cover for immediate, synchronised and orchestrated FIMI operations, with hostile actors exploiting the gap before official statements are issued to shape public perception; calls for this information gap to be duly addressed through enhanced European coordination, in particular by improving public-private coordination in the information domain; stresses the need to develop common tools such as communication playbooks enabling faster, coordinated and accurate communication before hostile narratives saturate the information space;

8. Expresses concern about Russia's use of historical revisionism, in particular regarding the Second World War and the Soviet legacy, FIMI, and the selective reinterpretation of historical events as tools of hybrid warfare aimed at polarising public opinion, undermining societal cohesion and democratic resilience, and delegitimising the territorial integrity of sovereign states;

9. Underlines that FIMI extends beyond traditional media into educational, cultural and religious domains; highlights the strategic use of religious institutions and faith networks, including the instrumentalisation of the Russian Orthodox Church, to project moral authority, disseminate state-sponsored narratives, and gradually undermine societal resilience and democratic cohesion; calls furthermore on the EU to detect hybrid threats exploiting religious channels, and train EU officials in interfaith engagement and religious literacy, and in the identification of financial influence, organisational capture and information manipulation that undermine democratic values and social cohesion;

10. Condemns the use of online platforms by hostile actors for hybrid activities; calls for stronger enforcement of existing EU rules on the transparency of recommendation systems, political advertising, coordinated inauthentic behaviour and the rapid dissemination of manipulated or AI-generated content linked to hostile foreign interference;

11. Underlines that hostile actors employ increasingly sophisticated and adaptive hybrid techniques; highlights that AI tools – deepfakes, algorithmic amplification and automated account networks – make influence operations faster, cheaper and harder to detect; considers that the EU response to AI-enabled FIMI must treat AI as both a threat vector and as a critical defence capability;

12. Notes that the EU's response to FIMI remains reactive, lacking real-time monitoring, attribution and proactive response capabilities; insists that FIMI must be treated as a serious security threat requiring an operational approach, better coordination and cooperation between Member States at all levels, including early

detection, adequate response options and stronger protection of democratic processes, particularly during electoral periods;

13. Welcomes the EEAS's work in monitoring, detecting and responding to FIMI and underlines the relevance of the EU's Rapid Alert System (RAS) for coordinated joint responses to disinformation; invites the Commission and the Member States to assess and build on the recommendations of the Special Committee on the European Democracy Shield (EUDS); calls for the RAS to be further strengthened to address information manipulation in real time with clear operational responsibilities; calls for standardised pre-bunking and rapid-response mechanisms across the EU and with partner countries, including structured early-warning communication channels; encourages the development of proactive strategic communication tools capable of warning populations in advance about anticipated disinformation tactics, narrative patterns and fabricated content ahead of critical events such as elections, energy negotiations or security crises;

14. Calls, furthermore, on the Commission, the High Representative and the Member States to fully operationalise and make consistent and coordinated use of the FIMI Toolbox and to apply the FIMI Deterrence Playbook, including through coordinated public attribution and, where appropriate, the use of restrictive measures, targeting not only individual incidents but the illicit financial flows, technical infrastructure, and intermediary and proxy networks that sustain FIMI operations;

15. Stresses that European public opinion remains a primary target of Russian hybrid operations; recalls that decades of peace have created conditions of strategic complacency that adversary influence operations exploit and deepen; considers that governments and EU institutions share responsibility to build public understanding of the nature and proximity of the hybrid threat, and that the failure to do so undermines preparedness and deterrence from within;

16. Calls on the Member States to adopt whole-of-government and whole-of-society approaches, prioritising resilience and preparedness as emphasised in the Niinistö report; recalls that hybrid threats target society as a whole, as hostile actors exploit vulnerabilities across interconnected domains, services, communities and information spaces; believes that trust and social cohesion are fundamental to societal resilience; underlines, therefore, that resilience against hybrid threats must extend beyond military, technical and institutional measures by bringing together public authorities, the private sector, civil society – including local communities and constituencies that are hard to reach – academia and independent media to strengthen democratic trust, public awareness and societal preparedness, thereby fostering a new European security culture;

17. Stresses the need to strengthen public resilience to FIMI through civic education, media literacy, strategic communications, support to independent media including investigative journalism, fact-checking networks such as the European Digital Media Observatory, and AI-enabled tools to detect and analyse disinformation campaigns at scale; calls for stronger cooperation with media and audiovisual actors in detecting, attributing and responding to FIMI; calls for incentivising, including through public-private initiatives, the detection, analysis and attribution of FIMI, secure data-sharing mechanisms and interoperable early-warning systems;

18. Expresses concern over continuous reports of foreign interference in European elections, including through cyberattacks and AI-enabled disinformation; recalls that the integrity and resilience of electoral processes are central to the EU's democratic foundations and a key target of hybrid operations; underlines that FIMI tends to intensify before elections and that continued vigilance and coordination are therefore essential to safeguard electoral integrity and democratic stability across the EU and in partner countries, including candidate and potential candidate countries; welcomes the Joint Communication 'European Democracy Shield: Empowering Strong and Resilient Democracies' and the establishment of the European Centre for Democratic Resilience and calls for a clear definition of its tasks to avoid duplication with existing initiatives;

19. Calls for recognising and addressing cognitive vulnerabilities in the context of hybrid warfare in the upcoming EU security strategy and for the Commission to take further steps by providing cognitive vulnerability mapping and resilience benchmarks;

Cybersecurity

20. Stresses that cyberattacks have become a central element of hybrid campaigns, exploiting the increasing digitalisation of critical sectors such as healthcare, finance and energy, causing cascading disruptions with potentially severe economic and societal consequences;

21. Notes that cyberspace has become established as the fifth military domain and as a central enabler of hybrid threats; underlines that the growing dependence of military platforms, critical infrastructure and command, control, communications and intelligence systems on digital technologies makes cybersecurity essential to operational superiority and resilience across all domains; stresses, therefore, the need for sovereign cyber capabilities for detection, attribution, response and intelligence, including offensive capabilities to neutralise threats and ensure credible deterrence;

22. Underlines the convergence between FIMI and cybersecurity, noting that cyberattacks often occur at the early stages of FIMI campaigns;

calls for counter-FIMI mechanisms to be systematically connected with cybersecurity capabilities in order to detect, attribute and disrupt coordinated manipulation infrastructure at an early stage;

23. Warns of the risks posed by convergent cyber operations, in which state-aligned actors actively adopt the operational profiles, methodologies and personas of independent hacktivists or commercially motivated cybercriminals to conceal attribution and align cyber activity with geopolitical events, elections or kinetic operations; stresses that responses to hybrid cyber threats must clearly distinguish between legitimate forms of political expression or civil dissent and financially motivated cybercrime and state-sponsored operations, so as to protect fundamental freedoms while improving attribution, accountability and deterrence;

24. Warns that the expansion of the Internet of Things increases the risk that cyberattacks generate physical effects in critical infrastructure and essential services, and calls for security-by-design obligations to ensure connected devices do not become entry points for hybrid operations with real-world consequences;

25. Warns that full cyber protection does not exist and that a shift in mindset towards cyber resilience is needed; stresses that Europe’s cyber resilience must be built up through frequent and realistic cyber exercises; underlines that cyber resilience not only concerns systems, but also data protection, which is both a target and an enabler of hybrid threats; underlines further the need to strengthen cyber resilience across the European economic fabric, including small and medium-size enterprises (SMEs) and providers of essential digital services;

26. Stresses the EU’s added value in helping Member States to connect national capabilities, build common situational awareness and enable faster, more coherent responses to hybrid threats; recommends that the Commission explore proposals for a more unified framework to support Member States in the planning, operational coordination and execution of cyber operations; welcomes the completion of the Permanent Structured Cooperation (PESCO) project on the Cyber and Information Domain Coordination Centre (CIDCC) and the progress towards its transition into a permanent EU Cyber Defence Coordination Centre (EU CDCC);

27. Calls for greater harmonisation of incident-reporting obligations and key legal concepts across EU cybersecurity and resilience frameworks, to reduce fragmentation, improve interoperability and ensure that rapid restoration of essential services remains a central priority in hybrid crisis scenarios;

28. Recognises the EU Cybersecurity Reserve, managed by the European Union Agency for Cybersecurity (ENISA) under the Cyber Solidarity

Act, as a strategic EU cyber rapid-response capacity; calls for its funding to be adapted to operational demand and highlights its first deployment in Moldova as an important step in strengthening the EU's operational cyber resilience and support to partner countries; calls on Member States' cybersecurity authorities to foster structured cooperation with the Reserve's trusted providers to make full use of available incident response capabilities when hybrid threats materialise through significant or large-scale cyber incidents;

29. Reaffirms the importance and calls for adequate EU resourcing of the PESCO Cyber Rapid Response Teams as a standing cyber defence capability, deployable upon request from Member States, partner countries and common security and defence policy (CSDP) missions facing cyber attacks with implications for security and defence;

30. Reiterates the importance of making full use of the Cyber Diplomacy Toolbox to prevent, deter and respond to cyber threats and malicious cyber activities; takes note of the launch in March 2026 of the first permanent UN Global Mechanism on cybersecurity, and believes that the EU should focus on areas where there is clear European added value while further strengthening European cyber diplomacy;

31. Stresses that cyber resilience and defensive measures are insufficient to ensure credible deterrence against hybrid threats as highlighted in the Joint White Paper for European Defence Readiness 2030; calls on the Commission and the Member States in cooperation with NATO to examine the legal, procedural and operational prerequisites for proportionate, legally compliant cyber countermeasures; welcomes the progress made towards the establishment of the EU CDCC and calls for its swift operationalisation and for the implementation of a mandate in line with the Council conclusions on the EU Policy on Cyber Defence, in order to achieve a more credible and capable EU cyber defence;

32. Warns in this regard that AI is not only a tool used in hybrid cyber activities, but is also a critical technology that can itself be targeted, manipulated or compromised through prompt injection, training data poisoning and supply-chain attacks; stresses that, given the growing reliance on commercial and dual-use AI systems in civilian, security and defence contexts, the EU must develop a clear position on the cybersecurity, resilience and governance of dual-use AI, including safeguards for model integrity, trusted supply chains and oversight at the boundary between civilian, defence and national security applications;

33. Stresses the need for increased protection of critical public digital infrastructure and sensitive state-managed data registers, including electoral infrastructure, as they form potential targets of hybrid threats, given their role in digital identity, public administration,

data governance, secure communications, access to essential services and the integrity of democratic processes;

Critical infrastructure

34. Condemns the hybrid attacks targeting the EU's critical infrastructure – in particular energy, transport, communications and satellite infrastructure, including that for military mobility – both critical enablers and strategic assets for the EU's collective defence, resilience and civilian protection; highlights that this critical infrastructure performs as an interconnected system that cannot be protected in isolation, and that greater digital connectivity increases vulnerability; welcomes the focus on the protection and resilience of energy and military mobility infrastructure in the Commission proposal for a regulation on military mobility (COM(2025)0847) and the Commission proposal for guidelines for trans-European energy infrastructure (COM(2025)1006); calls on the Commission and the Member States to take all necessary measures to ensure its protection;

35. Underlines that the space domain has become an increasingly important arena for hybrid warfare, with hostile actors targeting satellite-based communications, navigation and observation systems through cyber operations, physical attacks, jamming and spoofing or the exploitation of strategic dependencies; stresses that disruption of space assets can have significant consequences for the EU's civil security, critical infrastructure, military mobility and crisis-response capabilities; calls, therefore, for stronger resilience of EU space systems, including increased space situational awareness, protection of ground infrastructure, cybersecurity requirements, supply-chain security, regular exercises and alternative or backup positioning, navigation and timing (PNT) capabilities; calls further for the integration of the space domain into the EU's broader framework for countering hybrid threats;

36. Notes that hostile actors, mainly Russia, are increasingly weaponising energy infrastructure, energy markets and energy dependencies to exert political pressure; emphasises the strategic importance of critical energy infrastructure for both defence and civil needs; urges the Commission and the EU Member States to establish an EU legal and financial framework under the next multiannual financial framework 2028-2034 that would ensure sufficient protection and resilience of critical energy infrastructure, prioritising Commission proposals for guidelines for trans-European energy infrastructure (COM(2025)1006) and the Connecting Europe Facility (COM(2025)0547);

37. Condemns Russia's shadow fleet activities that increase the risk of maritime accidents, conceal state-linked sabotage, and jeopardise critical infrastructure such as undersea cables, offshore energy

installations and port facilities; calls for enhanced monitoring, inspection and enforcement measures in European waters and for the EU to step up its response to hybrid threats in maritime zones; encourages the Commission to explore – drawing on the Proliferation Security Initiative as a model – legal and operational frameworks to enable the boarding of vessels linked to shadow fleets, and calls on the Financial Action Task Force to further examine the role of opaque ownership structures, flag registries and associated financial networks in facilitating the circumvention of sanctions and illicit financial flows;

38. Stresses that undersea cables are a key strategic vulnerability and target of hybrid sabotage, espionage and influence operations due to their physical exposure and systemic disruption potential as they carry the vast majority of intercontinental internet traffic; commends the 2024 Commission Recommendation on Secure and Resilient Submarine Cable Infrastructures[9] and the 2025 Joint communication on the EU action plan on cable security (JOIN(2025)0009) as important first steps towards strengthening the security and resilience of submarine cable infrastructure; calls further for maritime domain awareness capabilities, integrating satellite, surface and subsea sensor data to detect, monitor and attribute physical threats to submarine cable and offshore energy infrastructure in strategic maritime areas, including the Baltic Sea, North Sea, Black Sea, and Arctic and Mediterranean regions; recommends strong criminal liability provisions to deter such attacks and redundant systems to ensure resilience; stresses further the need for a comprehensive, multilayered approach combining technological innovation, enhanced intelligence integration, improved attribution capabilities, and strengthened cooperation between NATO, the EU Member States, and relevant private-sector actors in order to ensure coherent protection of undersea infrastructure;

39. Calls on the Commission and the Member States to establish a coordinated, EU-wide interpretation of the United Nations Convention on the Law of the Sea (UNCLOS) in order to ensure coherent action against and effective criminalisation and deterrence of hybrid activities, acts of sabotage and violations of sovereign rights in the EU’s maritime areas, notably in the Baltic Sea, while recalling UNCLOS’s objective of ensuring the peaceful use of the seas; encourages the Commission and the Member States to draw on the Australian example of establishing ‘cable protection zones’, providing legal safeguards and criminalising damage to submarine cables beyond the 12-nautical-mile territorial sea limit, accompanied

---

9 Commission Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures (OJ L, 2024/779, 8.3.2024, ELI: http://data.europa.eu/eli/reco/2024/779/oj).

by active monitoring, surveillance and response in cooperation with relevant third-country partners;

40. Calls on the Member States and the European Defence Agency (EDA) to advance the PESCO projects Critical Seabed Infrastructure Protection (CSIP), Harbour & Maritime Surveillance and Protection (HARMSPRO), Integrated Multi-Layer Air and Missile Defence System (IMLAMD) and Counter Unmanned Aerial System (C-UAS) to boost surveillance, detection and defence capabilities against airborne and maritime threats; calls on the Commission, in cooperation with the High Representative and in consultation with the Member States, to propose a European defence project of common interest dedicated to the integrated defence of the maritime environment and the seabed;

41. Welcomes the adoption of the Critical Entities Resilience (CER) Directive[10] and the NIS2 Directive[11] as important steps towards strengthening resilience against hybrid attacks, but stresses that implementation delays across the Member States represent a shared urgent vulnerability and calls for their full and timely implementation; urges the Commission to make full use of its monitoring and enforcement powers; calls on the Member States to embed resilience by design as a standard requirement in all new and revised legislation;

42. Expresses concern over foreign ownership of critical infrastructure in the EU, in particular by Russia and China, which greatly increases the risk of espionage and interference and strategic dependence; welcomes the political agreement reached between Parliament and the Council on a strengthened EU foreign direct investment (FDI) screening mechanism; calls on the Member States to rapidly implement this regulation, complemented by a ‘Buy European’ approach, where possible, for critical infrastructure and defence equipment with a view to strengthening the EU’s strategic autonomy;

43. Recognises that a significant share of critical infrastructure linked to essential public services and military capabilities is privately owned or operated; calls for permanent and structured public-private cooperation frameworks, including for information sharing,

---

10 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, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

11 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, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

contingency planning and coordinated crisis response; stresses that, where private infrastructure supports essential services and sensitive data, public authorities must ensure effective regulatory and operational control; calls for defence requirements to be systematically integrated into civilian infrastructure planning, design and funding; insists that EU-funded infrastructure must comply with defence-relevant resilience standards as a condition for EU support; calls furthermore for defence technology developers and security providers to be systematically involved in the early phases of critical infrastructure threat assessment and contingency planning, ensuring that available technological capabilities are reflected in national and EU resilience frameworks; recognises the contribution of SMEs, start-ups and innovative technology providers to the resilience and protection of critical infrastructure and calls for their increased participation in relevant EU programmes, procurement schemes and public-private partnerships;

44. Calls on the Member States to conduct regular preparedness and resilience exercises for critical infrastructure, including joint exercises, and urgently deliver the priority capabilities identified in the White Paper for European Defence, in particular air and missile defence, drones and counter-drone systems, military mobility, cyber, and electronic warfare and maritime capabilities;

45. Is concerned about the EU’s structural dependence on high-risk non-EU countries, particularly China, for the supply of network-connected hardware and software assets, such as solar inverters, wind turbines, connected vehicles, and consumer digital devices, that can access, transmit or control systems remotely and therefore form a significant vulnerability; calls on the Commission to extend supply chain security assessments systematically, across all critical infrastructure sectors, and to accelerate efforts to reduce strategic dependencies; calls on the Member States to follow up on these assessments, diversify supply chains and prioritise European and like-minded suppliers in strategic sectors whenever security considerations so require; welcomes the fact that the proposed revision of the Cybersecurity Act aims to provide a framework to ban network-connected components from high-risk suppliers, and that the Strategic Roadmap for Digitalisation and AI in the Energy Sector – as part of the European Technological Sovereignty Package – provides for a review of the energy security-of-supply framework; calls for these measures to be adopted swiftly;

46. Stresses the importance of diversifying supply routes through secure and resilient transport networks with trusted partners in order to reduce strategic dependencies and strengthen the EU’s economic security and supply chain resilience;

47. Stresses that critical and emerging technologies – including AI, cloud infrastructure, advanced semiconductors, quantum technologies,

cyber, space, autonomous systems and secure communications – are part of the EU's critical security infrastructure given their essential role in defence readiness, economic resilience and operational continuity; considers a resilient, competitive EU digital infrastructure – including secure local data centres, sovereign EU cloud, edge computing, and gigabit networks – an important pillar of European security; stresses that the EU's ability to detect, withstand and respond to hybrid campaigns depends on its capacity to develop, secure and scale these technologies within a resilient European industrial and technological base supported by sufficient EU investment, including investment in secure, interoperable and resilient information-sharing systems and local data centres not subject to extraterritorial legislation;

Situational awareness

48. Stresses that effective countering of hybrid threats requires prevention, early threat anticipation, and continuous monitoring of strategic vulnerabilities to neutralise hostile actions before they have systemic effects and a shared threat picture, as targeted sectors cannot respond effectively on the basis of isolated incident reports; highlights in this regard the EU's potential unique added value in aggregating cross-border data to detect patterns of coordinated hybrid campaigns that no Member State can identify on its own, as well as in coordinating the development of procedures for joint situational awareness and attribution, common frameworks, methodologies, taxonomies and interoperability protocols between EU and national relevant bodies and structures that would support operational cooperation between the Member States; calls for these functions to be formally recognised as EU coordination and support competences;

49. Notes that the EU Hybrid Fusion Cell within the Single Intelligence Analysis Capacity (SIAC) remains the EU's central body of exclusive expertise on all-sources analysis of hybrid threats providing intelligence-based situational awareness; reiterates that SIAC should be the single hub for intelligence in the EU institutions and underlines its special status within the EU security architecture; endorses the Hybrid Trend Analysis as a key tool for analysing hybrid threats and detecting patterns, and its proper involvement in the policymaking processes;

50. Recalls the lack of progress in fulfilling the goal set out in the Strategic Compass and the Joint Paper by the High Representative and the Member States on Strengthening the EU Single Intelligence Analysis Capacity (EEAS(2024)2014), to strengthen SIAC by providing additional resources to compile, analyse and integrate relevant information in order to produce and facilitate efficient provision of intelligence in the areas of cyber and hybrid threats posed to the EU; calls on the Commission, the High Representative

and the Member States to make a firm commitment to the effective strengthening of SIAC;

51. Urges the Member States to increase intelligence sharing, including with EU INTCEN and the European Union Military Staff (EUMS) Intelligence Directorate, while respecting the sovereignty of the Member States, the need-to-know principle, and the protection of national classified information; stresses that data-driven, intelligence-based assessments must be systematically incorporated into EU planning, crisis management and policymaking;

52. Calls on the EU institutions, in cooperation with the Member States and the EEAS, to explore a secure – need-to-know and need-to-share – information-sharing system, whereby the EU would act as a facilitator connecting public authorities, relevant EU, national and international bodies, critical infrastructure operators, private companies, and trusted threat-information sources, in order to strengthen collective situational awareness while ensuring the utmost protection of sensitive information; believes that such a system would incentivise participating bodies to share information by enabling them to benefit from a more complete threat picture and higher-quality intelligence products, while progressively building the trust required for meaningful information sharing;

53. Calls for the establishment of a ‘Black Book of Hybrid Aggression by Russia, China and others’ in order to publicly document every hybrid operation against the EU and its Member States from the past 10 years; insists that the ‘Black Book’ be discussed in the Council and presented to Parliament annually in order to impose further costs on the states in question;

From fragmentation to a coordinated and decisive European response

54. Underlines that only through deeper integration, coordination, increased European defence readiness and capabilities, including through further developing the European Defence Technological and Industrial Base, can the EU respond effectively to escalating hybrid and conventional threats;

55. Considers that the EU must move from a reactive to a proactive strategy, which includes using its capabilities to disrupt, deter and respond to hybrid threats and credibly raise the cost of hostile action; stresses that any violation of the Member States’ sovereignty must be met with effective, proportionate and coordinated retaliation measures;

56. Stresses that to effectively counter and deter hybrid threats a shared and comprehensive threat picture is required, which depends on common frameworks, methodologies, taxonomies and operational standards; highlights the need to combine diplomatic, legal,

economic and restrictive measures to prevent, detect, identify, attribute and respond to hybrid operations including through asymmetric measures across all relevant domains; calls on the Commission, the High Representative and the Council to develop a cross-domain action plan against hybrid warfare, including strengthened civil-military cooperation, operational playbooks, collaborative and efficient response protocols, including calibrated EU retaliatory options proportionate to the severity of hostile activities and clear response chains that are interoperable with and complement those of NATO, while preserving the capacity of the EU and the Member States to act independently if necessary; calls for the designation of a single point of coordination between the Commission and the EEAS in order to establish a genuine whole-of-EU approach to hybrid threats;

57. Welcomes the ongoing initiatives to strengthen operational capacity, including EU Hybrid Rapid Response Teams and the launch of the EU's Eastern Flank Watch and the European Drone Defence Initiative; calls for swift progress in their deployment; stresses the strategic importance of regional defence and security clusters and calls for dedicated EU funding lines to integrate their know-how and capabilities into cross-border projects that increase European resilience;

58. Welcomes the Commission's and the High Representative's announcement of a new global EU security strategy and calls for it to comprehensively address the full spectrum of hybrid threats;

59. Insists on the need to urgently advance towards a genuine European Defence Union, as a stronger European pillar of NATO, separable but not separate, enabling the EU and its Member States to act independently when necessary; calls for the mutual defence clause (Article 42(7) TEU) to be further operationalised in armed aggression and severe hybrid scenarios; calls further for an Article 42.7 playbook – a concise but comprehensive operational guide for national governments and EU institutions, explaining what happens before, during and after a Member State invokes the Article; suggests that the playbook be tested regularly in severe hybrid crisis scenarios and through comprehensive cross-sectoral exercises;

60. Stresses that some of Russia's hybrid attacks against the EU and its Member States may amount to state-sponsored terrorism; encourages the Member States to use all available legal tools to counter them, including the solidarity clause (Article 222 TFEU), making full use of the cooperation and coordination mechanisms made available when the clause is activated;

61. Welcomes the work done under existing sanctions regimes targeting hybrid activities, in particular the sanctions regime established in October 2024 targeting Russia's destabilising activities and the

horizontal cyber sanctions regime established in 2019; deplores the fact that the EU sanctions framework is complex and fragmented across different hybrid threat vectors; calls for further strengthening the EU's restrictive measures in response to hybrid threats, including the immediate establishment of a horizontal EU sanctions framework – specifically designed for hybrid threats in order to fill the gaps in existing regimes and increase the deterrent effect – which would exist alongside the Russia hybrid sanctions regime to underscore Russia's active engagement in hybrid operations globally while enabling faster and more systematic sanctioning of entities responsible for hybrid campaigns; calls for the EU Hybrid, FIMI and Cyber Diplomacy Toolboxes to be further strengthened and used more effectively;

62. Reiterates the need to ensure accountability for hybrid operations and for those responsible, including proxies acting on behalf of state actors, by making full use of existing and dedicated tools; calls on the EU and the Member States to take urgent action to halt and disrupt the financial flows that fund attacks on democracy, including by mobilising banking regulators, criminal investigators and sanctions authorities to trace and examine illicit sources of financing, including cryptocurrency; calls on the EU and the Member States to break the financial and algorithmic incentives that allow disinformation to thrive, including by addressing the links between illicit funding, advertising revenues, attention-driven platform business models and manipulative content;

63. Takes the view that all criminal law tools available at Member State and EU level should be applied and, where appropriate, further developed to prevent and counter illegal conduct aimed at undermining democratic institutions and processes; stresses the need for competent national authorities to be equipped with adequate tools and cooperation channels to prevent, investigate, detect and prosecute criminal offences related to foreign interference; considers that corruption and intimidation of elected and public officials by criminal networks should be addressed as part of the EU's response to hybrid threats via strengthened cooperation between specialised anti-corruption agencies, law enforcement authorities and relevant EU bodies; asks the Commission to assess the added value of establishing minimum rules in EU law on the definition of and sanctions for the criminal offence of knowingly participating in organised activities of interference on behalf of foreign powers; notes that the forthcoming revision of the mandates for EU justice and home affairs agencies provides an opportunity to strengthen the EU's operational response capacity; calls on the Commission to explore the idea of convening a platform or task force for the Member States to voluntarily coordinate national legislative responses and share best practices;

Geographical considerations

64. Strongly condemns the instrumentalisation of migration by third countries or hostile non-state actors in order to destabilise a Member State or put pressure on the EU; notes the specific provisions on the instrumentalisation of migration recently included in key pieces of EU legislation; notes the Commission’s announced revision of the mandate for Frontex; underlines that this revision should provide for the legal basis, analytical capabilities, and adequate human, financial and technical resources required, which would also help strengthen the EU’s response to hybrid threats;

65. Strongly condemns the assault on the EU’s southern border in the city of Ceuta, carried out on 30 and 31 July 2026, as well as the subsequent invasion of Ceuta, constituting an attack on the territorial integrity and sovereignty of a Member State; deplores the use of irregular migration flows as an instrument of hybrid warfare directed against the stability and security of a Member State, and therefore calls for an independent and comprehensive investigation to clarify responsibility for the planning and execution of this attack and identify the objectives pursued;

66. Condemns Russia’s systematic drone incursions and cross-border provocations targeting the Member States along the EU’s eastern flank as a calculated campaign of intimidation against civilian populations; welcomes the Commission communication on the EU’s eastern regions bordering Russia, Belarus and Ukraine, and its explicit recognition that the EU’s eastern border regions face structural and sustained threats from Russia and Belarus; calls on the Commission to translate this recognition into dedicated funding streams under the 2028-2034 multiannual financial framework, including dedicated funding to enhance integrated border protection capabilities, modernise physical and digital border surveillance infrastructure – in line with NATO standards – at the EU’s external land borders; underlines that focus should be placed on advanced detection, monitoring and countermeasure systems against unmanned aerial systems to protect critical infrastructure such as airports, energy facilities, and transport hubs and support the Member States in deploying interoperable airspace awareness systems, electronic protection measures, and rapid incident response capacities; stresses that measures must be proportionate, defensive, and civilian-protection-oriented, ensuring continuity of essential services and freedom of movement within the Schengen area;

67. Stresses that hybrid threats increasingly affect the EU as a whole, while taking different forms across regions; underlines, in this regard, the exposure of the Baltic, Nordic-Baltic and Black Sea regions to threats against maritime and airspace security, as well as instrumentalised migration, the vulnerability of Mediterranean and southern border regions to threats targeting maritime infrastructure, energy networks, logistics corridors, strategic transport routes, disinformation campaigns and the instrumentalisation of migration

flows, the exposure of south-eastern Europe to economic coercion, energy dependencies and coordinated information manipulation linked to neighbouring theatres, the specific vulnerability of major urban and digital information spaces across the EU to cognitive warfare, polarisation and foreign interference; underlines the growing strategic significance of the Arctic region for European security, including the protection of critical infrastructure, freedom of navigation, satellite communications and emerging transport corridors; calls on the EU and NATO to reflect the geography of hybrid threats in their strategies, including the upcoming EU security strategy, while maintaining a 360º security approach to resilience, preparedness and response; stresses that funding to counter hybrid threats should be based on strategic exposure, operational needs and demonstrated vulnerabilities, while ensuring support for all regions facing hybrid threats;

EU and NATO coordination and cooperation

68. Reaffirms that NATO remains the cornerstone of collective defence for its members; calls for increased EU-NATO cooperation to strengthen European preparedness, resilience and deterrence against hybrid threats; highlights in this regard the importance of critical infrastructure protection, military mobility, cyber resilience and preparedness; highlights the need for a more systematic exchange of lessons learned from the war in Ukraine in the hybrid domain;

69. Stresses that EU and NATO action in the hybrid domain must be complementary, mutually reinforcing and operationally coordinated, while ensuring the EU’s capacity to act when required, against the backdrop of the alignment of EU minimum preparedness requirements with NATO baseline requirements;

70. Notes that NATO’s 2025 revised hybrid strategy marks a shift from resilience to active deterrence; welcomes the pre-agreed Military Response Options and expanded authorities of the Supreme Allied Commander Europe (SACEUR) to enable faster action at the start of a hybrid attack, reducing delays between threat detection and response while preserving political oversight;

71. Welcomes NATO’s Hybrid Tracking Mechanism, an intelligence aggregation tool via NATO’s Joint Intelligence and Security Division, which provides allies with a consolidated threat picture, drawing on national intelligence services; recognises the ongoing cooperation between NATO and the EU in the intelligence domain, and calls on the Commission and the EEAS to establish a structured interface within the Hybrid Fusion Cell with this mechanism so that EU situational awareness and NATO’s hybrid threat picture are regularly and systematically aligned;

72. Stresses the important role of NATO’s Arctic Sentry, Baltic Sentry and Eastern Sentry as agile instruments in responding to hybrid threats within operationally relevant time frames, especially regarding the protection of maritime critical infrastructure and supply routes, and the monitoring of hybrid activities in those regions; notes that their effectiveness is constrained by the high cost of intercepting drones, gaps in situational awareness and the fragmentation of counter-drone regulatory frameworks across the Member States; calls for the implementation of the EU action plan on drone and counter-drone security to be accelerated, including the provision of dedicated funding for layered defence capabilities in front-line Member States to combat meteorological balloons and drones kinetically and electronically, and for the action plan’s systematic alignment with NATO operational requirements, ensuring harmonised, adequately resourced counter-drone capabilities across the Member States; further supports greater cooperation in the development and deployment of cost-effective counter-drone technologies across the EU;

73. Welcomes the EU–NATO Parallel and Coordinated Exercises (PACE) framework as a valuable instrument for testing and improving joint response capacity, scale, and scope and for the systematic integration of lessons learned into EU policy, planning and institutional arrangements; calls for regular EU and NATO exercises simulating hybrid attack scenarios, including sabotage against military mobility infrastructure, coordinated cyberattacks, large-scale FIMI campaigns, airspace violations and attacks on critical infrastructure;

74. Calls on the Commission, the EEAS, in close coordination with NATO and the Member States, to develop a common understanding of hybrid threats and to establish a coherent response mechanism for the EU and NATO;

75. Recognises the valuable role played by specialised centres of excellence, including the European Centre of Excellence for Countering Hybrid Threats in Helsinki and the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, in strengthening preparedness, resilience, cyber defence and counter-hybrid capabilities across Europe; further welcomes the work of the EU-NATO Task Force on the Resilience of Critical Infrastructure, particularly in strengthening cooperation on energy, transport, digital infrastructure and undersea connectivity;

76. Calls on the Member States to harmonise their laws in closing the legal gaps preventing allied personnel from participating in below-threshold hybrid response operations; welcomes Estonia’s recently adopted amendments to its Defence Forces Organisation Act as a concrete step in this direction;

Partner countries: cooperation and support

77. Underlines that Russian hybrid operations beyond the EU aim to shift the foreign policies of third countries in line with Moscow's interests, undermine the EU's relationships with its partners and weaken international support for Ukraine; reiterates, therefore, the importance of close cooperation with international partners and organisations to enhance situational awareness and to prevent, deter and respond more effectively to hybrid threats; acknowledges the value of deepening bilateral sectoral dialogues and consultations with like-minded partners on hybrid threats, especially within the framework of security and defence partnerships;

78. Emphasises that strengthened cooperation with Ukraine, Moldova, Armenia and partners in the Western Balkan is a strategic necessity, as they face continuous attacks from Russia and form key testing grounds for Russia's hybrid tactics, combining FIMI, cyber operations, covert influence networks, energy coercion, and corruption-based leverage to undermine democratic institutions, societal cohesion, and EU and NATO integration prospects; calls on the Member States to adopt lessons learned from these countries and establish structured mechanisms for the systematic exchange of best practices and operational experience, including on Ukraine's capacity to maintain essential services, continuity of government, protection of critical infrastructure, strategic communication and societal functioning and resilience under sustained attack; reiterates its strong support for Ukraine's progressive accession to the EU and accession to NATO once the relevant conditions have been fulfilled;

79. Highlights the strategic importance of continuing and deepening hybrid resilience support to candidate, potential candidate and partner countries, who are often primary targets of Russian hybrid activities and whose resilience directly contributes to the security of the EU; welcomes the EU's and the Member States' active contribution to strengthening their resilience through the Foreign Policy Instrument, strategic communications, Hybrid Rapid Response Teams, the Hybrid Risk Survey and CSDP missions in partner countries including Ukraine, Moldova, Armenia and Montenegro; calls for the organisation of regular joint exercises, simulation scenarios and training programmes aimed at enhancing preparedness, improving rapid response capacities and fostering interoperability in addressing hybrid threats; notes with appreciation the coordinated EU-NATO response in Moldova, including the parallel deployment of an EU Hybrid Response Team and a NATO Counter Hybrid Support Team with complementary mandates; encourages candidate countries and potential candidates to fully align with the EU common foreign and security policy (CFSP), including restrictive measures, as a key aspect of the EU integration process;

80. Commends Moldova’s and Armenia’s pro-European forces for their democratic resilience during and in the lead-up to their 2025 and 2026 parliamentary elections, demonstrating strong resistance to Russia’s sustained years-long FIMI campaigns; underlines the effectiveness of the whole-of-government approach as an operational model, including its use of law enforcement action against networks conducting hybrid operations on behalf of Russia; calls on the Member States and the Commission, in cooperation with the EEAS, to develop EU-level frameworks enabling comparable enforcement responses; notes the important role played by EU institutions, state institutions, civil society, and independent media in countering FIMI, including AI-enabled large-scale coordinated information manipulation campaigns contributing to the notably high level of public awareness of hybrid threats;

81. Calls for reinforced cooperation on hybrid threats with like-minded non-EU partners, in particular the United Kingdom and Norway, as key European security partners, as well as Canada, Japan, the Republic of Korea, Australia, New Zealand, Taiwan and other like-minded partners, including where possible through security and defence partnerships, information sharing, cyber, maritime security, space and resilience cooperation; stresses that EEA/EFTA states and their defence industries should be fully included in EU hybrid resilience frameworks and capability development programmes, recognising their direct contribution to European security and their shared exposure to hybrid threats;

82. Regrets that the recent shift in US policy has weakened the common front of democracies at a time of intensifying hybrid threats; stresses that transatlantic unity remains essential to fighting them;

83. Highlights that Russian influence operations in Africa, Latin America and the Caribbean are not peripheral to European security, as they seek to undermine the EU’s partnerships, weaken support for Ukraine and undermine European diplomacy, security assistance and development cooperation; notes that in Africa, these operations mostly rely on state media, and cultural and religious fronts, while in Latin America and the Caribbean, Russia has built a Spanish-language influence ecosystem that complements its anti-European messaging elsewhere; calls on the EU and the Member States to strengthen strategic communication, support independent and trusted local media, engage credible local voices and reinforce cooperation with partners in both regions to expose and counter hostile information operations;

84. Underlines the importance of the experience of Gulf States, Jordan, and other relevant partners in addressing hybrid influence networks associated with the Muslim Brotherhood, including through governance, regulatory, and societal resilience approaches, and calls for structured exchange of best practices with these partners in

order to strengthen the EU's understanding of hybrid threats, improve policy responses, and step up cooperation in countering foreign interference while respecting fundamental rights and the diversity of legal and political systems;

85. Notes Taiwan's extensive experience defending itself against China's hybrid attacks and FIMI; commends Taiwan's comprehensive resilience model, including the establishment of a Whole-of-Society Defence Resilience Committee, large-scale civil defence training, cooperation with civil society organisations, digital resilience networks and public preparedness initiatives; underlines that Taiwan's experience shows that societal resilience is not a secondary aspect of defence, but a central pillar of national security, particularly when hybrid pressure targets critical infrastructure, public trust and social cohesion; calls for regular exchanges between the EU and its Taiwanese counterparts on relevant security issues, and for stronger cooperation, in this regard, on countering FIMI and cognitive warfare, protecting critical infrastructure and undersea cables, and strengthening whole-of-society resilience between the EU and Taiwan; calls on the EU to expand trade and industrial cooperation with Taiwan, particularly in high-tech components and strategic technologies critical to the resilience and security of essential infrastructure and supply chains, including semiconductors, 5G/6G telecommunications equipment, drones, and dual-use items; stresses also the need to provide IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite) to Taiwan and Ukraine;

°

° °

86. Instructs its President to forward this resolution to the Council, the High Representative and the Commission.