CEPS YOUNG THINKERS

HOW TO PROTECT THE EU AGAINST HYBRID THREATS

CEPS Young Thinkers Initiative
Security & Defense 2023

Laura Lisboa

Summary

Over the past decade, European governments and the EU have actively renewed their interest in **hybrid threats**. These are strategic policy issues that should receive much more consideration by the EU and its Member States in the decades to come.

Hybrid threats and attacks are coordinated actions that exploit the thresholds of detection and attribution designed to further strategic goals by deliberately targeting vulnerabilities [1]. They cover a **broad spectrum of techniques** used by malign actors to compromise security, undermine decision-making processes and destabilise democratic institutions.

As highlighted by recent examples, such as the **sabotage of Nord Stream 2** or **the weaponisation of migration** at the Belarusian border, hybrid threats are often hard to pin down and deliberately target states' vulnerabilities. Thus, this Policy Brief puts forward concrete recommendations to *improve the attribution of hybrid attacks and to develop a coordinated strategy for addressing critical vulnerabilities* across the European Union. Both are key to making states more capable to withstand and recover from shocks. In short – more resilient [2].

Acknowledgements

The author would like to acknowledge and thank Leonardo de Agostini for his insights and comments during the drafting of this Policy Brief.

[1] This Policy Brief uses hybrid 'threat' and 'attacks' interchangeably.
Weissman, Conceptualizing and countering hybrid threats and hybrid warfare, 63.

[2] Resilience is identified in the EU's 2016 Global Strategy as key to resisting and recovering from internal and external crises. In recent years, it has been increasingly used when referring to hybrid and cyber threats, as in the 2022 Strategic Compass. It entails the capacity to detect, attribute, respond and recover from such attacks and contributes to credible deterrence. This includes building resilience through deterrence by denial, to discourage hostile players by portraying hybrid attacks as unlikely to succeed; and through deterrence by punishment, by the threat of a severe and quick response.

Hybrid Threats: Old Technics, new challenges

The development and implementation of EU initiatives regarding hybrid threats has proven to be particularly challenging for three main reasons.

First, hybrid attacks now have a greater impact than in previous decades, even if the techniques used are not new – sabotage, espionage, deception or economic coercion for example have long been used to destabilise adversaries and geopolitical competitors, often as foreign policy tools in peacetime. Rapid technological change and global connectivity, however, facilitated the **speed, scale and intensity** of the use of hybrid techniques. Moreover, they often aim to provoke disruptions to constrain liberal democracies' freedom of maneuver, spread confusion among populations, and undermine the ability of leadership to make decisions.

Second, they present advantages for both state and non-state actors. The latter may resort to these techniques to leverage their relatively small force compared to the conventional forces that a state or a group/alliance of states possess. The former may find them convenient as they often fall under the threshold of military violence, are often ambiguous and hard to attribute, but capable of very tangible results that compromise the security of populations. Both scenarios require creative and effective solutions from governments that align with democratic values while avoiding escalation.

Third, a broad array of threats falls under the umbrella of 'hybrid'. While strategies addressing specific hybrid techniques have been developed, such as for cyberattacks or disinformation campaigns, hybrid threats remain broad and often hard to predict. States should thus focus on developing flexible approaches that can easily be adapted to address unforeseen hybrid scenarios.

In line with the above, instead of focusing on a specific category of threats, this Policy Brief focuses on cross-cutting issues and the common features of these threats. Streamlining attribution, mitigating critical vulnerabilities and safeguarding critical infrastructure are national competencies where the EU plays only a limited, but key role that can be boosted further.

Attribution: How to walk the fine line

Attribution is here understood as political attribution. Separate from the technical or legal capacity to attribute an attack, **it refers to the decision to either publicly or privately assign malicious actions to a specific actor differentiating it from an accident.**

In the EU, determining attribution, coordinating its political and public disclosure, and the decision on how to respond is a sovereign competence of the Member States. What role can the EU then play in this matter? Here we may consider different scenarios: (I) a national or cross-national attack, where one or more Member States are targeted or suffer tangible consequences and respond accordingly; (II) an attack causing a major disruption in a Member State that would require punitive measures to be taken at the EU level (for example economic sanctions), or that leads to invoking the **EU Solidarity Clause;** (III) an attack beyond the threshold of the **EU Mutual Defense Cause** demanding a collective response.

In the first two scenarios that fall below this threshold, the EU can serve as a coordination platform to enhance information sharing and improve national mechanisms for effective attribution. This includes sharing best practices, determining what level of attribution states are willing to commit to, aligning responses and enhancing national capacities to detect and support attribution with higher degrees of certainty.

The EU policy framework on countering hybrid threats had its first major document in the 2016 **Joint Framework on Countering Hybrid Threats**. Attribution is, however, barely mentioned in the text. A second major document released in 2018 addressing the need to **increase resilience and bolstering capabilities to address hybrid threats** emphasises the need for Member States and the EU to improve their attribution capacity in the cyber domain. In 2022 the Council dedicated two paragraphs to attribution in its guidelines for the establishment of a **Framework for a coordinated EU response to hybrid campaigns.** The document recalls that, although the attribution of an attack to a state or a non-state actor remains a sovereign political decision, Member States may request a Council body to examine it. This should rely on a fast and efficient decision-making process on a case-by-case basis, to define and approve coordinated EU responses to hybrid campaigns.

Both the EU Strategic Compass and NATO Strategic Concept identify hybrid attacks as qualifying for a collective response. This – and even less extreme scenarios – would require national governments to coordinate on who to attribute the attack to in a context where decisions have to be made quickly and full certainty in attribution is unlikely, if not impossible. Thus, to avoid ineffective responses, and to ensure resilience and proportionality, **EU policymakers should create common standards for attribution and collective response, with a focus on tailoring coordinated responses on a case-by-case basis.** Standards that on the one hand allow for flexible political decision-making processes and on the other hand do not undermine the credibility of responses.

The development of a coordinated approach creates challenges stemming from different national perspectives. **Future coordination will have to encompass divergences between national approaches that strive for more agile and assertive political attribution and those that prioritise the need to improve detection capacities first.** Moreover, Member States have different risk tolerances when it comes to attribution. Even when made with high levels of certainty, it may rebound, allowing for plausible public deniability by the accused party.

On top of this, there is no consensus on its strategic effectiveness. While assigning an attack to a state or non-state actor may disrupt further malicious plans, it does not necessarily deter them from a larger offensive. So...mission impossible? These challenges only highlight the need to address the key role the EU can play in building bridges and making the response to hybrid attacks much more effective.

Critical Vulnerabilities: Map and mitigate

The debate around the security implications of the Nord Stream pipeline explosions in September 2022 brought to the forefront ambiguity in attribution and the undermining of critical infrastructure as two sides of the same coin – i.e. two features of hybrid attacks tailored to cause similar damage to conventional attacks, but **without the same consequences.**

Critical Infrastructure is here understood **as an asset or system that is essential for society to function and whose damage or destruction highly compromises the security and well-being of the citizens.** It may refer to **different sectors** ranging from energy to the transport of people and goods, the food supply or digital communications infrastructure. Although the responsibility to safeguard critical infrastructure, evaluating and mitigating its vulnerabilities is primarily the responsibility of the Member States, stepping up the capacity to protect critical infrastructure is part of **Union efforts to counter hybrid threats**, an area where the EU can play a valuable support and coordination role.

Moreover, even if European countries have been improving the protection of vital infrastructure, the knowledge and resources to do so could be increased by multinational cooperation through the EU in coordination with NATO. The **EU-NATO Task Force** on strengthening resilience and the protection of critical infrastructure launched in March 2023 aims at joint work by both organisations' staff to identify, draw scenarios and develop responses to threats to critical infrastructure.

On EU level initiatives, in October 2022 following the attack on the Nord Stream pipelines, the European Commission presented a **5-point plan** stressing the need to secure critical European infrastructure by enhancing preparedness for attacks. This includes stress-testing, mechanisms to enhance the effectiveness of any response, the timely adoption of technologies to detect potential threats, and international coordination with other key partners to boost resilience and improve information sharing.

In December 2022, the Council of the EU approved the **Critical Entities Directive**, which replaced a similar document from 2008. The Directive invites states to update their risk assessments to reflect current threats, encourages them to monitor the operation of critical infrastructure and to develop a blueprint to coordinate responses to critical infrastructure threats with cross border relevance. Member States' attitudes toward this and similar initiatives are, not surprisingly, **divided**.

On national-level initiatives, countries such as Finland and Sweden are exemplars to extract best practices from the whole-of-society approach to security. This involves improving resilience through better coordination of contingency plans, increased preparedness at national and local levels for possible disruptions or emergency conditions, and setting up joint objectives and awareness.

This approach recognises that security is not exclusively a responsibility of the state but rather **involves numerous societal actors**. This requires citizens to be better prepared for disruptions and less vulnerable to disinformation campaigns or cyber-attacks.

Similarly, civil society can play a role in offering training and distributing information for better preparedness and in building networks to assist authorities in case of disruption. The **private sector** can ensure security of supply through back up plans for their critical purposes or contributions to defense planning. These represent two excellent examples of 'best practices' to be shared among EU Member States that help to develop better policy in this field.

Policy Recommendations: How to protect the EU against hybrid threats

Following on from the above, this Policy Brief makes three key recommendations on how to improve the EU's collective response against hybrid threats.

1 **An agreement on an attribution framework that establishes common standards for attribution and a collective response in the event of a hybrid attack.**

This encompasses previously agreed degrees of certainty and corresponding actions and guidelines for the deployment of defensive measures in case of an attack on one or more Member States. EU-level structures can play a key role in harmonising divergent opinions by facilitating dialogue among national policymakers through a hybrid threats awareness network and by supporting the coherent development of national legislative frameworks for better coordination and flexibility.

2 Broaden the scope of the EU Mutual Defense Clause (Article 42.7 of the TEU) to explicitly allow hybrid attacks to qualify for mutual defense.

Future action should build on the **2022 Council conclusions on a coordinated EU response to hybrid threats** that recognises the need to further invest in mutual assistance through both the EU Mutual Defence Clause and the Solidarity Clause. This would not necessarily imply a Treaty change but would at minimum require an increased display of firm political will and commitment. Since 2016, **NATO has publicly stated** that hybrid actions against one or more Allies could lead to invoking Article 5 of the North Atlantic Treaty. Progress was later made in this respect at the EU level, with the Strategic Compass and President von der Leyen's statement that attacks on active European energy infrastructure would lead to the **'strongest possible response'**.

3 There needs to be further support for existing and newly coordinated efforts on the protection of critical infrastructure.

This includes the tighter guarding of facilities, enhanced surveillance, and effective threat detection to allow for swift responses by national and international bodies; as well as responses that reinforce supply routes and mitigate the potential impact of disruptions. Priority should be given to energy and **underwater infrastructure** as the majority of the world's oil and gas is either extracted at or transported by sea and a large majority of global data flows are **transmitted through undersea cables.**

Conclusions: The way ahead

Hybrid threats are key strategic policy issues for the EU and its Member States. Efforts are being made to test the Union's preparedness and increase its capacity to prevent attacks and respond jointly and coherently to them – as seen in the **EU Integrated Resolve 2022 joint exercise**.

The implementation of the proposed recommendations, however, faces challenges that Member States should aim to overcome through constructive discussion, mutual respect, and a dose of pragmatism. When dealing with hybrid threats, to be realistic is to be ambitious, and inaction would take a heavy toll, with possible disastrous effects. Increased credibility in detecting, deterring, and defending against hybrid threats requires stronger cohesion and tighter coordination within the EU and with key international bodies.

CEPS YOUNG THINKERS

Place du Congrès 1
1000 Brussels
Tel: +32 (0) 2 229 39 11

youngthinkers.ceps.eu

youngthinkers@ceps.eu

@CEPS_thinktank