GLOBSEC
IDEAS SHAPING THE WORLD

GeoTech Center

Beyond Resilience: Power, Coercion, and Credibility in European Cyber Strategy

Alexandr Burilkov

Framing the Problem

Over the past decade, European cyber policy has evolved from a primarily technical and internal market concern into a matter of strategic security. The 2020 EU Cybersecurity Strategy for the Digital Decade commits to build resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies and to strengthen operational capacity to prevent, deter, and respond to cyber incidents. The strategy further states that cybersecurity is essential for building a resilient, green, and digital Europe.

Although the language of deterrence appears explicitly, the analytical core of EU cyber policy remains centred on resilience. Prevention, regulatory harmonisation, supervisory mechanisms, and recovery capacity continue to structure the policy field. The underlying assumption is that reducing vulnerability will diminish both the likelihood and impact of malicious cyber activity.

This assumption is defensible in relation to opportunistic or profit-driven actors. It is less clearly sufficient in a strategic environment characterised by sustained state-linked cyber operations designed to signal, probe, and exert pressure below the threshold of armed conflict. In such a context, resilience mitigates harm but does not necessarily alter adversary incentives. The central analytical question is therefore whether the current resilience-oriented model can generate credible deterrence.

The 2017 Joint Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" recognised that malicious cyber activities can have devastating effects on economy, democracy and society at large and called for a framework for a joint EU diplomatic response to malicious cyber activities. The conceptual foundations for deterrence are thus present in EU doctrine. What remains less developed is a systematic articulation of how resilience, diplomacy, and economic instruments combine to shape adversary behaviour over time. The difficulty is therefore not a complete absence of means, but a weaker-than-necessary theory of how existing instruments can be sequenced, signalled, and repeated so that they shape adversary expectations. The Union already possesses a meaningful toolkit in the form of regulatory powers, sanctions authorities, cyber diplomacy instruments, law-enforcement cooperation mechanisms, and market-shaping leverage. The strategic gap lies in converting this dispersed repertoire into a more intelligible and actionable pattern of consequence.

The Current Posture: Institutional Consolidation and Strategic Ambiguity

The EU has constructed an extensive legal and regulatory architecture for cybersecurity. EU Directive 2022/2555 (NIS2) seeks to achieve a high common level of cybersecurity across the Union by imposing risk management and reporting obligations across critical sectors. EU Regulation 2022/2554 (DORA) aims to consolidate and upgrade ICT risk requirements as part of

the operational risk requirements in the financial sector.

In the diplomatic domain, Council Decision (CFSP) 2019/797 establishes a framework for restrictive measures against cyber-attacks threatening the Union or its Member States. This framework enables the imposition of targeted sanctions in response to significant cyber incidents.

Taken together, these instruments demonstrate institutional consolidation and regulatory sophistication. They reduce fragmentation across member states and embed cybersecurity within binding EU law. They also reflect an understanding that cyber threats are systemic and transnational. This matters because it suggests that the next step in European cyber strategy is not necessarily institutional proliferation. It is a disciplined use of the instruments already in place, with clearer expectations about how regulatory enforcement, attribution, diplomatic messaging, sanctions, and where necessary law-enforcement action relate to one another. A posture built on existing instruments, if employed consistently and cumulatively, may prove more credible than one centred on headline declarations unsupported by an observable pattern of action.

However, institutional consolidation does not automatically produce deterrent clarity. Sanctions have been imposed in a limited number of cases, and public attribution statements are often issued after protracted coordination. The resulting pattern of response may appear cautious and procedurally complex. From the perspective of deterrence theory, ambiguity regarding thresholds and consequences can weaken the signalling effect of available instruments.

Meanwhile, the threat landscape continues to evolve. ENISA's Threat Landscape 2023 reports that ransomware remains one of the prime threats to the EU and that threat actors increasingly exploit supply chain vulnerabilities. These trends indicate that adversaries are adapting to defensive measures rather than being deterred by them. The gap between defensive maturation and behavioural change remains analytically significant. They also point to a deeper structural reality. Much of the infrastructure exposed to cyber coercion is privately owned, privately operated, and often privately monitored. In practical terms, this means that the private sector is not an auxiliary actor standing outside European cyber strategy. It is one of the principal sites through which the Union's resilience, visibility, and response capacity are constituted.

Classical Deterrence and the Cyber Domain

Classical deterrence theory is grounded in credibility and clarity. Adversaries must believe that certain actions will trigger not just proportionate but also meaningful consequences. In the physical domain, retaliatory

capabilities were observable, thresholds were comparatively stable, and escalation pathways were structured, even if inherently dangerous.

For that reason, deterrence has never rested on capability alone. It has always rested on the credibility that capability will be mobilised, communicated, and sustained under political pressure. In the cyber domain this distinction is especially important. A capability that exists but is rarely activated, weakly signalled, or procedurally delayed may add little to adversary risk calculations.

Cyberspace complicates these conditions. Attribution requires technical investigation and political judgement. Legal thresholds remain contested. The United Nations Group of Governmental Experts affirmed that international law applies in cyberspace, but operationalising this principle in specific cases is complex.

NATO has sought to incorporate cyber operations within its broader deterrence framework. The 2022 NATO Strategic Concept states that cyber and hybrid operations against Allies could reach the level of armed attack. This formulation signals that cyber aggression is not categorically insulated from collective defence, while preserving political discretion.

For the EU, deterrence must operate primarily through economic, regulatory, and diplomatic instruments. The Union does not possess a centralised military cyber capability. Its deterrent potential therefore lies in multi- and cross-domain cost imposition and coordinated political signalling. The analytical challenge is to determine how these instruments can be configured to influence adversary expectations in a sustained manner. That challenge also sharpens the importance of EU-NATO coordination. The Union's comparative advantage lies in regulation, market power, sanctions, and civilian resilience. NATO's comparative advantage lies in collective defence, military signalling, and alliance consultation. If these tracks remain too weakly connected, adversaries may conclude that they can exploit the seams and gaps between civilian and military response. If they are aligned more visibly, the cumulative effect is likely to be greater than the sum of the parts.

From Resilience to Credibility

A resilience-oriented model assumes that reducing vulnerability decreases both the success rate and strategic utility of cyber operations. This assumption is valid but incomplete. State actors pursuing strategic objectives may tolerate higher operational costs if expected gains, including intelligence acquisition or political leverage, remain significant.

Credibility requires more than the existence of instruments. It requires consistent and intelligible patterns of response. The 2020 Cybersecurity Strategy commits to using all its tools and resources to prevent, deter and respond. Translating this commitment into deterrent effect implies clearer linkage between categories of malicious behaviour and structured repertoires of consequence. These need not take the form of publicly defined red lines, but they must generate expectations among potential adversaries. The analytical distinction here is important. Capability describes what the Union could in principle do. Credibility describes what adversaries expect it to do in practice. European cyber strategy will remain deterrence-light if instruments are treated mainly as reserve assets rather than as components of a patterned and cumulative signalling strategy. It is repeated, intelligible use, rather than abstract institutional inventory, that gives deterrence operational content.

Consistency is central. When restrictive measures, public attributions, and diplomatic actions are deployed predictably and in coordination with partners, they shape adversary risk assessments. When responses are rare or delayed, they risk being interpreted as largely symbolic. Over time, observable patterns of action are likely to carry more deterrent weight than declaratory language.

Alliance coherence further amplifies credibility. The 2016 EU-NATO Joint Declaration emphasised the need to broaden and deepen cooperation including in cyber defence. If EU regulatory instruments, national capabilities,

and NATO signalling operate in parallel without coordination, adversaries may perceive opportunities to exploit institutional boundaries. More regular coordination with NATO would therefore strengthen European cyber deterrence even without major institutional redesign. Joint consultation on attribution, shared crisis communication where appropriate, better alignment between EU diplomatic measures and NATO signalling, and more systematic integration of cyber scenarios into common exercises would all reduce ambiguity. The objective is not fusion. It is a more coherent division of labour that produces multi and cross-domain effects that are legible to adversaries.

The Political Economy of Cyber Coercion

Cyber coercion often unfolds incrementally rather than through discrete, high-visibility events. Activities such as pre-positioning within critical infrastructure, systematic intellectual property theft, influence operations, and the exploitation of supply chain vulnerabilities generate latent forms of leverage. These actions do not necessarily precipitate immediate crises. Instead, they expand an actor's range of strategic options in future contingencies and can shift the balance of bargaining power over time.

This dynamic intersects with debates on technological sovereignty. Sovereignty is frequently framed in terms of infrastructure control, data governance, and supply chain resilience. These dimensions are necessary components of defensive robustness. However, strategic sovereignty also encompasses the capacity to impose consequences and to manage escalation risk. Regulatory authority without credible enforcement mechanisms may produce an imbalance between normative ambition and strategic capability.

Europe's structural assets are considerable. The size of the single market, trade policy instruments, and sanctions regimes provide leverage that can be mobilised in response to malicious cyber activity. Coordinated export controls, financial restrictions, and legal actions can impose material costs. Their deterrent value depends on timeliness, repetition, and political cohesion across member states. Yet the operational effectiveness of these levers depends heavily on the private sector. Telecommunications operators, cloud providers, managed service firms, cyber security vendors, industrial operators, and major platform companies often see malicious activity first, hold critical forensic data, and manage the systems through which disruption spreads or is contained. In that sense, public authority and private capability are not parallel domains. They are interdependent layers of the same strategic posture.

Member state heterogeneity complicates cohesion. Threat exposure, economic interdependence, and strategic cultures differ across the Union. Nevertheless, deterrence operates at the collective level. An adversary need only identify where consensus is fragile to exploit that vulnerability. Strategic credibility is therefore shaped as much by political alignment as by technical capability. This gives greater weight to the institutionalisation of relations with industry. Ad hoc outreach after major incidents is unlikely to be enough. More formalised channels for information-sharing, protected mechanisms for technical evidence exchange, structured contingency planning, and clearer expectations for crisis cooperation would strengthen both resilience and deterrent credibility. The more routinised these relationships become before crisis, the more usable they are under pressure.

Institutional Implications

Embedding credibility within European cyber strategy requires reform rather than outright structural overhaul. At the strategic level, future EU policy documents could more explicitly integrate deterrence theory into cyber strategy. Resilience may be conceptualised as the baseline condition of security, while deterrence by cost imposition and signalling functions as a complementary pillar. This would also anchor a more practical shift in emphasis, from designing new instruments toward using existing ones with greater discipline and strategic coherence. The issue is less one of toolkit expansion than of clearer doctrine regarding sequencing, signalling, and cumulative effect.

At the operational level, coordination timelines among the Commission, the European External Action Service, the Council, and national authorities merit scrutiny. The signalling value of response is partly a function of speed and visibility. The same is true of public-private information flows. Where firms detect incidents first, hold telemetry, and manage affected systems, response timelines will depend in part on whether secure and trusted channels for information-sharing already exist. A more credible posture therefore requires not only state coordination, but faster integration of private-sector visibility into public decision-making.

At the political level, structured dialogue among member states regarding proportionality, escalation management, and cross-domain response options would strengthen coherence. Shared analytical frameworks can enhance collective credibility, even where operational details remain confidential.

At the alliance level, continued alignment between EU instruments and NATO crisis consultation mechanisms would reduce institutional ambiguity. Greater clarity regarding attribution processes and coordinated messaging would further reinforce deterrent signalling. Regularisation matters here. Coordination with NATO should not be reserved for exceptional moments alone. More habitual consultation, scenario-based planning, and aligned signalling practices would make European responses more predictable to allies and less exploitable to adversaries. In parallel, relations with industry would benefit from more formal structures, whether through standing consultation formats, secure coordination channels, or pre-agreed crisis protocols. The strategic purpose is straightforward: to ensure that the actors who own, operate, monitor, and secure much of Europe's digital infrastructure are integrated into response planning before incidents occur, not only mobilised after the fact.

Conclusion

The European Union has developed a substantial architecture of cyber resilience. Regulatory harmonisation, sectoral standards, and diplomatic instruments reflect institutional learning and sustained political investment. These measures have strengthened the defensive baseline across the Union.

However, the strategic environment is characterised by persistent, calibrated cyber coercion. In this context, resilience is necessary but not sufficient. A credible European cyber strategy requires clearer signalling of consequences, more consistent use of cost-imposition instruments, and closer alignment with alliance frameworks. It also requires fuller integration of the private sector into the Union's strategic posture, because visibility, ownership, and operational control over critical digital systems are distributed well beyond the state.

Moving beyond resilience does not entail abandoning normative commitments or embracing escalation. It entails integrating resilience within a broader framework of credibility. If adversaries come to associate coercive cyber activity with structured, cumulative, and timely consequences, deterrence may acquire operational meaning. Without such association, resilience risks functioning primarily as mitigation in a domain increasingly shaped by strategic competition.

Recommendations:

Strategic level — Explicitly integrate deterrence theory into future EU cyber policy documents, with resilience as the baseline and cost-imposition/signalling as a complementary pillar.

Operational level — Faster integration of private-sector visibility into public decision-making (not just state-to-state coordination).

Political level — Structured dialogue among member states on proportionality, escalation management, and cross-domain response options.

Alliance level — More habitual EU-NATO consultation, scenario-based planning, and aligned signalling practices (not reserved for crises alone).

Industry relations — More formal structures for engagement with industry — standing consultation formats, secure coordination channels, or pre-agreed crisis protocols.

GLOBSEC
IDEAS SHAPING THE WORLD

Vajnorská 100/B
831 04 Bratislava
Slovak Republic

+421 2 3213 7800
info@globsec.org
www.globsec.org