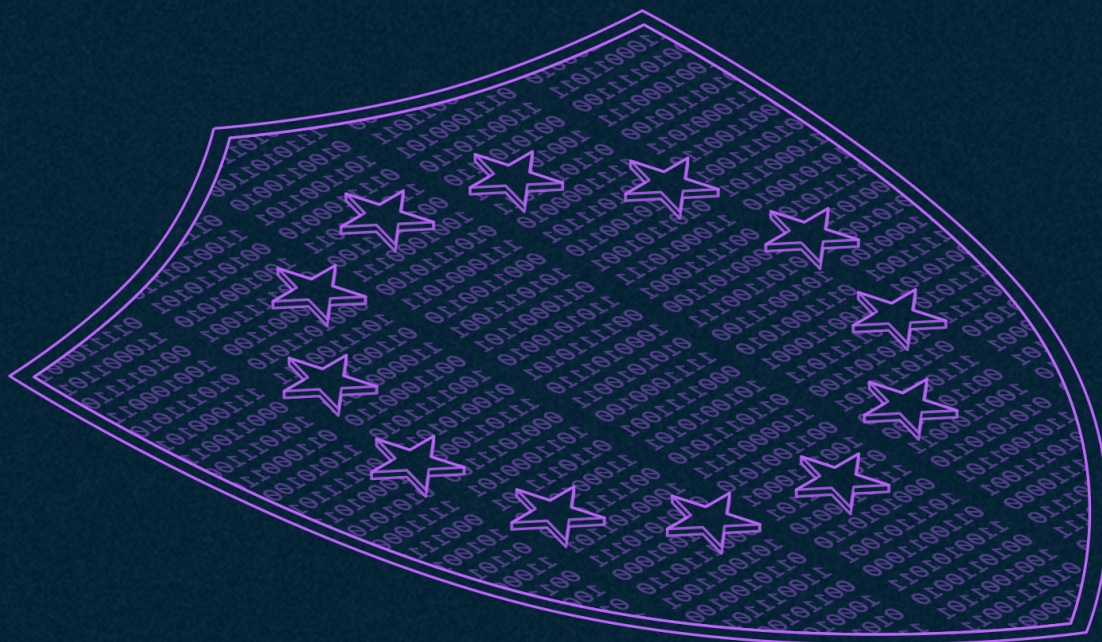




## Strategic Digital Security

# In This New Geopolitical Reality, Europe Needs a Coherent Digital Deterrence Strategy

By **Trinabh Banerjee**

ESP Series 2, Policy Brief No. 7

Editors: **Giulia Convertini**, **Margherita Rossi**,  
**Matteo Nilsson**, and **Mariona Fortuny Jané**

European  
Strategic  
Policy

EP

Europe's digital resilience is weakened by the Union's inability to deter the very digital security threats it seeks to resist.

## Executive Summary

The von der Leyen Commission's proclamation of a "geopolitical Europe" envisioned a sovereign and strategically driven European Union in charge of its own future. In setting out these stakes, Brussels has already deployed an extensive legislative arsenal to build digital resilience and set global standards. But at a time when geopolitical tensions, grey-zone hybrid warfare, and digital threats are growing, it is clear that the Union's digital security strategies have not evolved to move beyond resilience. Indeed, the Union's abilities remain largely focused on resilience and deterrence by denial, undermining the EU's strategic credibility. This issue must be overcome to better protect Europe's

strategic orientation and geopolitical power.

This gap between resilience and deterrence is sustained by structural problems: fragmented intelligence, national vetoes, slow attribution processes, and institutional barriers that allow hostile actors to continue to exploit vulnerabilities. In response, this brief proposes three broad recommendations, namely a Common Foreign and Security Policy (CFSP)-based intelligence capacity, pre-negotiated retaliation templates, and a comprehensive EU-Ukraine digital security 'lessons learned' framework that all aim to strengthen the EU's geopolitical capabilities.

*Trinabh Banerjee* is Euro Prospects' Strategic Digital Security Analyst within the European Strategic Policy Unit (ESP). Read the author's full description [here](#).

*Euro Prospects* is an independent publication focused on the analysis of European politics and policy. *ESP* is Euro Prospects' dedicated think tank unit on EU strategic policy.

# Key Recommendations

## Build a dedicated deterrence capability rooted in the existing possibilities of the CFSP

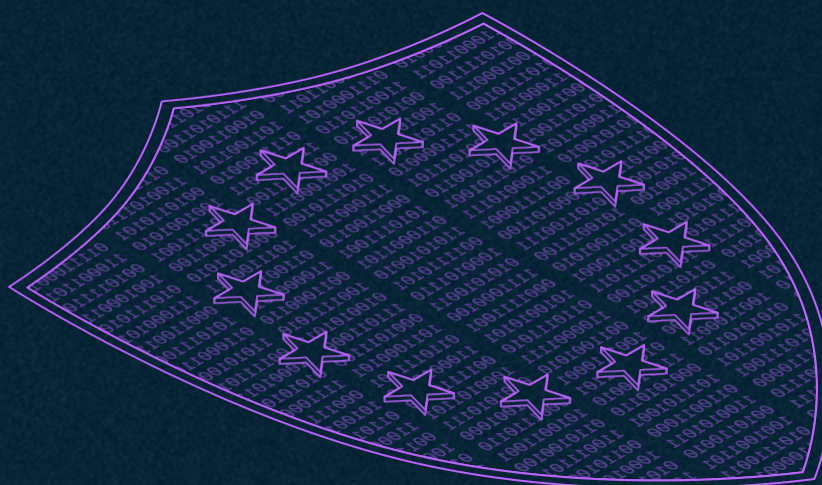
Focus on resolving a broken intelligence picture that damages the EU's own situational awareness. The aim should be to cohesively share intelligence within existing legal parameters and structures, while operationalising mechanisms to use intelligence as a shaping tool.

## Move toward pre-agreeing attribution and response templates

Overcome slow barriers to action by negotiating beforehand on a list of (retaliatory) options in the event of cyber incidents, placed under the authority of existing CFSP protocols. These 'menus' of actions would require agreement beforehand, but would nevertheless send signals to adversaries of costs.

## Obtain, understand, and apply lessons learned from Ukraine

Ukraine's dual resilience-deterrence cybersecurity strategies have been shaped both by physical warfare and a flood of cyberattacks which, thanks to these strategies, have become less effective over time. The EU, together with its member states, among Ukraine's largest backers, should work intensively to build a digital security deterrence strategy to understand and apply lessons within the European context.



# Analysis

## Playing Defence: Existing Structures

The EU's current digital security architecture combines legislation, policy, and institutional instruments that are designed to build a common level of cybersecurity. The EU has implemented legislation like the NIS2 Directive that expands the applicability of cybersecurity measures to sectors including energy, health, transport, and digital infrastructure. By imposing mandatory risk-management measures, accountability, and penalties for non-compliance, the directive aims to strengthen digital security within the 18 identified sectors. The Cyber Security Resilience Act (CRA), adopted in 2024, sets a minimum security threshold for all commercial products containing digital elements, requiring security to be built into the design of the product. The Digital Operational Resilience Act (DORA) aims to harmonise digital security for financial services providers and related finance digital services providers. Other policies, like the Cyber Solidarity Act, also focus on building resilience into the EU's cybersecurity infrastructure. Indeed, EU bodies like ENISA have also benefitted from expanded authority to provide technical guidance, support, and capacity-building to prepare European actors for ongoing and future cybersecurity challenges.

In so doing, the EU has excelled at resilience, the capacity to absorb, withstand, and recover from a cyber attack or threat. This is a largely defensive posture, focused on hardening infrastructure and services, ensuring continuity of operations, and incident response. Deter-

*“The EU has built considerable capacity and ability to deny adversarial actors success but without the means to impose timely and credible costs on them.”*

rence, the capacity to shape or restrict an adversary's behaviour beforehand, is focused on two elements. The first is denial, which are strategies designed to make an attack fail. Instruments like NIS2, the CRA, and DORA do give the Union a reasonable measure of success in deterrence by denial because these measures lower the likelihood of successful attacks. Yet, the EU lacks a comparatively credible capacity for deterrence by punishment. Without the effective ability to impose costs on adversaries for hostile behaviour, these actors continue to engage in cyber incidents and grey-zone cyber attacks that threaten European digital security.

The Cyber Diplomacy Toolbox, which is the Union's main tool designed to impose restrictive measures against entities responsible for cyber-attacks, ultimately becomes reactive and difficult to deploy because of cumbersome unanimity requirements, unclear attribution protocols, and continued lack of Union-wide evidence-based cybersecurity situational awareness. Indeed, though it has been used several times since its inception in 2017, it has not been employed at the scale necessary to sufficiently deter digital security threats. As such, the EU has built considerable capacity and ability to deny adversarial actors success

but without the means to impose timely and credible costs on them.

## Why EU Deterrence Fails

The EU's lack of credible digital deterrence by punishment is underpinned by several structural and political issues that undermine its strategic approach.

Firstly, a credible deterrence by punishment strategy requires a unified and timely intelligence picture. Without clear intelligence that can accurately attribute cyberattacks to the responsible parties, punishment becomes significantly more difficult. The EU's intelligence landscape remains largely fragmented along national lines, undermining the ability to credibly and reliably attribute cyberattacks and propose punishment at the Union level. Article 4(2) of the Treaty on European Union (TEU) enshrines the principle that "national security remains the sole responsibility of each Member State", creating a tension between an EU that seeks increasingly to act as a geopolitical entity and the inherent sovereignty of 27 member states in the realm of intelligence. With unclear intelligence efforts in the realm of digital deterrence, fragmentation allows hostile actors to exploit gaps in the Union's situational awareness, leaving the EU's response slow, inconsistent and based on incomplete information. Although the Union called for the establishment of a Joint Cyber Unit in 2021 to address some of these intelligence sharing and awareness issues, its scope and effectiveness remains largely unclear, given the fact that it has not been mentioned again since a supportive Council conclusion memo in 2021.

Secondly, the EU's cyber sanctions regime, as presented above, is legally sound but suffers from procedural hurdles. The process of attributing a cyberattack to an actor and subsequently securing unanimous agreement to impose punitive measures against that actor is notoriously slow, especially because attribution remains a national state competence. When punitive measures are imposed, the EU is left taking steps reactively, at a time when the strategic moment has passed. This leaves the Union out of step with the urgency of digital threats, undermining its credibility as a strategic actor and demonstrating its inability to deliver lasting consequences, subsequently allowing adversaries to act with greater impunity.

A counter-example to the EU's digital deterrence struggle is evident in Ukraine's construction of a whole-of-country cybersecurity strategy that implements both deterrence and resilience. Despite being a country at war, and in a visibly different political situation than the EU, Ukraine's experience building defensive models, integrating specialists, and employing deep public-private coordination to build a shared strategic picture yields lessons that can strengthen the Union's digital deterrence posture. Indeed, deterrence forms a key part of the country's digital security strategy, particularly focused on punitive steps. These actions have lowered the number of cyber attacks considered severe between 2022 and 2024, from 1048 to 59, even as registered attacks rose from 2194 to 4315 in the same period due to the ongoing conflict. With the development of a comprehensive and balanced strategy, it is thus possible to reduce the impact of cyber attacks and also build resilience. As cybersecurity threats continue to intensify, from targeted hacks on officials to breaches of government databases, it is also clear that the EU's inability

to fully deter them weakens its overall strategic strength.

## | What the EU Can Do

Based on the issues identified, this brief makes three recommendations to strengthen the EU's digital deterrence posture, taking into account existing capabilities, legal obligations and opportunities to improve knowledge and best practices.

### | Knowledge is Power: A CFSP-Based Digital Intelligence Capacity

The EU should establish a dedicated digital deterrence intelligence capacity under the CFSP, building on the existing EU Intelligence and Situation Centre (INTCEN). Rather than creating a new body, this approach would pool and analyse intelligence shared by Member States focused specifically on strategic threats to digital infrastructure and the actors behind them. If the Joint Cyber Unit is still a viable project, then its structure can be adapted to clearly fall under the INTCEN and CFSP frameworks.

This intelligence capacity is compatible with TEU article 4(2), as it relies on voluntary sharing of national intelligence. What this capacity would aim to do would be to harmonise, strengthen and clearly centralise information on digital threats. This would begin to overcome current fragmentation and improve situational awareness. The goal should be to proactively uncover, identify, and counter adversary actions before they escalate.

The EU should also be able to leverage this intelligence capacity as a deterrent tool by operationalising its intelligence for public warning of potential cyber threats. The quick declassifi-

cation of intelligence clarifying Russia's intentions in the lead-up to its invasion of Ukraine in 2022 is an example of how intelligence can be used to shape and coordinate actors around a shared intelligence picture. The same can, and should, be done for cyber threats, especially given the fast-moving nature of the threat.

In light of the growing transatlantic fractures, and although 23 of 27 EU states are also NATO members, this new intelligence capacity, and indeed broader EU actions regarding digital deterrence should exist independently of NATO. A Europe fit for the current geopolitical era means a Europe able to act independently, especially in the realm of digital security. Where necessary, the EU can cooperate with NATO. But fundamentally, it must act independently of NATO, and focus on strengthening European digital security.

### | Time to Act: Pre-Negotiated Templates for Attribution and Retaliation

To address the weaknesses of the Cyber Diplomacy Toolbox, the EU should establish pre-negotiated templates or standards for attribution and retaliation and place this under the prerogative of the CFSP. These templates would outline a menu of responses, from diplomatic démarches and asset freezes, to sanctions that could be flexibly deployed based on set evidentiary standards and procedural conditions in response to different types of digital aggression.

Agreeing on these templates would initially require unanimity. This step would take place once and in advance of any one specific incident. The goal is to have these structures in place before a digital security breach occurs.

This would serve a deterrence function akin to the Anti-Coercion Instrument, the ‘trade bazooka’ in European trade policy. By clearly signalling the consequences of digital breaches and providing a mechanism for rapid application (as opposed to the current structure of the Cyber Diplomacy Toolbox), the templates raise the anticipated cost for adversaries.

The application of these templates in a rapid and strategic manner lies in Article 31(2) TEU, which provides for qualified majority voting (QMV) in the Council for decisions implementing a Union action or position. If the templates are pre-agreed and adopted unanimously beforehand, their application against a given actor can be taken by QMV as an implementing decision. Naturally, this would require drafting the templates precisely and with clearly defined triggers, evidentiary requirements and sets of measures so that the activation does not itself create new policy. Additionally, given that actions with defense or military implications are excluded from QMV, the templates should be designed with measures that fall below that threshold, focusing on diplomatic, economic, and restrictive measures.

### Learn from the Best: Integrating Lessons from Ukraine

The EU should more comprehensively integrate lessons learned by Ukraine in its defence and offense against Russian cyber threats. Given that the EU and Ukraine already cooperate extensively on cybersecurity issues, whereby the Union most recently integrated Ukraine into the EU Cybersecurity Reserve, it is clear that Ukraine-EU cooperation in digital security remains a cornerstone of the broader relationship.

The Union should take full advantage of Ukraine’s existing cybersecurity capacities and the wider EU-Ukraine relationship, to set up a high-level working group involving the Commission, Council and EU agencies, alongside Ukrainian counterparts. The aim of this group should be focused on establishing a cohesive deterrence-focused digital security strategy within the European context, focusing on the strengths and weaknesses of Ukraine’s own experience.

## Conclusion

The EU’s ambition to be a geopolitical actor cannot be realised if its digital security strategy remains too focused on resisting attacks rather than also holding adversaries accountable. If Europe’s digital security is to be strengthened, then Europe must be able to meet these tense strategic moments with tools that can also be used to punish aggressive actors.

The policy recommendations proposed in this brief offer a pragmatic way to allow the EU to craft a digital strategy designed around shaping adversary actions. In an era where digital attacks are becoming a tool of statecraft itself, the EU must move toward a posture of credible digital threat deterrence. Only then can it claim to be an actor in charge of its own future.

*“The EU’s ambition to be a geopolitical actor cannot be realised if its digital security strategy remains too focused on resisting attacks rather than also holding adversaries accountable.”*

## | About Euro Prospects

Euro Prospects is an independent platform for in-depth analysis of European political affairs. We publish articles and policy briefs on the issues shaping Europe today, from the EU–Mercosur trade agreement and Europe’s semiconductor supply chains to the EU’s strategic positioning on Syria and Serbia’s global arms trade.

But informing readers is only part of our Mission. Euro Prospects was founded to help cultivate a European public sphere, a transnational space of political curiosity and civic engagement among Europe’s citizens. A healthy European democracy depends on citizens who transcend pro- or anti-EU debates and instead engage in the substantive policies before them.

To this end, Euro Prospects offers a platform for reflection and debate on Europe’s politics, policies, and prospects, bringing together a diverse team from across the continent.

[Visit Euro Prospects](#)

## | Partnerships

Are you an organisation interested in partnering with Euro Prospects? We are actively building relationships with researchers, institutions, and publications working on European policy. If you'd like to discuss this issue or explore ways to work together, email us.

[Contact Us](#)

## | About ESP

The ESP is Euro Prospects’ dedicated think tank unit dedicated to advising on EU strategic policy across security, technology, trade, energy, industry, and digital infrastructure.

**Francesco Bernabeu Fornara**  
*Head of Unit; Editor-in-Chief, EP*

**Giulia Convertini**  
*Digital Systems Sovereignty*

**Finn Sands Robinson**  
*Trade & Industrial Strategy*

**Rimsha Arif**  
*Energy Market Resilience*

**Matilde Minetti**  
*EU-China Strategic Competition*

**Orla Harris**  
*Digital Infrastructure Sovereignty*

**Jerfi Wigley**  
*Supply Chain Resilience*

**Annika Gerbig**  
*Defence Industrial Autonomy*

**Trinabh Banerjee**  
*Strategic Digital Security*

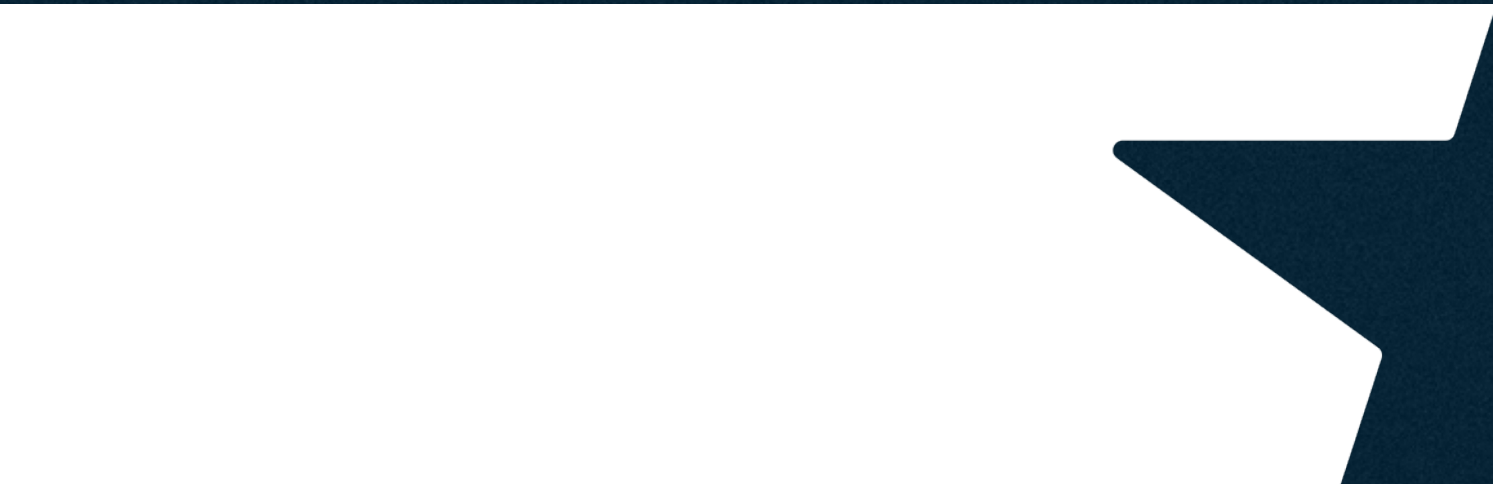
**Luka Okropirashvili**  
*Eastern Neighbourhood*

**Juan Carlos Leunissen**  
*Transport & Energy Connectivity*

**Antoine Cerqueira Da Costa**  
*Fintech Sovereignty Analyst*

**Sofia Cigolini**  
*EU Fiscal & Monetary Sovereignty Analyst*

**Erik Giuliano Würthner**  
*ESP Outreach & Partnerships  
Coordinator*



EP | *European  
Strategic  
Policy* 