HYBRID THREATS, ACCOUNTABILITY, AND RESILIENCE: RETHINKING THE EU RESPONSE

Input paper for the European Union Security Initiative Policy Dialogue

Patryk Pawlak
European University Institute / Carnegie Europe

INTRODUCTION

The European Union now faces a hybrid threat environment that is broader, faster, and more interconnected than the policy frameworks built to address it. Hybrid campaigns increasingly combine disinformation, cyber operations, economic coercion, sabotage, strategic corruption, supply-chain manipulation, and pressure on democratic institutions in ways designed to remain below the threshold of open conflict while steadily weakening the target's ability to respond (Brown *et al*., 2026). These campaigns are not episodic; they are sustained, adaptive, and often embedded in wider geopolitical strategies pursued by revisionist state actors, particularly Russia, and, in some domains, also by China.

For the EU, the challenge is not only operational but strategic. The Union is confronting a deteriorating international environment in which hostile actors use hybrid methods to exploit interdependence, weaponise openness, and erode trust, while key tenants of the international rules-based order are under mounting pressure. This convergence matters because the effectiveness and strength of the EU's external action are built around policies promoting an open market, a human-centric digital governance model, and a security cooperation grounded in international law and the multilateral system, all of which presuppose a degree of predictability in international behaviour that can no longer be taken for granted.

The paper makes two specific recommendations. First, it argues that the EU should move beyond a fragmented approach based on accumulating separate toolboxes for cyber, hybrid threats, foreign information manipulation and interference (FIMI), and emerging technologies. Existing instruments remain valuable, but the proliferation of partially connected frameworks risks bureaucratic layering rather than strategic effect. A more credible approach would be a Comprehensive Accountability Toolbox that integrates attribution, sanctions, regulatory measures, law-enforcement cooperation, market restrictions, diplomatic responses, and resilience support into a single, coherent operating concept.

Finally, the paper contends that strengthening Europe's security ecosystem requires a wider understanding of who produces resilience to hybrid threats. Security cannot be limited to the defence sector. Critical infrastructure operators, financial institutions, civil society organisations, digital rights groups, election watchdogs, investigative networks, and vulnerable communities often detect weak signals of hybrid operations before governments do and therefore form part of Europe's frontline defensive capacity. A comprehensive EU strategy should therefore protect and resource this wider ecosystem as a matter of security policy, not only democratic values policy.

1. Threat landscape and trends

Hybrid threats in Europe are no longer abstract combinations of tools; they are visible in a series of concrete, often public, incidents across member states. Hybrid campaigns have included suspected Russian linked sabotage of railways, logistics hubs, and other critical infrastructure in several EU countries, as well as damage to subsea cables and energy links in the Baltic and North Seas, which have been treated by European authorities as part of a broader pattern of hostile activity below the threshold of armed attack. They have also featured repeated drone overflights of military sites, energy facilities, and border areas, prompting multiple member states to tighten airspace controls and cooperate more closely at EU level on counter UAS measures. These incidents show how physical, cyber, and informational levers are combined to test defences, create ambiguity, and generate political pressure.

Public intelligence and strategic assessments across Europe describe these developments as part of a broader shift toward persistent, multidomain competition. Italy's 2026 intelligence report, for instance, characterises hybrid threats as the "operational synthesis" of technological, informational, economic, and migration related pressures, with Russia and China as the most active state sponsors of such tactics against Western countries (Presidenza del Consiglio dei Ministri, 2026). EU institutions have similarly warned that disinformation, cyber attacks, economic coercion, lawfare, and instrumentalised migration are now core instruments of hybrid campaigns targeting member states and partners, not peripheral risks (European Commission, 2016; European Commission, 2018). Information manipulation has become structurally embedded in this environment, with foreign actors building scalable manipulation "infrastructures" like bot factories that operate across platforms and languages. Powered by artifical intelligence, these tools can be rapidly retargeted toward new issues or countries (Council of the EU, 2026).

Five trends stand out in the current threat landscape.

1. **The information domain is now central to hybrid warfare, information environment more complex, and operations more sophisticated.** Systematic disinformation campaigns, foreign information manipulation and interference, and influence operations running across mainstream and fringe platforms have become a cost effective core tool of hybrid warfare, not just background noise. Operations such as Russian "Doppelganger" style campaigns that clone media brands, set up fake news sites in multiple EU languages, and flood social networks with coordinated content seek to erode trust in institutions, fragment audiences, and normalise pro Kremlin narratives on sanctions, Ukraine, migration, and energy. These efforts increasingly combine overt state media, covert inauthentic networks, and the amplification power of influencers and micro targeted advertising to reach specific communities and exploit existing grievances.

A closely related practice is the use of transnational repression, where regimes surveil, intimidate, or directly target members of the political opposition, journalists, and dissidents living in other countries, often through a mix of online harassment, smear campaigns, threats to family members back home, abuse of legal instruments such as Interpol notices, and, in extreme cases, physical attacks. By projecting coercion across borders, these actors seek not only to silence critics but also to send a wider signal that exile does not guarantee safety, thereby shrinking the space for independent voices and undermining the integrity of European political and information ecosystems. As a result, the information environment is both a target and a vector in hybrid campaigns: shaping perceptions and constraining opposition are treated as strategically important as disrupting infrastructure.

2. **Technological acceleration has lowered the cost of entry and blurred traditional boundaries.** Generative AI tools make it easier to produce large volumes of plausible sounding text, deepfake audio and video, and tailored imagery that can quickly overwhelm fact checking and verification capacities. Automated botnets and inauthentic accounts can artificially inflate the visibility of certain narratives or harass journalists, activists, and officials, while commercially available drones and off the shelf cyber tools give state and non state actors alike access to capabilities that were once restricted to specialised services. At the same time, key authoritarian actors are investing heavily in what they describe as digital sovereignty, building quasi autonomous internet ecosystems with their own platforms, infrastructure, and technical standards, as seen in the progressively more closed and state controlled online environments in Russia and China. Others, such as Iran, resort to severe restrictions on internet access, pervasive filtering, and targeted shutdowns to manage information flows and suppress mobilisation, while still projecting propaganda and coercive narratives outward. Together, these developments enable adversaries to combine sophisticated offensive capabilities with tightly managed domestic information spaces, complicating attribution, shielding their own societies from external scrutiny, and further accelerating the tempo and deniability of hybrid operations.

3. **Hybrid campaigns increasingly exploit interdependence as a lever of coercion.** Economic, infrastructural, and human interconnections that were once framed as unambiguous goods are now treated as potential pressure points in strategic competition. Critical infrastructure – from energy grids, pipelines, LNG terminals and ports to subsea cables, satellite links and rail corridors – becomes both a physical target and an instrument of signalling: disruptions, unexplained incidents, and threats of future interference can be used to create uncertainty, drive up costs, and test crisis management arrangements. At the same time, complex supply chains and dependencies on specific countries for critical raw materials, components or technologies are turned into tools of influence. Export controls, informal embargoes, licensing delays, and targeted bans on key goods or inputs allow hostile actors to reward or punish particular sectors and member states, shape business expectations, and deter policy choices that they perceive as contrary to their interests. These measures sit alongside more traditional economic coercion – such as punitive tariffs, arbitrary inspections, or politically motivated boycotts – to create a climate in which companies and governments alike must factor in the risk of sudden, strategically motivated disruption.

Combined with the manipulation of financial channels and, in some cases, the instrumentalisation of migration routes and border flows, this turns interdependence itself into a tool of hybrid pressure: the aim is not only to inflict immediate economic harm, but to internalise vulnerability into European decision making and constrain the Union's room for manoeuvre over time.

4. **Social grievances and cultural fault lines within European societies are exploited in a systemic manner.** Adversaries deliberately amplify anxieties linked to the cost of living crisis, fears about LGBTQI+ rights, ethnic minorities, refugees, and controversies over environmental protection in order to polarise public opinion and erode trust in institutions. Campaigns targeting climate policies, low emission zones, or renewable energy projects, for example, frequently blend genuine local concerns with orchestrated disinformation and harassment to portray green transition measures as illegitimate impositions by "out of touch elites" or "foreign interests". In the same way, narratives directed at LGBTQI+ communities, migrants, or religious minorities are weaponised to deepen identity based divides and to frame the EU's legal and human rights framework as a threat to national traditions. This technique does not create grievances from scratch; it repackages and amplifies them in ways that fragment the public sphere and make democratic compromise harder to sustain.

5. **Opaque financing and new technologies are used to fund hybrid operations and shape political ecosystems from within.** Covert or semi covert funding of political parties, individual politicians, media outlets, and front organisations enables hostile actors to influence electoral processes and policy debates while maintaining plausible deniability (Redlowska et. al, 2026). This can take the form of illicit donations, loans routed through intermediaries, or consultancy contracts. Such financial channels complement information and cyber operations by ensuring that sympathetic voices are present inside parliaments, party systems, and public debate, thereby normalising externally driven frames on issues such as sanctions, Ukraine, migration, or the EU's green and digital transitions. A growing concern in this context is the use of crypto assets as enablers of hybrid operations and covert political influence (Lockhart and Williams-Dunning, 2026). Pseudonymous, borderless, and in many cases lightly regulated, crypto systems provide hostile state and non state actors with additional channels for moving value across jurisdictions, evading sanctions, financing influence operations, and supporting proxy organisations with reduced detection risk. From a hybrid threat perspective, the ability to route funds through opaque wallets, mixers, decentralised exchanges, or loosely supervised service providers undermines traditional financial intelligence and political finance controls designed for the banking system. As a result, questions of political finance transparency, beneficial ownership, and enforcement of party funding rules are no longer purely matters of integrity; they are central components of the Union's defence against hybrid interference in democratic decision making.

Together, these developments mean that hybrid threats in Europe are best understood not as isolated episodes but as a continuous contest over the resilience of democratic institutions, the integrity of critical infrastructure, and the cohesion of EU decision making.

2. The EU's foreign and security policy response

On the external side, the EU has progressively reframed hybrid threats as a structural feature of the Union's security environment, not a marginal "grey zone" problem. This is visible in the way hybrid issues are now embedded in the EU's Strategic Compass, in CFSP statements, in sanctions practice, and in the operational cooperation with NATO on resilience, situational awareness, and critical infrastructure protection. Hybrid campaigns combining cyber operations, disinformation, sabotage and economic coercion have been explicitly linked to Russia's broader war of aggression against Ukraine and to Chinese pressure on European partners, which has helped move these issues from technical working groups into the centre of EU foreign and security policy debates. Externally, the EU's response has therefore focused on three main axes: enhancing the deterrent effect of sanctions and restrictive measures; supporting partners exposed to hybrid campaigns in the EU neighbourhood; and integrating hybrid considerations into defence and capability planning.

First, the EU has begun to use sanctions more systematically against individuals and entities involved in information manipulation, cyber operations, and other forms of hybrid aggression. Restrictive measures targeting Russian and Belarusian actors, including those connected to disinformation and sabotage, signal that hybrid activity is now treated as sanctionable state behaviour rather than as an unregulated space "below" foreign policy. Second, the EU's external instruments – from the European Peace Facility and security and defence related capacity building to neighbourhood programmes – have been used to help partners such as Ukraine, Moldova, and Western Balkan states strengthen cyber defence, media resilience, and critical infrastructure protection, recognising that vulnerabilities in the neighbourhood translate directly into risks for the Union. Third, there is a gradual – though still incomplete – convergence between EU defence initiatives and hybrid resilience, for example in joint work on military mobility, protection of seabed and space infrastructure, and the development of Hybrid Rapid Response Teams, which can be deployed to assist member states and partners facing hybrid incidents. This brings hybrid threats into the core of deterrence and defence planning, even if the EU's hard security instruments still depend heavily on the transatlantic framework.

The external response is also starting to acknowledge the fourth and fifth elements of the threat landscape: social grievances and interference into political processes. In relations with partner countries, EU delegations and specialised teams now track foreign information manipulation around issues such as migration, energy, and environmental regulation, and engage with local authorities and civil society to counter hostile narratives. In parallel, political finance and anti corruption conditionality are being used more assertively in external funding to reduce the space for opaque foreign financing of parties and politicians in accession and neighbourhood states. However, the link between these external instruments and the internal integrity of the Union's own political and media systems remains underdeveloped. The EU's credibility in calling out hybrid interference abroad will increasingly depend on its willingness to address similar vulnerabilities within its borders, including in major member states.

3. The EU's internal response

Internally, the EU response has been dominated by regulatory and resilience building measures that address the first three elements of hybrid threats: cyber and physical vulnerabilities, critical infrastructure, and the information environment. Directives such as NIS2 and the Critical Entities Resilience framework broaden the range of sectors subject to risk management and incident reporting obligations and encourage a more systematic approach to security of supply and continuity of essential services. Complementary instruments, including the Digital Operational Resilience Act for the financial sector and strengthened frameworks for the protection of transport, energy, and digital infrastructure, are meant to reduce the attack surface for hybrid campaigns that exploit technical and organisational weaknesses. At the same time, the EU's work on countering disinformation and foreign information manipulation – from codes of practice for platforms to the establishment of dedicated analytical units – aims to address the information layer of hybrid activity by improving detection, transparency, and coordinated responses.

In parallel, there is a growing recognition that hybrid threats are also a challenge to the integrity of democratic processes and the cohesion of societies. This has led to initiatives focused on election resilience, support for independent media and fact checking networks, and proposals such as the European Democracy Shield, which seek to connect the protection of elections, media pluralism, and civil society to the broader security agenda. These efforts begin to address the fourth element of the threat landscape: the weaponisation of grievances around cost of living, identity, migration, and environmental policy. Yet the implementation remains uneven, and local authorities – often the first to detect and absorb hybrid pressure – are still only partially integrated into EU level information sharing, training, and funding structures. A more mature internal response would treat municipalities, regional authorities, and community-based organisations as essential nodes within Europe's security ecosystem rather than as peripheral stakeholders.

The fifth element – covert financing and political influence – is only starting to be reflected in EU internal policy. Reforms of anti money laundering rules, beneficial ownership transparency, and party financing standards at EU level will shape the space available for foreign funding of political actors, but enforcement remains largely national and uneven. Cases of suspected foreign financing of parties, campaigns, or media outlets in several member states have demonstrated how financial channels can complement information and cyber operations to influence electoral processes from within. From a hybrid threat perspective, rules on lobbying, transparency of political advertising, and cross border financial flows are not merely technical integrity measures; they are frontline defences against strategic interference. Within the internal response, the EU's crypto framework can be framed explicitly as a hybrid threat countermeasure rather than a purely technical financial reform. By adopting the Markets in Crypto Assets Regulation and extending AML "travel rule" obligations to crypto asset transfers, the Union is effectively closing off a set of pseudonymous channels that hostile state and non state actors could use to move funds across borders, evade sanctions, and covertly bankroll disinformation outlets, proxy organisations, or sympathetic political actors.

These measures bring crypto asset service providers into the core of the EU's financial integrity and supervision architecture, making it harder to route money through opaque wallets, mixers, or lightly regulated platforms without leaving a compliance trail. In hybrid threat terms, crypto regulation therefore complements efforts on party finance transparency, beneficial ownership disclosure and media integrity: together, they narrow the space for foreign financing to distort electoral competition, sustain polarising campaigns, or quietly capture influence within European political and information ecosystems.

An effective internal response therefore requires closer alignment between security communities, financial supervisors, electoral authorities, and regulators responsible for party funding and media, so that patterns of influence can be detected and acted upon before they translate into shifts in policy and public trust.

4. The dismantling of the multilateral order as a threat accelerator

The worsening hybrid threat environment facing the EU cannot be understood only through the proliferation of tools and instruments enabling hybrid operations. It must also be read against the gradual weakening of the multilateral system and of the international rules based order that once constrained how states used those tools. What is changing is not simply that more actors are willing to engage in coercion, but that the normative, legal, and institutional frameworks designed to regulate coercive behaviour are being openly violated, selectively ignored, or instrumentally reinterpreted. For the EU, this is particularly consequential because its own security model is deeply embedded in multilateralism: the Union depends on the application and credible enforcement of rules governing sovereignty, trade, human rights, maritime access, and dispute settlement far more than most traditional great powers do. As these regimes weaken, hybrid threats become easier to deploy, harder to stigmatise, and more difficult to punish.

The most serious example remains the weakening of the UN Charter's core principles of sovereignty, territorial integrity, and the prohibition on the use of force. Russia's war against Ukraine is the most acute European case, combining large scale aggression with cyber operations, disinformation, political subversion, and economic blackmail as part of a single campaign, while a permanent member of the Security Council uses its veto to block effective Council action. Yet from the perspective of many states, these violations do not occur in a vacuum. Earlier US led uses of force without clear Security Council authorisation, such as the 2003 invasion of Iraq, as well as more recent unilateral military strikes framed as self defence but contested in terms of their compatibility with Article 2(4) and the necessity and proportionality requirements, have long fuelled perceptions that Washington applies international law selectively. Israel's conduct of military operations in densely populated areas, repeated large scale campaigns in Gaza, settlement policies in the occupied Palestinian territories, and disregard for advisory opinions and resolutions on the legal consequences of occupation are likewise widely cited as examples of sustained non compliance with international humanitarian law and with obligations deriving from the UN Charter and related instruments.

For many observers, the cumulative effect is a pattern in which major powers and close partners of the EU appear able to stretch or ignore fundamental rules with limited consequences, even as those same rules are invoked in defence of the European security order.

This matters directly for the hybrid threat context. When the prohibition on the use of force and basic obligations under international humanitarian law are seen as malleable, it becomes easier for other actors to frame their own coercive practices – including sabotage, transnational repression, targeted assassinations, information warfare and political interference – as part of a continuum of "normal" power politics rather than as clear violations of a shared legal baseline. The perception that the UN system cannot or will not constrain either adversaries or close partners erodes the stigmas attached to norm breaking and lowers the political costs of experimenting with hybrid tactics below the threshold of open war.

A similar pattern is visible in the trade regime. The WTO system was designed to channel economic disputes into rule based procedures and to reduce the use of trade as a blunt instrument of political coercion. Yet, cases such as China's actions targetting Lithuania in response to the opening of a diplomatic office in Taiwan, show how customs controls, informal embargoes, discriminatory treatment, and pressure on firms to remove Lithuanian components from supply chains can be deployed to punish political choices while maintaining a degree of deniability. The significance of this case lies not only in the pressure exerted on one member state, but in the message it sends to the wider Union: trade interdependence can be weaponised to force anticipatory compliance and to exploit asymmetries inside the single market. When such practices proliferate, the distinction between legitimate economic policy and coercive statecraft becomes blurred, and tariffs, export controls, licensing restrictions, and supply chain exclusion become part of the repertoire of hybrid pressure rather than exceptional departures from normal economic relations.

The maritime regime is under comparable strain, with direct implications for the EU. The UN Convention on the Law of the Sea (UNCLOS) is designed to provide predictable rules on maritime zones, navigation and the peaceful settlement of disputes, including rights over resources in the exclusive economic zone (EEZ). Yet in the Eastern Mediterranean, Turkey's repeated unauthorised exploration and drilling activities in areas claimed by the Republic of Cyprus as part of its EEZ, as well as Ankara's assertion of maritime claims based on agreements such as the contested 2019 Turkey–Libya memorandum, have been condemned by the EU as illegal and as infringing the sovereign rights of Cyprus and other member states under international law. Turkish drilling ships escorted by naval vessels have operated in blocks licensed by Nicosia to international energy companies, despite arrest warrants issued by Cyprus and repeated European Council conclusions warning that these activities jeopardise regional stability and violate the Law of the Sea. The EU has responded with diplomatic pressure and the adoption and renewal of a targeted sanctions framework allowing asset freezes and travel bans on individuals and entities involved in unauthorised drilling, but the underlying dispute remains unresolved. For the EU, the Cyprus case demonstrates how contestation of maritime law and EEZ boundaries can be turned into a form of hybrid pressure around energy security, as uncertainty over legal rights, combined with the presence of drilling platforms and naval assets, is used to signal coercive leverage and to test both the Union's solidarity and the resilience of a rules based maritime order in its immediate neighbourhood.

The human rights regime is also being undermined in ways directly relevant to hybrid threats, especially in the information domain. Disinformation, coordinated harassment, and transnational repression are not only political tactics; they often amount to sustained attacks on freedom of expression, access to information, political participation, privacy, and the security of journalists, dissidents, and minority communities.

When regimes engage in smear campaigns against exiled opposition figures, threaten activists abroad, manipulate digital platforms to drown out independent reporting, or target vulnerable groups with hate based narratives, they are exploiting open information environments while rejecting the human rights obligations that are supposed to protect them. Russia's departure from the Council of Europe and the removal of ECHR protections from its domestic legal framework are emblematic here: they illustrate how authoritarian actors can deliberately sever themselves from accountability mechanisms while still projecting influence and coercion outward into democratic societies. This weakens not only a particular treaty system, but also the broader expectation that individuals can rely on supranational safeguards against politically motivated abuse.

Other regimes are under similar pressure. Refugee and asylum norms have been strained by the instrumentalisation of migration, as seen in the Belarus crisis at the EU's borders, where vulnerable people were used as vectors of coercion against neighbouring states. Arms control and non-proliferation norms have also eroded in recent years, adding to a broader sense that the legal architecture restraining coercive behaviour is thinning. The cumulative effect is not only fragmentation across sectors, but a wider loss of confidence that rules will be upheld consistently or enforced impartially.

This broader erosion has consequences beyond each individual regime. When trade rules are bypassed, maritime rulings ignored, sovereignty violated by force, and human rights mechanisms abandoned or neutralised, the damage is not confined to those domains; it undermines trust in the very idea that rules meaningfully structure international conduct. That loss of trust creates negative externalities that are highly relevant to hybrid threats. It encourages hedging behaviour, normalises unilateralism, and rewards actors willing to test legal limits aggressively while others remain constrained by procedural caution. It also fuels public cynicism within democratic societies, where citizens may come to see international law and multilateral institutions as selectively applied, ineffective, or little more than instruments of power politics.

For the EU, this matters at several levels. Strategically, declining trust in rules weakens deterrence because hostile actors assume that attribution, legal action, or diplomatic protests will not be followed by meaningful collective consequences. Politically, the adversaries exploit the EU's institutional weaknesses and complex decision-making processes that make coordinated action harder. Socially, it creates fertile ground for disinformation narratives that depict the EU's normative commitments as naive, hypocritical, or ineffective, thereby feeding directly into domestic polarisation and anti-institutional sentiment. In this sense, the dismantling of the rules-based order is not simply a parallel crisis alongside hybrid threats; it is an accelerator of them. As confidence in the restraining power of rules declines, the threshold for coercive experimentation falls, the costs of norm-breaking decrease, and hybrid tactics become more attractive as a standard instrument of state competition.

In this environment, the EU's challenge is not only to defend itself against individual hybrid incidents, but to preserve the normative conditions that make restraint, predictability, and accountability possible in the first place. A credible response therefore requires more than resilience and better detection. It also demands that the Union treat defence of the multilateral system, of dispute settlement mechanisms, and of international legal standards as part of its hybrid threat strategy rather than as a separate diplomatic agenda. Without that connection, the EU risks managing symptoms while the strategic environment that generates them continues to deteriorate.

5. Shifting towards a Comprehensive Accountability Toolbox

Hybrid campaigns are more effective when international norms are weakly enforced, and the weakening of those norms accelerates when revisionist actors can employ coercive tools without bearing meaningful costs. For the EU, which is structurally invested in rule-based cooperation, market openness, and legal predictability, this produces a strategic asymmetry: its strengths can become vulnerabilities when adversaries are prepared to instrumentalise openness while disregarding reciprocal restraint. This is why business as usual is no longer sufficient. The conventional EU instinct has often been to separate internal market regulation, external action, sanctions policy, development cooperation, cyber policy, and democratic resilience into adjacent but distinct policy silos. That model may have been manageable when threats were compartmentalised, but it is poorly suited to adversaries that deliberately operate across bureaucratic, legal, and geopolitical seams. A departure from business as usual does not mean abandoning the EU's legal and normative identity. Rather, it means accepting that legality without speed, attribution without accountability, and resilience without enforcement are insufficient in a strategic environment where hostile actors design campaigns precisely to exploit hesitation and institutional fragmentation.

The central issue is therefore not only whether the EU has tools, but whether it can combine them with sufficient coherence and political will. Over the last decade, the EU has assembled a growing array of instruments to respond to complex threats. These include cyber diplomacy measures, sanctions regimes, FIMI analysis and response frameworks, resilience regulation, platform governance mechanisms, crisis response arrangements, and sector-specific requirements for digital and critical infrastructure security. Each instrument addresses a real problem, but together they do not yet amount to a unified operating doctrine. The risk is a form of strategic inflation in which every emerging challenge generates its own toolbox. A separate hybrid toolbox, cyber toolbox, FIMI framework, tech-security agenda, and preparedness agenda can create the appearance of action while dispersing responsibility across institutions and timelines. In practice, hostile actors do not distinguish neatly between cyber intrusion, information manipulation, corruption, economic coercion, and exploitation of legal loopholes; they combine them. The EU response should therefore be integrated around effects rather than around bureaucratic categories.

A Comprehensive Accountability Toolbox (CAT) would build on existing instruments rather than replace them. Its purpose would be to align the EU's capacities for attribution, exposure, sanctions, legal action, regulatory intervention, market denial, financial scrutiny, diplomatic signalling, and support to affected states and sectors into one escalation framework. In operational terms, this would mean that once a hybrid campaign is identified, EU institutions and member states should be able to move through a common sequence: joint assessment, coordinated attribution where feasible, proportional consequences, targeted resilience support, and follow-on monitoring. It would also promote more cross-institutional cooperation instead of siloed approaches that are dated and unsuitable for the current security context.

Such a toolbox should contain at least six elements:

1. Define clear procedures and mechanisms for communication towards a broader public and all relevant actors, such as media agencies or critical infrastructure operators, to reduce the opportunities for malicious information operations.
2. Connect intelligence-informed analysis with public evidence standards suitable for political attribution and legal defensibility.
3. Enable faster and more routine use of sanctions and restrictive measures against individuals, entities, and infrastructures involved in destabilising activity.
4. Integrate regulatory levers such as platform obligations, critical-sector compliance, procurement restrictions, and market access controls where these can reduce the attacker's room for manoeuvre.
5. Combine these punitive measures with rapid assistance to targeted member states, institutions, and actors.
6. Create a feedback loop so lessons from incidents are folded back into preparedness planning and sectoral regulation.

The value of such an approach is political as much as technical. Accountability changes the incentive structure of hybrid aggression. Resilience raises the cost of interference, but accountability raises the cost of choosing interference in the first place. For a Union that is often criticised for being normatively ambitious but operationally slow, this would help connect strategic language to credible consequences.

6. Building a comprehensive European security ecosystem

A stronger EU response also requires a broader understanding of the security ecosystem. Traditional policy debates still tend to privilege defence institutions, intelligence services, and the private sector. These actors are indispensable, but they are not the whole picture. Hybrid campaigns often unfold first in the social, financial, and informational space, where weak signals are picked up by journalists, researchers, local watchdogs, digital rights communities, election monitors, and vulnerable social groups before they are visible in national security channels. This wider ecosystem matters for at least three reasons. First, many hybrid operations target the connective tissue of democratic life rather than only state assets: trust in elections, confidence in media, civic cohesion, minority rights, and public willingness to accept institutional decisions. Second, non-state actors are often better positioned to detect narrative shifts, coordinated harassment, covert influence, or localised pressure campaigns. Third, hybrid actors frequently probe social fractures precisely where institutional attention is weakest.

Financial institutions should also be integrated more fully into the security ecosystem. As hostile actors diversify methods of concealment, movement of value, sanctions evasion, and influence financing, the line between financial integrity and security becomes thinner. This is especially relevant where crypto-related channels, opaque ownership structures, and transnational financial services can be exploited to support destabilising activity or obscure responsibility.

Even where direct evidence is case-specific, the policy implication is clear: anti-money-laundering, sanctions enforcement, beneficial ownership transparency, and digital finance supervision should be seen as part of hybrid threat defence rather than as separate compliance domains.

Civil society organisations deserve special emphasis. LGBTQI+ groups, digital rights organisations, anti-corruption actors, fact-checkers, and broader digital resilience communities are often targeted because they are visible, values-based, and socially embedded. Yet these same characteristics make them effective early-warning nodes for detecting intimidation, narrative manipulation, and attempts to fracture democratic solidarity. Treating them solely as beneficiaries of democracy support underestimates their security function. They should instead be recognised as resilience assets and incorporated into EU preparedness, funding, protection, and information-sharing arrangements.

A genuinely comprehensive approach to hybrid threats also requires security policy to "go local". Local authorities are often the first to detect anomalies in their communities, whether through unexplained infrastructure disruptions, suspicious activity around border areas, or sudden spikes in disinformation and intimidation targeting specific groups. Across the EU's eastern flank, including in Poland, municipalities and regional authorities have had to manage the immediate consequences of hybrid incidents linked to Russia's war against Ukraine – from orchestrated pressure at border crossings and critical infrastructure sites, to localised campaigns designed to inflame tensions over refugees, energy infrastructure, or minority communities. In these situations, mayors, local councils, and municipal services effectively become first responders in the hybrid domain, yet they frequently lack structured access to threat information, tailored training, or sustainable funding for resilience-building. Treating local authorities as integral components of Europe's security ecosystem – with dedicated channels for information-sharing, capacity building, and protection of those on the front line – is therefore not an optional add-on, but a core requirement for credible hybrid defence. A comprehensive investment strategy would therefore combine hard security and social resilience. It should include stronger protection of critical infrastructure and digital networks, as well as sustainable support for independent monitoring capacities, civic organisations, local investigative networks, and trusted community intermediaries. In a hybrid threat environment, resilience is produced not only by fortifying systems but also by enabling actors to notice, absorb, and expose hostile activity before it scales.

7. Conclusion

Hybrid threats against the European Union are no longer best understood as isolated acts of cyber disruption, disinformation, or sabotage. They are part of a wider strategic environment in which hostile actors combine informational, technological, economic, political, and social instruments of pressure while operating in a context where the multilateral system and the international rules-based order are themselves under strain. Violations of the UN Charter, the growing use of economic coercion, the contestation of maritime law, the weakening of human rights protections, and the instrumentalisation of migration and information spaces have together lowered the normative and political barriers to coercive behaviour.

For the EU, this means that hybrid threats are not simply a security problem to be managed at the margins, but a structural challenge to the legal, political, and economic foundations on which European integration depends.

The central implication is that resilience alone is no longer enough. The EU has built an increasingly dense architecture of preparedness, critical infrastructure protection, cyber regulation, FIMI monitoring, and sectoral resilience, but these efforts remain too fragmented to match the integrated character of contemporary hybrid campaigns. A more credible approach requires moving beyond the multiplication of separate toolboxes toward a more coherent accountability framework that connects attribution, sanctions, regulatory action, financial scrutiny, diplomatic signalling, and operational support within a single logic of response. Put differently, the EU needs not only to absorb pressure better, but also to impose clearer costs on those who generate it.

At the same time, the Union's security stakeholders ecosystem must be understood more broadly than in traditional state centric terms. Defence actors and operators of critical infrastructure remain essential, but so too are financial institutions, local authorities, civil society organisations, journalists, watchdog groups, and communities targeted through identity based polarisation or transnational repression. These actors often detect weak signals before central authorities do and are frequently the first to absorb the impact of hybrid operations. Treating them as peripheral to security policy underestimates how hybrid campaigns actually work.

Ultimately, the EU's response to hybrid threats will be effective only if it connects internal resilience, external action, and defence of the multilateral order into a single strategic vision. The task is not simply to counter individual incidents, but to defend the institutional trust, legal predictability, and democratic cohesion that hybrid actors seek to erode. In that sense, strengthening Europe against hybrid threats is inseparable from strengthening Europe's capacity to uphold rules, impose accountability, and protect the wider ecosystem of actors on which democratic resilience depends.

References

Will Brown, W., Kobzová, J., Popescu, N., Torreblanca, J. I. (2026). From shield to sword: Europe's offensive strategy for the hybrid age, ECFR Policy Brief, 6 March 2026. Available at: https://ecfr.eu/publication/from-shield-to-sword-europes-offensive-strategy-for-the-hybrid-age/

Council of the EU (2026) Council conclusions on advancing the European Union's capacity to counter hybrid threats. Brussels, 16 March 2026, https://data.consilium.europa.eu/doc/document/ST-7349-2026-INIT/en/pdf.

European Commission (2016). Joint Framework on countering hybrid threats a European Union response. JOIN/2016/018 final, Brussels, 6.4.2016.

European Commission (2018) Increasing resilience and bolstering capabilities to address hybrid threats. JOIN/2018/16 final, Brussels, 13.6.2018.

Lockhart, E. and Williams-Dunning, S. (2026) Recording: Emerging Technology and Democratic Processes. 7 May 2026. Available at: https://www.rusi.org/members-event-recordings/recording-emerging-technology-and-democratic-processes

Presidenza del Consiglio dei Ministri (2026) Governare il cambiamento: Scenari della sicurezza nazionale. Relazione annuale sulla politica dell'informazione per la sicurezza. Available at: https://www.sicurezzanazionale.gov.it/data/cms/posts/1163/attachments/4d8b721a-3c8f-456c-9bce-cbe649e7522b/download?view=true

Redlowska, K., Popyk, M. and Keatinge, T. (2026) Responding to Russian sabotage financing, RUSI Insight Papers, 14 January 2026. https://www.rusi.org/explore-our-research/publications/insights-papers/responding-russian-sabotage-financing