GPC POLICY BRIEF

FEBRUARY 2025

STRENGTHENING EUROPE'S ACTIONS AGAINST HYBRID THREATS: SETTING UP A PROTEUS PROGRAMME

Bernard Brunet, Former Head of Unit, DG NEAR, European Commission

EU countries face a growing and unprecedented wave of hybrid threats originating from Russia and other third countries. These actions have affected military installations, critical civilian infrastructures, health facilities, as well as sown discord and spread disinformation. More than eight years ago, the EU and its Member States agreed on actions to counter hybrid threats, yet the response has remained largely ineffective and has not succeeded in deterring hostile actors, in fact hybrid actions against the EU and Member States have increased in both audacity and sophistication. The preparation of the new long-term EU budget is an opportunity to create a new EU programme to counter hybrid threats. Named PROTEUS, this new programme would support EU Member States in countering hybrid threats more effectively, notably with critical infrastructure, resilience, and better analysis. In the meantime, immediate actions should be taken to bolster EU capacities, including the creation of an EU Cyber Command and establishing rapid response teams against disinformation.

Global Policy Center
School of Politics, Economics and Global Affairs, IE University

GPC Policy Brief
February 2025

INTRODUCTION

The European Union confronts an escalating crisis of hybrid warfare that threatens to undermine its fundamental security architecture. These sophisticated attacks combine cyber warfare, electoral interference, critical infrastructure sabotage, and coordinated disinformation campaigns. The scale and complexity of these threats, primarily orchestrated by Russia but increasingly deployed by other state and non-state actors, expose significant vulnerabilities in the EU's collective defense capabilities.

As Kaja Kallas, the new EU High Representative for Foreign Affairs and Security Policy and Vice President of the European Commission, emphasized in her speech at the European Defence Agency on January 22, 2025. "Putin's regime is already undertaking increasingly brazen acts of sabotage: cyber-attacks in Spain and Czechia; election interference in Romania and Moldova; parcel bombs in Germany; disinformation campaigns; jamming of GPS systems that stops aircraft from landing [in Estonia and Finland]; damage to underwater cables".

> Many authoritarian regimes now openly attempt to weaken EU Member States' political institutions, economies, and societies.

THE SCALE AND NATURE OF CURRENT THREATS

Many authoritarian regimes now openly attempt to weaken EU Member States' political institutions, economies, and societies. Notably Russia, Belarus, Iran, and China pursue two main, if broad, objectives: undermining democratic societies and promoting autocratic governance models, while reducing EU resistance to their destabilisation efforts globally. These include Russia's war against Ukraine and Iranian's support of Houthi attacks on Red Sea maritime traffic.

Even EU partner countries engage in hybrid destabilising actions (and no longer try to hide these efforts). Azerbaijan, despite energy partnership negotiations with the EU, supports independence movements on French territories. Gulf states promote radical ideologies in European countries, including Austria, Germany, and Belgium, through state-funded religious leaders.

The current era of affordable technology and widespread social media has made it relatively easy to deploy hybrid campaign capabilities. Criminal groups have notably been targeting the European medical sector, with Member States reporting 309 cybersecurity incidents in 2023, and 54% of cybersecurity incidents between 2021-2023 involved ransomware attacks (i.e. demanding payment of ransom in exchange for a decryption key to unblock paralysed IT systems). Meanwhile, defence against such campaigns are both long and complicated.

THE EU RESPONSE FRAMEWORK

The EU has recognised its increased vulnerability and developed its response in a 2016 "joint framework on countering hybrid threats – a European Union response". The Joint Communication between the European Commission and the High Representative for Foreign Affairs and Security Policy proposed mechanisms to exchange information, enhance resilience, and counter hybrid threats in critical sectors, and called for strengthened EU-NATO coordination and greater involvement of Member States in implementing the framework. A 2018 follow-up Communication strengthened these initiatives.

Implementation of the two Joint Communications has included the establishment of the Centre of Excellence for Countering Hybrid Threats, located in Finland, which serves as a training and development hub for bringing together public, private, and military stakeholders.

The EU established its EU Hybrid Fusion Cell integrated in the EU Intelligence and Situation Centre (INTCEN) to enhance situational awareness. An operational playbook was developed and tested through exercises. NATO's Counter hybrid support teams, established in 2018, provide targeted assistance to Allies on request. The EU Hybrid Toolbox launched in 2023 and 2024 with the support of the Commission services and the European External Action Service, coordinates responses to hybrid threats through internal and external measures. In 2024, the EU agreed to set up EU Hybrid Rapid Response Teams to provide short-term and tailored assistance to Member States and partner countries for responding to these threats – but, as of yet, these remain inactive.

The EU has also established two dedicated sanctions frameworks. In May 2019, it created a framework for restrictive measures against cyber-attacks threatening the EU and its member states. In early 2025, the EU used this framework to list three officers of the General Staff of the Armed Forces of the Russian Federation. A second framework, established in 2024, targets Russia's destabilising actions abroad, enabling the EU to target individuals and entities engaged in actions and policies – including cyber-attacks, by the government of the Russian Federation – that undermine the fundamental values of the EU and its member states, their security, independence, and integrity, as well as those of international organisations and third countries.

THE GROWING CHALLENGE

Despite eight years of EU initiatives, hybrid threats from foreign states and criminal groups have only increased in scope and intensity. Recent incidents demonstrate heightened aggression: electoral interference in Moldova and Romania, sabotage on German warships, discovery of incendiary devices destined for cargo planes flying from Germany and England to North America, and disruptions to Baltic Sea underseas cables in late 2024 and early 2025.

> EU Member States lack resources to address these multidimensional threats on their own. EU level action is crucial given the scale and multidimensional natures of the threats.

On 30 October 2024, former Finnish President Sauli Niinistö issued a comprehensive report on "Strengthening Europe's Civilian and Military Preparedness and Readiness" at the request of European Commission President Ursula von der Leyen. This report details the comprehensive nature of the challenges posed by malign and aggressive actors bent on destabilising and undermining the EU and calls for a paradigm shift in EU security, emphasizing that EU Member States lack resources to address these multidimensional threats on their own. EU level action is crucial given the scale and multidimensional natures of the threats.

RECOMMENDATIONS FOR EU PREPAREDNESS

The Niinistö report addresses a variety of threats to the EU – from environmental crisis and natural disasters to violent conflict. Its recommendations related to

hybrid threats focus on developing a comprehensive EU Risk Assessment, enhancing situational awareness, and strengthening EU intelligence structures. For the 2028-2034 multiannual financial framework, the report proposes integrating preparedness through:

1. **A preparedness-by-design approach** in the next EU budget, reinforcing long-term 'investment impact, crisis recovery spending, ring-fencing funding for preparedness action, and strengthening the dual-use spending potential.
2. **A European Preparedness and Readiness Investment Framework** with an Investment Guarantee Programme to boost Europe's defence technological industrial base and expand European Investment Bank funding for the defence sector.

> While it is unlikely that an open military conflict will start on the territory of the European Union in the short to medium term, there are serious reasons to be concerned about an escalation of hybrid actions

The report argues that at least 20% of the EU budget should be allocated to security and crisis preparedness through two distinct facilities: the Defending Europe Facility for defence and dual-use instruments, and the Securing Europe Facility for civil security, civil protection, and other emergency response services.

The European Council's December 2024 Conclusions reaffirmed these recommendations, emphasizing the urgency of strengthening EU resilience, preparedness, crisis prevention capabilities in response to the evolving threats and environmental challenges. The Commission, the High Representative, and the Council have been invited to implement the measures and support EU Member States.

THE NEED FOR ENHANCED EU ACTION

There is an increased hybrid threat level, yet the EU's responses have so far lacked sufficient urgency and ambition. The reasons for this sorry state of affairs are the same that have hampered an effective EU action in the security area: divergences among Member States about the EU role on security; discussions on the respective roles of the EU and NATO and how to ensure effective cooperation; resistance by many Member States and the EU institutions (including the Commission), about ceding power and responsibilities in the management of new projects; lack of sufficient funding for all the envisaged initiatives, including the EU Hybrid Rapid Response Teams. Without addressing these structural challenges, the EU risks delivering responses that are too little and too late.

While it is unlikely that an open military conflict will start on the territory of the European Union in the short to medium term, there are serious reasons to be concerned about an escalation of hybrid actions, targeting military and civilian infrastructures, with the clear intent of testing EU Member States and Candidate countries' readiness, degrading key capacities and eroding the will to defend and protect EU interests.

In the spirit of the Niinistö report, what is needed now is not so much awareness-raising about hybrid threats or creating new institutional structures, but a major initiative to boost operational capabilities of both EU Member States and the EU institutions. This requires developing capacities to anticipate, prevent, and respond rapidly and effectively to hybrid threats, alongside mobilising collective political will for EU action.

GPC Policy Brief
February 2025

The imminent start of the discussions on the new 2028-2034 multiannual financial framework, with its corollary discussions on the shape of EU policies and programmes, offers the opportunity to launch a major new initiative at the EU level. The new College of Commissioners led by President von der Leyen is due to make its proposals to the Member States and the European Parliament in the first semester of 2025. Negotiations among the three institutions will then likely last until 2027, for an entry into force of the new programmes on January 1, 2028.

THE PROTEUS PROGRAMME: A COMPREHENSIVE RESPONSE

As a contribution to the implementation of the recommendations of the Niinistö report, the European Commission should propose a new EU-wide programme to strengthen collective capabilities to anticipate, detect, and counter hybrid threats. Named PROTEUS after the Greek god known for his ability to change shape and adapt to any situation, this programme would include the following components:

- **Critical infrastructure protection**: Support Member States in implementing the new EU Directive on the resilience of critical entities. PROTEUS would fund protective works, re-design, security measures, and IT investments based on national risk assessments due January 17, 2026, with critical entity identification by July 17, 2026.
- **Exercises and simulations**: Conducting regular table-top exercises and simulations to protect critical infrastructures (on land and at sea.) This would identify vulnerabilities, test security measures and communication channels, prepare for various scenarios, improve public-private coordination, clarify roles and responsibilities, train staff, and, importantly, generate insights and post-action analysis.
- **Training and analysis**: Partnership with the European Centre of Excellence for Countering Hybrid Threats to support smaller and more vulnerable Member States and candidate countries (such as the Baltics and Moldova). It is a clear EU interest to help these state from becoming weak links in the collective defence of the EU. The PROTEUS programme would allocate funds following a needs assessment and common priorities.
- **Hybrid fusion cell enhancement**: Strengthen analytical capabilities through AI and big data analytics for early identification of hybrid attack patterns. The EU hybrid fusion cell remains modest in scale and resources, and a share of PROTEUS funding could be allocated to new analytical tools and projects, some of which could be managed by the ENISA (European Union Agency for Cybersecurity) and the Computer Emergency Response Team for the European Union.

The PROTEUS programme would allocate funds following a needs assessment and common priorities.
Hybrid fusion cell enhancement: Strengthen analytical capabilities through AI and big data analytics for early identification of hybrid attack patterns.

- **Rapid response teams**: Implement the May 2024 Council guiding framework for the practical establishment of the EU Hybrid Rapid Response Teams and finally ensure quick deployment capabilities. The PROTEUS programme would have a clear window for the predicable financing of such teams, and sufficient flexibility to ensure quick mobilisation of funds.
- **Community resilience**: As the Niinistö report stressed, "being adequately

prepared for major threats requires working according to a whole-of-government and a whole-of-society approach". Financing community resilience programmes in vulnerable regions and sectors would strengthen collective security.

- **Candidate countries support**: Provide dedicated financing and expert assistance to strengthen domestic hybrid threat capacities in candidate countries, notably Moldova and most Western Balkans. The PROTEUS programme would offer dedicated financing as well as the mobilisation of EU Member States experts to support candidate countries and ensure they have stronger capacities even before they join the EU.

Clearly, this list of possible activities remains indicative and this new EU programme should remain flexible to react to the evolving circumstances, especially given the seven-year period of the MFF. This also would reflect the adaptive, multifaceted nature of hybrid threats and the need for a dynamic and versatile response.

Under the European Commission, PROTEUS would operate through regular consultations with Member States and key institutions, notably the Centre of Excellence for Countering Hybrid Threats. Member States would approve and regularly consult on the work programme and its implementation.

A budget of €7 billion for the seven years period would help to address the multi-dimensional nature of hybrid threats and fund critical infrastructure protection, AI and big data-enhanced threat detection threats, and capacity building for all Member States.

IMMEDIATE ACTIONS REQUIRED

While the PROTEUS programme addresses long-term needs, several urgent measures should be taken before January 1, 2028:

1. Establishing an EU Cyber Command closely linked to the EU hybrid fusion cell for real-time intelligence sharing and coordinated cyber-attack response.

2. Create a dedicated Commission department to fight disinformation more resolutely, bringing experts from Member States in rapid response teams.

3. Establish a separate sanctions regime targeting disinformation actors.

4. Negotiate information sharing and best practices with the UK, Norway, and Switzerland to strengthen the response to hybrid threats.

> Europeans should not close their eyes to the new grim realities of our times. Never have EU Member States faced so many direct violent and destabilising actions from third countries bent on undermining peace and stability in Europe.

As NATO Secretary General Mark Rutte stated at the European Parliament in January 2025, Europe faces a clear destabilisation campaign orchestrated by Russia with the implicit and opportunistic support of other powers. The time is now to scale up support for those EU Member States that most require it, in parallel with a stronger effort on defence spending. SG Rutte's warning that "We are not at war, but we are not at peace either" stresses the urgency of strengthening the EU's defensive capabilities.

CONCLUSION

Europeans should not close their eyes to the new grim realities of our times. Never have EU Member States faced so many direct violent and destabilising actions from third countries bent on undermining peace and stability in Europe. The breakdown of what remained of the post-cold war international order ushers a new era when many geopolitical actors will see the demise of the European Union as the final objective to finally nail down any pretence of an international system in which the power instincts are checked by common rules.

With the possible exit of the US from the collective security of Europe, the EU and its Member States have started to realise that now is the time to focus more on collective security and defence. Establishing a dedicated EU programme focusing on hybrid threats – the PROTEUS programme – should be part of the new collective EU toolbox. PROTEUS resources would help to protect critical infrastructure of Member States, strengthen threat analysis, step up preparations, deploy rapid response teams swiftly and effectively when threats arise, and build the resilience of communities and institutions. While PROTEUS resources could only be mobilised as of 2028, much can be done now to significantly ratchet up the collective response. Establishing an EU Cyber Command would be a first immediate step and the deployment of rapid response teams is also urgent.

Recent months have shown that the audacity and sophistication of hostile actions against the EU have only increased. We should not be surprised when bolder and more nefarious actions strike. The faster we prepare, the higher the chance that peace and prosperity will prevail.

Global Policy Center
School of Politics, Economics and Global Affairs
IE University

IE Tower
Paseo de la Castellana 259E.
28046, Madrid, Spain
www.ie.edu/gpc/
GlobalPolicyCenter@ie.edu
+34 915 689 600

GPC Policy Brief
February 2025