MARCH 2026

Enter Europe's Cyber Deterrence

By Alexander Klimburg

Executive Summary

Europe has entered a gray zone between peace and war. Russian hybrid warfare campaigns dominate the environment, leveraging cyber and information mechanisms to erode European cohesion and capacity without triggering a conventional military response. The implicit EU digital deterrence strategy—countering cyberattacks and information warfare through norms, entanglement, and resilience—does not sufficiently inhibit Russian hybrid campaigns. Moreover, the ability of the NATO to deter aggression by promising overwhelming retaliation largely based on U.S. capabilities aligns poorly with the scope of the Russian threat.

Instead, Europe must adopt a posture of compellence and independent deterrence, embracing cyber and information capabilities as a central instrument of statecraft. Neither the European Union nor NATO is structurally equipped to deliver the two necessary pillars of European cyber deterrence: (1) strategic operations in wartime and (2) gray zone compellence to counter hybrid warfare activities. Additionally, Europe remains highly dependent on U.S. cyber capabilities, creating strategic risk as U.S. involvement in European security declines.

To mitigate Europe's structural cyber vulnerabilities, this paper proposes a coalition of the willing: a **European Cyber Operations Group (ECOG).**

- **Overview:** a select group of nations operating under the European Intervention Initiative or a similar structure to strengthen the European component of NATO's "cyber umbrella." The ECOG would provide a single unified front with which to engage in counter-hybrid warfare cyber operations that could be considered countermeasures under international law.
- **Method of Operation:** a corkscrew governance framework—an adaptive coordination model that allows actors to draw on different levels of support, participation, and institutional anchoring depending on the mission.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

- **Enabling Factors:** substantial support and novel initiatives across three pillars.
  - **Targeted Strategic Investment:** Members must invest heavily in key capabilities, leveraging existing defense-oriented financial instruments.
  - **Modernized Procurement:** To convert investment into capability, ECOG must bypass sluggish acquisition cycles by adopting new and existing frameworks.
  - **Elite Workforce Development:** Acknowledging a massive shortfall in cyber professionals, ECOG should focus on personnel quality.

If Europe recognizes the integrated threat posed by Russian cyber and information operations and builds a cohesive capacity to withstand and respond, it can change Russia's strategic calculus and discourage future bellicose behavior.

European Perspectives Since 2022

> *"In the hybrid domain, perception matters more than certainty: the goal is not only to strike, but to instill doubt and insecurity."*
>
> *—Guido Crosetto, Italian Minister of Defense, November 2025*

As Russia's war against Ukraine enters its fourth year, Europe is increasingly sure worse is still to come. In June 2025, NATO Secretary General Mark Rutte **said**, "We are not at war, but we are not at peace either." Europe finds itself struggling to respond to a persistent Russian campaign of hybrid warfare and perceives a broader shortfall in military deterrence. Several leading officials, including President of the European Commission Ursula von der Leyen, have **called for** an urgent buildup of strategic capabilities to deter aggression.

Deterrence theories evolve alongside the strategic environment. European military powers increasingly recognize that their **current efforts are insufficient** to compel Russia to scale back gray zone activities intended to curtail support for Ukraine, undermine rearmament efforts, and limit Europe's ability to act. Further, Europe's comprehensive rearmament program must address a fundamental overreliance on the United States to effectively project a cyber umbrella as part of NATO's conventional deterrence mission. Cyber capabilities—and the digital environment as a whole—must constitute a focal point of this new dimension of European statecraft. Due to the structural limitations of both the European Union and NATO, neither institution can address these challenges alone.

DETERRENCE AND COMPELLENCE: BEFORE AND AFTER THE *ZEITENWENDE*

In recent years, both Western and Russian strategic planners have misinterpreted the costs and benefits of deterrence. One recent exponent of the current "fifth wave of deterrence theory" was put forward by the theorist Joseph S. Nye. His model envisions a **deterrence ladde**r with norms, entanglement, denial or resilience, and punishment. Scholarship has also focused on the close relationship between **compellence and deterrence**, especially within punishment.

Since 2022, there has been a marked shift in how NATO and many European military powers consider deterrence. Europe has shifted away from simple concepts of conventional retaliation and a policy of

general deterrence by punishment. **Deterrence by denial** is now a formalized NATO goal to confront Russian aggression, just as resilience is a focal point of many EU digital deterrence measures. At the same time, deterrence alone is broadly insufficient in the face of Russian hybrid warfare. Instead, Europe must compel Russia to scale back its activities intended to curtail European support for Ukraine, undermine Europe's rearmament efforts, and sap Europe's warfighting will. As such, **offensive cyber operations** are becoming an increasingly important focal point of a new era of European security.

Several authors have claimed that the West, and especially the United States, **failed to enact** a credible deterrence strategy in the aftermath of the 2014 Russian coup de main occupation of Crimea. Many subsequent acts of **Russian aggression** against the West seemingly went without cost to the Kremlin. Some believe a perceived **timid Western response** encouraged Russian President Vladimir Putin to embark on a massive escalation in 2022. The window during which Russia expected to suffer political and economic consequences for the invasion of Ukraine was short. This has become the Kremlin's most notable strategic miscalculation.

Many were surprised by the European political response in the first week of the war—well before it was clear Russia's military would fail to secure a rapid victory. Russia did not anticipate the readiness and speed of nearly all European governments and institutions to **enact sanctions**, signal political support, and provide Ukraine with military hardware and budgetary support. Russia likely underestimated the cumulative cost of previous cyber **norm violations**, which before 2022 had already cast it as an overall malicious actor. Russia also depended on achieving deterrence by entanglement via Russia's so-called "**energy weapon**"—its important oil and natural gas deliveries to Europe. Russia's miscalculations on deterrence, combined with the Biden administration's successful push to share **previously classified intelligence** on the Russian military buildup before the invasion, motivated European governments to resist.

German Chancellor Olaf Scholz proclaimed a **European *Zeitenwende***—a historic, epoch-defining turning point—just three days after the invasion; it was a rallying cry for a monumental rethink of European security. Two years later, however, some felt the ***Zeitenwende* had failed**. Germany, and Europe overall, had only partially delivered on the historic changes to Europe's defense readiness that was clearly needed. Partially this was likely due to wishful thinking on how the war would proceed. Given Ukraine's early battlefield successes, it seemed perfectly plausible, until the end of 2023, that the **war would conclude quickly** and on Ukrainian terms. The United States was also expected to remain fully committed to European security, consistent with a strategy formulated at the end of World War II. Both assumptions have proven wrong.

Since early 2022, the geostrategic situation has shifted repeatedly, with confrontations on battlefields and in political centers of power recasting fundamental pillars of European deterrence. Until the failed summer 2023 Ukrainian counteroffensive, the West seemed content to double down on **existing deterrence models**. Many policymakers, both in the United States and Europe, thought it was possible to return to previous approaches to counter malicious Russian behavior.

The Biden administration's October 2022 invocations of "**integrated deterrence**" were largely a continuation of existing U.S. and European policy. Deterrence was to be enacted across all domains of national power but largely relied on the threat of overwhelming military retaliation—deterrence by

punishment—to prevent broader Russian aggression. Below the threshold of all-out war, economic sanctions remained the most important compellence factor, and the West hoped this alone would force Russia to change course. Just as Russia overestimated the potency of its energy weapon in limiting political resistance to the invasion of Ukraine, the West overestimated the impact of compellence by entanglement—especially when economic warfare was, at best, tepid.[1]

RUSSIA'S STRATEGY OF RESILIENCE THROUGH INFORMATION SECURITY

Following the West's collective response to Ukraine, one of the greatest surprises was Russian economic and social resilience. **Early predictions** that Russia's economy would collapse due to sanctions by 2024 were widely incorrect. Russia's sociopolitical resilience has also confounded expectations. In February 2026, CSIS analysts assessed that Russia had suffered **1.2 million combat casualties**, with 325,000 fatalities, since February 2022. During particularly brutal phases of the war, such as fall 2025, NATO Secretary General Rutte said Russia was suffering **25,000 fatalities every month**—exceeding the total number of Soviet soldiers lost in the decade-long Soviet-Afghan War. While the **Soviet war in Afghanistan** bred significant civilian unrest in Russia in the 1980s, the Russian populace has, until recently, displayed a **remarkable level of passivity** in the face of this bloody toll.

A major factor in Russia's sociopolitical resilience is likely the Kremlin's dominance of Russia's information sphere. National information security was already considered an overriding national priority in 2000, and the publication of the first **Information Security Doctrine** (updated in 2016) treats Russia as a "**besieged fortress**" beset by foreign attempts of subversion. To counter this, Russia has invested heavily in complex reactive and proactive measures that have given the Kremlin dominance over most information generated and consumed by Russians. **Censorship** and highly advanced internal surveillance and message control measures are well documented and permeate all media consumption.[2] The government exercises overt propaganda but also engages in more subtle mass influence and preference setting. Together, these measures have been astonishingly successful. Large swaths of the Russian population **grudgingly accept** the "special military operation," take a nonpolitical stance, or are constrained by repressive surveillance and repression means. Just as the information domain is critical for domestic security, it also plays a decisive role in Russian security strategy abroad.

RUSSIAN DETERRENCE IS INFORMATION COMPELLENCE

Some scholars believe Russian deterrence thinking differs significantly from that of the West. They have **asserted** that the very concept of deterrence—which Western theory defines as preserving the status quo by discouraging adversary action—is largely alien to Russian strategic thought. Instead, they argue that **Russian strategy** has historically followed a policy of compellence—measures designed to change the status quo. From this perspective, Russian military force and coercive signaling are tools to proactively shape an adversary's behavior rather than merely prevent undesired actions.

---

1. For instance, U.S. sanctions began to have a significant impact on Russia only in 2025. Meanwhile, in the same year, Europe continued imported 15–19 percent of its energy from Russia. There has been remarkably little action against Russia's "shadow fleet" of tankers exporting oil, and European businesses have often sought to moderate more decisive action of their governments.

2. See, for instance, Serge Poliakoff, "ANO Dialog: Innovation in Controlling Russia's Digital Information," *Post-Soviet Affairs* 42, no.1 (2026): 107–30, https://doi.org/10.1080/1060586X.2025.2559218, and Human Rights Watch, "Disrupted, Throttled, and Blocked: State Censorship, Control, and Increasing Isolation of Internet Users in Russia," press release, July 30, 2025, https://www.hrw.org/report/2025/07/30/disrupted-throttled-and-blocked/state-censorship-control-and-increasing-isolation. On external influence, see Maxime Audinet and Colin Gérard, *Under the Radar* (Washington, DC: George Washington University, November 2024), https://therussiaprogram.org/russia_information_influence.

> *Russian strategy has historically followed a policy of compellence—measures designed to change the status quo.*

The Russian word ***sderzhivanie***—used in strategic documents—encompasses deterrence, coercion, intimidation, and even warfighting preparation within a single framework. It consists of demonstrative or limited use of force to prevent aggression and de-escalate conflicts on favorable terms. Samuel Charap **argues** that Russian blurring of deterrence and compellence represents a fundamentally different strategic culture, one that considers controlled escalation a legitimate and even stabilizing tool of statecraft rather than an avoidable outcome. This fundamentally conflicts with the Western peacetime-wartime dichotomy rooted in international law.

"Active measures"—a long-standing Soviet-era concept akin to hybrid war—is a key instrument to accomplish sderzhivanie in peacetime through asymmetric means. This is encapsulated in the often entitled "**Gerasimov Doctrine**," which defines indirect or asymmetric warfare as the new normal and positions informational means of conflict as supreme.[3] Building on nearly half a century of strategic thought and the so-called Reflexive Control Theory, the Gerasimov Doctrine has shaped a Russian concept of **information confrontation**, which seeks to blend technical and informational activity in cyberspace to achieve psychological effects and dominate the adversary. Information confrontation covers a range of overt, covert, and plausibly deniable third-party activities in cyberspace and adjacent arenas. As such, hybrid warfare measures are intended to weaken European will to fight, undermine public trust, and fracture cohesion within and among Western states—all as a potential precursor to a wider conflict to be resolved on Russia's terms. Hybrid warfare is not simply a subordinate strategy but a key effort to prevail in political-military confrontation, one that did not start in February 2022 but has been ongoing at least since 2014.

THREE PILLARS OF RUSSIAN INFORMATION CONFRONTATION

Russian efforts to compel through **nuclear threats** have been well documented, but hybrid warfare efforts are equally important and increasingly relevant. Researchers have documented **219 incidents** of suspected Russian hybrid warfare in Europe between 2014 and 2025, including sabotage, assassination attempts, and electromagnetic attacks, with almost half (46 percent) occurring in 2024 alone. In February 2026, German media **revealed** that authorities had counted **321 cases of sabotage** in Germany in 2025 alone.

The first pillar of Russian hybrid operations comprises cyberattacks against critical infrastructure. Attacks attributed to Russian state actors are common. In 2025 and early 2026, Russian hackers targeted **Polish critical infrastructure**, a **Norwegian dam**, **Danish utilities**, **EU institutions**, and perhaps other targets in attacks that remain officially unattributed. Distributed denial-of-service (DDoS) attacks **routinely interfere** with internet traffic across Europe. These operations are intended to cause direct physical harm and spread fear and chaos.

---

3. While not a doctrine per se, the publication of Russian Military Chief of Staff Valery Gerasimov's article in 2013 (nearly exactly a year before the occupation of the Crimea) is largely seen as the cumulation of traditional Russian thinking on the benefits and utility of asymmetric warfare. It also provides the justification to do so—a need to push back in a counter-struggle against purported Western-backed pro-democracy movements.

The second pillar of Russian hybrid warfare is physical attacks facilitated by cyber means. These include attacks on **railroad infrastructure**, threats of assassination and physical intimidation of **key figures**, sabotage of **subsea cables**, and **domestic terrorism**. Many of these are carried out by European "**throw-away agents**," often petty criminals recruited via social media for extremely modest pay—for instance, Bulgarian criminals enticed to engage in false-flag antisemitic **vandalism** in France were paid €1,000 for the task.

The third pillar of Russia's hybrid campaign is information manipulation and disinformation aimed at weakening societal trust and influencing political outcomes. Operations such as **Storm-1516**, a Russian-linked social media network, have produced and disseminated misleading content targeting elections and public debates. This operation spread narratives designed to discredit Western political leadership and foster polarization, particularly around support for Ukraine. These overt efforts are combined with subtle, difficult-to-attribute efforts to influence national debates by amplifying stories and messages that **deemphasize support for Ukraine**, which plays a key role in shaping European perceptions.[4] High-profile victims have seen their personal information stolen and publicly posted, further weakening public trust.

The hallmark of **Russian hybrid information operations** is that each pillar operates in multiple domains simultaneously.[5] In the model sketched out by General Gerasimov, these methods are intended as precursors for open military confrontation. A **February 2026 Harvard study** indicated this could take the form of a small border violation that challenges NATO and EU unity, or even an outright attempt to isolate the Baltic states militarily. Previously, European nations may have felt that even a "**salami tactics**" approach—slicing away at large objectives or opposition groups in a **piece-by-piece manner**—would meet a firm NATO response, carried by the United States. But the recent **U.S pivot** away from European security has proved the single-largest transatlantic upset in post-World War II history and has greatly increased European urgency to act.

LIVING WITH THE U.S. PIVOT

The U.S. pivot from Europe is not new. The term was first used in 2011 to describe President Barack Obama's **focus on the Indo-Pacific**. However, transatlantic security relations entered a new dimension following President Donald J. Trump's 2016 election. His administration **made it clear** that NATO should not take the U.S. commitment to Article 5 solidarity for granted. Originally, many Europeans hoped that this was yet another attempt to make them take defense expenditure seriously—most NATO members fell well short of the then-spending target of **2 percent** of gross national product—but the European mood has since **shifted considerably**.

Europe has experienced U.S. threats to **draw down troops** in Eastern Europe; uncertainty over the provision of intelligence, logistical support, and combat enablers; ambiguity about U.S. willingness and ability to counter Russian (and Chinese) compellence; and political capriciousness and outright

4. Such messages include "It is not our war," "Western warmongering," "Russian victory is inevitable," and "We have issues other than Ukraine to worry about." Russia has openly supported political parties in the West that align with these aims and seeks to encourage reporting on issues seen as conducive to their efforts—for instance, irregular migration, often considered the single most divisive issue in many EU member states. The European Union has repeatedly described Russian attempts to encourage irregular migration (most visibly at the Polish and Finnish border, but also elsewhere) as part of a hybrid warfare strategy.

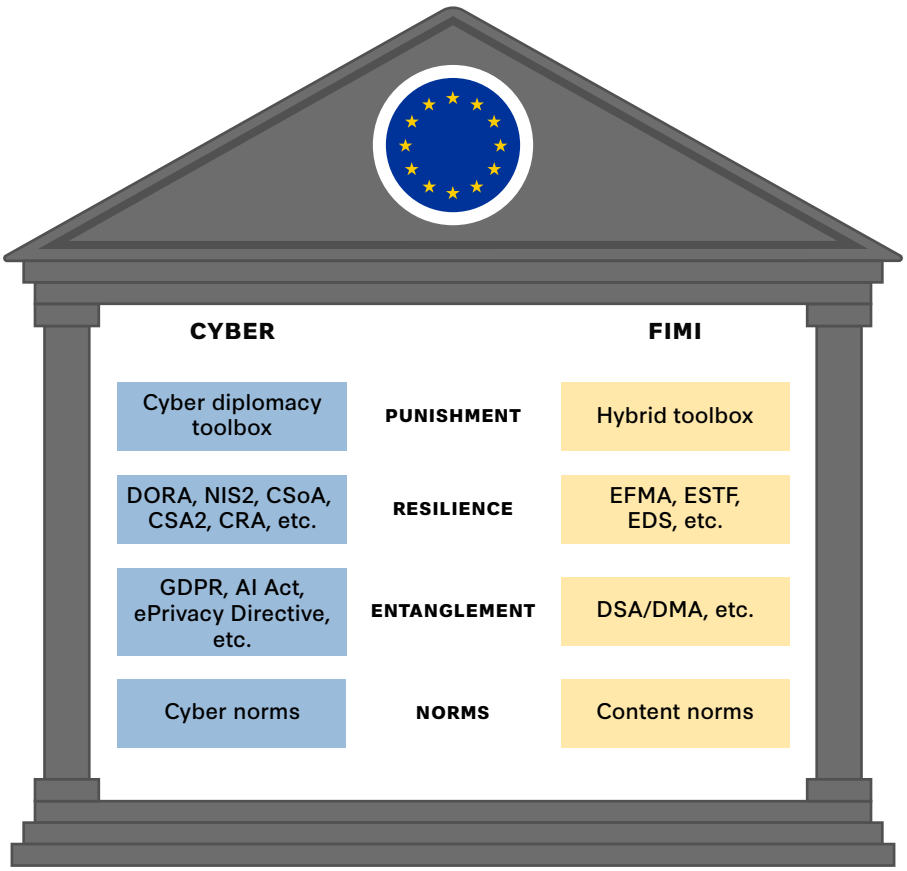
5. Joseph Nye once described this approach to political power as the "three faces of power"—overt coercion, more subtle co-option, and finally, the most subtle of all, conviction. According to a former U.S. general speaking at a February 2015 dinner, this model is one of the reasons that Russia "considers Joe Nye the secret architect of American power." See also Nye (2011), *The Future of Power.*

hostility by the Trump administration. Europeans see this reflected in the **2025 U.S. National Security Strategy** and recent questioning of Danish sovereignty over Greenland, which have fundamentally **shaken confidence** in the United States as the "**indispensable nation**." Europe's shortfall in offensive cyber capacities and the urgency to acquire them likely outstrip even most conventional military rearmament needs. Whether the U.S. pivot is due to priorities, politics, or profits, Europe must learn to resist foreign compellence and do so from a position of strength.

EU Digital Deterrence: A Four-Level Paradigm

While the European Union lacks an official digital deterrence strategy, one exists implicitly between its economic policies, cyber, and counter-hybrid measures. Two key pillars relate to countering critical infrastructure cyber threats and resisting complex information warfare campaigns—or what the European Union calls "**foreign information manipulation and interference (FIMI)**." Historically, these domains have been kept separate. However, the rationale for separation has eroded as Russia increasingly merges both cyber and FIMI activities.

Figure 1: European Digital Deterrence



Source: Author's analysis and Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (January 2017): 44–71, https://doi.org/10.1162/ISEC_a_00266.

The EU digital deterrence strategy reflects Europe's broader international roles as a normative power, regulatory hub, and increasingly security-aware actor in a multipolar age. The European Union has

powerful tools to deter both cyberattacks and FIMI, but considerable gaps remain—especially in the upper-end of the deterrence ladder.

> *The EU digital deterrence strategy reflects Europe's broader international roles as a normative power, regulatory hub, and increasingly security-aware actor in a multipolar age.*

NORMS: SHAPING INTERNATIONAL AND REGIONAL EXPECTATIONS

Normative engagement constitutes the foundational layer of the EU digital deterrence strategy. In international relations, norms are key to defining appropriate conduct by states, referred to as "**soft law.**" Norms also work at a more subtle level to shape specific interests.[6] For this reason, Russia long rejected the term "**cyberspace**" in international discussions as Western framing. The European Union's **normative logic** is rooted in international law and multilateral engagement, seeking to influence adversaries' cost-benefit calculations by reinforcing commonly accepted standards.

The European Union consistently champions responsible state behavior in cyberspace in international forums. In its statements to the United Nations, the European Union **affirms** that international law, including the UN Charter and existing norms of state conduct, applies fully in cyberspace and **supports** the continued work of the United Nations Group of Governmental Experts (GGE) as a mechanism to build consensus on voluntary, nonbinding norms of responsible state behavior. The UN GGE has been repeatedly mentioned by high-level government ministers worldwide and was **endorsed** by the UN General Assembly in 2015, opening the door for the Open-Ended Working Group. Despite the Ukraine war, the working group delivered ab in July 2025 establishing a "global mechanism" to discuss cyber threats annually. The European Union has also actively **promoted** similar discussions in multilateral settings, such as the G20, and in regional groups, such as the African Union. The European Union was also an early believer that internet content should be subjected to **agreed-upon norms**.[7] Like most norms, these agreements are considered politically rather than legally binding.

EU norms promotion demonstrates commitment to the rules-based international order. While some consider norms to be toothless, the global response to Ukraine has shown that collectively identifying violations can helpfully establish a global coalition. In March 2022, the UN General Assembly adopted by an overwhelming majority a resolution **rejecting the Russian invasion**. Russia's repeated norm violations prior to the invasion made it abundantly clear that its actions were driven by a long-term

6. For nearly 20 years, Russia was steadfast in refusing to use the term "cyberspace" to discuss matters pertaining to the use of information and communication technologies within the UN context. It also was extremely consistent in promoting its own narrative terms, such as the threat of "cyberterrorism," as an effort to mainstream concepts core to its own security interests, such as internet content considered a threat to the interests of the state.

7. For instance, the Christchurch Call—initiated by New Zealand and France following Christchurch mosque shootings in 2019—is a set of commitments to bring together actors to combat the use of social media to organize and promote terrorism and violent extremism.

malicious calculus, despite its protestations otherwise. However, after 2023, when the prospect of a quick resolution to the war had receded, Russia **exploited the failure** of Europe and the United States to build upon this global consensus.

ENTANGLEMENT: INTERDEPENDENCE AS STRATEGIC LEVERAGE

Entanglement refers to **complex interdependencies**—economic, regulatory, and institutional—that raise the cost of hostile digital conduct. Unlike overt actions, entanglement works indirectly to shape adversaries' incentives by embedding them in structures that discourage confrontation or interference. Entanglement is directly connected to norms of behavior, in that violation creates implicit costs. The European Union constitutes the world's **second-largest economy** by GDP, providing considerable market power. Access to this market is increasingly managed through expansive regulations that also export European norms worldwide.

European leaders have demonstrated their desire for Europe to become the world's **digital regulator**. Early legislation had some success in this objective, in particular the **2016 General Data Protection Regulation (GDPR)**. As Europe's comprehensive data privacy law, the GDPR has been widely emulated abroad and serves as an example of the "**Brussels effect**," despite being reviled as antibusiness as much as it is considered a win for consumers. More recent regulations have continued these efforts. The Digital Services Act and Digital Markets Act constitute a **twin regulatory framework** designed to rebalance digital markets and make online environments safer and more accountable. The Digital Services Act imposes transparency and content moderation requirements on several companies offering digital services, especially large online platforms, making them accountable for digital risks, including FIMI. By contrast, the Digital Markets Act went into force in 2024, seeking to increase competition between the "gatekeepers" of the digital economy, with less bearing on FIMI or cybersecurity.

Economic considerations fundamentally drive these initiatives as part of the European Commission's long-term strategy to fully enact a **digital single market** in Europe. The **EU International Digital Strategy** represents a key accompanying effort, aiming to boost European competitiveness, promote a digital agenda focusing on the security of Europe and its partners, and shape global digital governance and standards. **Affiliated dialogues** with Canada, Japan, Singapore, and South Korea are ongoing. Facilitating digital trade plays an equally key role. Both stand-alone digital trade agreements, such as with Singapore and with South Korea, and wide-ranging digital trade chapters within larger planned trade agreements, such as with Indonesia, provide significant opportunities to bind foreign countries more closely with Europe.

EU research funding and the opportunity to invest in large projects also help entangle international interest in Europe's security. Many programs dedicated to artificial intelligence (AI), cloud, and other new technologies exist and continue to expand. For instance, the Horizon 2020 framework may see its research budget for 2028–34 rise to **€175 billion**. These dynamics represent the opening to what increasingly constitutes the single main framework for European digital resilience: the multipronged "**digital sovereignty**" strategy. The European Union has fully committed to the idea of digital sovereignty as a new binding framework, which will shape both resilience and entanglement for decades to come.

Lastly, the European Union increasingly understands that a veritable flood of regulations tests the ability of the private sector to respond and even threatens to lessen the attraction of doing business in Europe. In response, the European Union has embarked on a **digital omnibus revamp** that seeks to simplify various parts of existing legislation, including elements of the GDPR, AI Act, ePrivacy Directive, Network and Information Systems Directive 2, and other regulations. The European Union's ability to leverage economic interdependence to bolster digital resilience will depend on executing this agenda. In other words, the European Union's success in bolstering resilience and entanglement will hinge on simultaneously offering streamlined, harmonized, predictable, rule-based regulations (making the European Union an attractive place to do business) and achieving EU economic goals.

RESILIENCE: DENIAL AS DETERRENCE

Resilience—the capacity to absorb, withstand, and recover from all kinds of incidents—is the core of **deterrence by denial.** Instead of threatening retaliation, resilience undermines adversaries' strategic benefits by making attacks less effective and more costly. In nuclear deterrence, a core element of **denial** is hardening command and control structures but also protecting the "value"—the population and wider industry—to limit the attractiveness of an attack.

"**Resilience**" is the most commonly invoked word in the European Union related to security. It is liberally applied to many of the so-called **digital agenda** legislative acts. While originally interpreted in a technical sense, it is now increasingly used in a political context. The rapidly developing **EU digital sovereignty strategy** is thus shifting the meaning of digital sovereignty to encompass basic cybersecurity and societal resilience from psychological coercion, as well as independent and secure supply chains.

The European Union has constructed a dense and multilayered framework for **cyber resilience** that reflects internal market logic and growing geopolitical concerns over systemic vulnerability. Since 2017, nearly **100 legislative acts** have been passed. Some, like the financial sector-specific **Digital Operational Resilience Act**, are concentrated on a certain industry or service. But some legislation reaches further. The **Network and Information Systems Directive 2**, though slow to transition to national law, will significantly expand the scope and enforcement of cybersecurity requirements by replacing voluntary cooperation with harmonized risk management, stronger oversight, and clearer accountability across key sectors. This framework goes well beyond classical critical infrastructure protection and will likely impact over 160,000 public and private entities in Europe alone, with violations triggering substantial penalties. The sister legislation, the **Critical Entities Resilience Directive**, sets out physical security requirements for the same entities.

The updated **Cybersecurity Act 2** may also allow the Commission to designate a non-EU entity as "high risk" and force its removal from EU information and communication technology supply chains and services (including 5G/6G networks). The **Cyber Resilience Act** extends the European Union's preventive approach to the product level, embedding cybersecurity baseline requirements across the life cycle of digital products and software and aligning cyber resilience with broader single-market regulation. The **Cyber Solidarity Act** is dedicated to addressing large-scale incidents and includes setting up a "cyber shield" of cross-border security operations centers and a Cybersecurity Emergency Mechanism, with a standby EU Cybersecurity Reserve recruited from industry.

EU resilience to FIMI is seemingly less pronounced but often overlaps with cyber legislation and benefits directly. Counter-FIMI resilience also draws on the **2024 EU regulation** on transparency targeting of political advertising to track foreign interference and ensure large platform operators take due diligence seriously or risk significant penalties. The **European Media Freedom** Act helps address concerns about political interference, declining journalistic independence, and opaque media markets.

The most significant step is to come—the **European Democracy Shield (EDS)**. The EDS was announced in November 2025 and is still in draft. It may build on or include one of Europe's most visible counter-disinformation bodies, the **East StratCom Task Force**, and its flagship program, EUvsDisinfo, a group of fact-checkers exposing FIMI efforts. The EDS will be enacted through avenues that encompass some existing cybersecurity legislation. New elements are likely to include the Centre for Democratic Resilience—a media resilience program—and an overarching strategy for civil society engagement. Strong interest from the Commission president and the European Parliament likely means the EDS will feature prominently in 2026.

PUNISHMENT: THE BLUNT END OF THE SPEAR

Any successful deterrence approach must include punishment. Although the European Union aspires to be a supranational entity encompassing all levers of state power, security issues have—by design—been the least-integrated policy area. Formerly considered the second pillar of the European Union, control over **national security and defense** is still largely in the hands of individual member states. Although the Treaty of the European Union established a mutual defensive obligation (Article 42.7, "**Mutual Defence Clause**"), EU efforts to create a **functioning security union** have faltered. Although multiple attempts have been made to **expand** the roles and duties of EU military staff, the only military forces currently provided by EU member states are in numerous flagged peacekeeping operations, as well as the never-tested **EU Battlegroups** rapid reaction force concept. On virtually all **Common Security and Defence Policy** issues, the current rules demand unanimity by all member states voting in council.

To enable like-minded cooperation on security issues, two widely differing initiatives have been pursued. The **EU Permanent Structured Cooperation** instrument was enabled by the Treaty of the European Union to allow member states to deepen cooperation on important issues, but it is a capacity-building and readiness initiative, not a mechanism to field forces or plan operations. Outside the EU structure, the French government proposed a **European Intervention Initiative** in 2018 to create a common strategic culture and provide joint forces for ad hoc missions. Currently, 14 nations have signed up, including the United Kingdom. Most operational is the UK-led **Joint Expeditionary Force**, inaugurated in 2014 and with all Scandinavian nations and the Netherlands as partners. It is designed to deploy an expeditionary capability of up to 15,000 troops on demand. However, these initiatives are designed to operate **next to NATO**, not replace it. NATO remains the principal tool for deterrence by punishment in Europe.

EU options are severely limited and principally economic. Under the Common Security Defence Policy **Cyber Diplomacy Toolbox**, the EU specified a road map with the *ultima ratio* to enact economic and individual sanctions against entities accused of malicious cyber acts. This was expanded with a **Hybrid Toolbox** intended to counter FIMI and hybrid warfare abilities. These toolboxes have been used five times to date and do not include the much wider-reaching **sanctions regime** enacted against

Russia following the Ukraine invasion. The general sanctions regime is, however, marred by numerous carve-outs and exceptions, **limiting efficacy**. The **2022 Anti-Coercion Instrument**, which allows the Commission to retaliate swiftly with tariffs or other economic measures, is a potentially powerful (non-cyber or FIMI) deterrence measure not yet used.

There is wide-scale acknowledgment across policy circles that the European Union needs to do much more to expand its capabilities to deliver punishment. Recent discussions have centered around expanding the **Foreign Direct Investment Screening Regulation**, allowing the Commission to step in and limit (or even reverse) national or commercial investments by non-EU entities posing an overall threat to the European Union. But Russia's hybrid war against Europe often falls in a gray area not adequately covered by deterrence—above the EU economic sanctions that seem only marginally successful but beneath NATO's Article 5 retaliatory measures.

Europe's greatest tool of punishment remains inflicting economic harm while spending money on defense. Several senior EU officials have said in closed settings, "We will outspend Putin," invoking the **significant mismatch** in EU and Russian economic power. However, it is unlikely that Russia's principal strategy with Europe will be to wait for that obvious power to unfold over time. Hybrid warfare is likely not just part of Russia's strategy but its principal one, seeking to contribute to or even achieve victory before the full force of Europe's economic might unfolds. The European Union's inability to address it directly means responses to hybrid warfare attacks have largely defaulted to individual EU nations. As such, Europe often operates as less than the sum of its parts.

Europe's Hard Road to Compellence in Cyberspace

Core to European military deterrence, NATO for many years maintained a declared policy of **massive retaliation**, though it has since evolved to include greater elements of deterrence by denial, such as the Eastern Flank Deterrence Line. For decades, **NATO's conventional military capabilities**—led by the United States—profoundly overmatched those of any potential aggressor. Without the United States, even on base metrics such as numbers of modern tanks and fourth- and fifth-generation aircraft, Europe represents a major military power. Immediately following the Cold War, Russia did not represent an acute military threat. Until 2014 there were significant efforts expended on **cooperation between NATO and Russia** on a host of issues, including troop deployments in Afghanistan.

Russian rapid rearmament may soon **challenge** NATO's ability to defend the Baltics, as well as Scandinavia and the Eastern Balkans, if the Ukraine war is concluded. More alarmingly, Russia under Putin may have the ambition to seek this wider confrontation. Regarding when an attack on a NATO ally might occur, Simon Saradzhyan **collated** over 30 predictions by leading European and U.S. public figures, and all assessed a date from 2027 to 2030.[8] Europe has engaged in a crash **rearmament program**, but confidence in meeting this **challenge** by 2030 is low. The United States will remain, at least in the short term, a crucial enabler of **essential capabilities** underpinning all aspects of European military deterrence. While discussions on supply, intelligence, and communication assets receive the most attention, European dependence on U.S. cyber capabilities is just as extensive. The possibility the United

8. After 2035, the European security landscape will likely be substantially different, as Europe's massive rearmament program should address the imbalance in at least conventional forces, though the hybrid and strategic weapons threat would largely remain the same.

States might be fully engaged in other conflicts, such as with China, or simply pivot away from European security, means Europe now faces what the EU high representative calls an "**existential threat.**"

"PUNISHMENT" AND OPENING EUROPE'S CYBER UMBRELLA

For nearly a decade, a de facto cyber umbrella has been taking shape within NATO security structures. However, unlike the nuclear umbrella—which also can count on UK and French capabilities—the cyber umbrella depends largely on the United States.

The NATO doctrine for deploying this umbrella is the **Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)** framework. SCEPVA was a groundbreaking concept when first publicized in 2018 and has been further **built out** since 2022. SCEPVA gives NATO's Supreme Allied Commander Europe (SACEUR) the ability to call for offensive cyber operations as part of an overall military campaign. While the cyber mission sets and terminology remain classified, approximations of conventional military missions will likely form an important part of these cyber operations. These include counter-command-and-control strikes (against communications systems and military commands), interdiction operations (against troops moving to the battle area and their supplies), and deep precision strikes (on critical infrastructure).[9] SACEUR would deliver a request for a **SCEPVA mission** to allies via the NATO Cyberspace Operation Centre, which would then match the request with an ally to deliver on it, who would then directly coordinate with SACEUR at an operational level.

The **Cyber National Mission Force (CNMF)**, a subcommand of U.S. Cyber Command, would likely deliver U.S. capabilities for SCEPVA. The CNMF reportedly has a complement of roughly 6,400 personnel, supporting **133 teams** with regional and thematic leads. According to the **CNMF mission statement**, it engages in "scalable offensive cyber capabilities to hold at risk a range of assets that the leaders of strategic adversaries value most highly."

Before 2022, several European allies had already stood up significant cyber commands of their own. Today, all major NATO and EU nations have operational cyber commands. Only the United Kingdom has publicly announced a **National Cyber Force** akin to the U.S. CNMF, but most EU and NATO nations operate **declared offensive cyber units**, even if they are hybrid units shared with intelligence agencies.[10] U.S. intelligence and cyber operators have reportedly **worked closely** with European commands and intelligence agencies, including to secure new insights or access.

The development of independent European cyber capabilities, though nascent compared to U.S. capabilities, has been comparable to historical nuclear developments. **NATO's nuclear umbrella** was primarily provided by the United States, but increasingly depended on European nuclear sharing initiatives.[11]

---

9. According to author interviews, SCEPVA does not include a key area of cyber conflict known as Cyber Electromagnetic Operations (CEMO, also CEMA). CEMO has been called "battlefield cyber" and includes many of the activities seen in conventional electronic warfare operations as well. This field is rapidly expanding in significance and not merely due to its ability to counter drones and long-range fires. According to recent industry reports, CEMO may no longer depend on expensive singular platforms (such as the EC-135 aircraft, of which Europe holds very few) for delivery but may be delivered using types of ASEA systems found in many European aircraft. If accurate, these reports indicate a historic transformation of the deployability of battlefield cyber means within the next few years.

10. One published version of this is the Dutch Joint Sigint Cyber Unit, first stood up in 2014 and likely akin to the original National Security Agency Tailored Access Operations unit.

11. Before the nuclear sharing arrangement took root in the 1970s, there was wide-ranging discussion between the United States and Europe on how to share nuclear deterrence. Successive U.S. administrations from Dwight D. Eisenhower to Lyndon B. Johnson

A cyber umbrella might also require proficient European partners to deliver cyber effects alone or in conjunction with the United States—or at least to stay out of the way. Cyber mission deconfliction is a known problem for many actors. However, despite over a decade of cyber experience in European armed forces, **European capabilities** are largely considered far less sophisticated than those of the United States. At the same time, experts have **argued** developing a "minimum deterrence" strategic offensive cyber capability for many European small and medium powers is possible.

There is remarkably little available material on the effectiveness of any strategic cyber campaign, and estimates range considerably. The lessons of Ukraine can be completely applicable or not at all, given how little is public regarding cyber operations in early 2022. A glimpse of what a country-crashing cyber campaign could look like was the leaked Obama administration contingency cyberwar plan against Iran called Nitro Zeus. Nitro Zeus was a **comprehensive cyber campaign** aimed at crippling Iran's critical infrastructure and cost "millions, maybe billions" to prepare.[12] However, some European analysts have claimed strategic cyber deterrence effects were "**overrated,**" especially compared to minimum nuclear deterrence. These statements demonstrate that associating nuclear weapons with deterrence confuses what cyber operations can contribute to multidomain national defense.

A better conventional comparison for a strategic offensive cyber capability may be the new deep precision strike mission requirements in several European militaries. Sweden, for example, recently **published** its stated aim to acquire a long-range cruise missile capability with at least a 2,000 kilometer range—a power projection capability far beyond anything the country could have previously aspired to. The rush to purchase and design **long-range drones and cruise missiles** is also apparent in industry research endeavors such as the European Long-Range Strike Approach (ELSA), which is explicitly aimed at developing a European version of the Tomahawk cruise missile. Clearly, European militaries are desperate to acquire any kind of deep strike capability.[13]

COMPELLENCE IN TIMES OF NON-PEACE

In 2018, the U.S. Department of Defense engaged in a **doctrinal pivot**, marking a comprehensive break from past views on cyber deterrence. The United States would not continue to simply react to significant malicious cyber behavior on a case-by-case basis; it would actively pursue and engage bad actors on its own terms and without lengthy approval processes. Persistent engagement was **explained** and **endorsed** by U.S. General Paul Nakasone, head of U.S. Cyber Command and the National Security Agency, thus providing apparent carte blanche for a wide range of offensive cyber operations. Persistent engagement would "degrade the infrastructure and other resources that enable our adversaries to fight in cyberspace" and "raise the costs that our adversaries incur from hacking the United States."

---

actively proposed a NATO Multilateral Force of dedicated warships and ballistic missile submarines staffed by NATO personnel in a pan-European fleet and armed with their own nuclear-equipped missiles. Launch approval would be delegated to SACEUR. The plan likely failed due to French and UK resistance, as these nations had already fielded autonomous nuclear capabilities.

12. In contrast, an Austrian Ministry of Defence official revealed in 2018 that a crippling cyber and physical attack on Austria would require very limited resources—as little as €10 million according to *Der Standard*.

13. The urgency of Europeans dashing to acquire this hallowed deep precision strike capability has extended to questions of the adapting planned new cargo aircraft as cruise missile carriers. This was expressly mentioned in the Franco-British Lancaster House 2.0 Declaration of 2025 and may also apply to the Brazilian C-390 medium-lift cargo aircraft replacing the C-130 Hercules in some European air forces. Clearly, European militaries are desperate to acquire any kind of deep-strike capability. Strategic cyber capabilities, even if of limited effect, could likely contribute significantly to this mission – and at a fraction of the price, if the human resources can be found and maintained.

Persistent engagement as a theoretical framework and operational doctrine has faced **significant criticism**. What is certain is that **persistent engagement** changed markedly as an operational policy, especially in terms of retreating from overt signaling of specific operations that may have come close to violating international law and were contentious to some experts. It also did not result in de-escalation of cyber tensions, as shown by any cursory review of the long list of **serious cyberattacks** on the United States since 2017. However, persistent engagement has highlighted the importance of compellence. More **recent deterrence theory** has explored the interplay of deterrence and compellence, and it is evident that non-peace (or quasi-war) compellence is a route to restoring deterrence—clearly a principal objective for Europe today.

> *It is evident that non-peace (or quasi-war) compellence is a route to restoring deterrence.*

Responding to Russian belligerence toward Europe with compellence in cyberspace can be legal under **international law**, which generally agrees it is acceptable for a state to respond to another state's unlawful act with countermeasures that would normally be unlawful. Most cyber operations that would likely claim this status could be designed to comply with the most current interpretation of the law. Operations that would likely fall in this category could be connected to **statements of condemnation** or EU sanctions announcements made via the **EU Cyber Diplomacy Toolbox**. They could also be public, semipublic, or completely covert, known only to the perpetrators and possibly the victim.

This point on communication of cyber compellence activities is crucial. These capabilities can be, and perhaps already are, exercised covertly without any public discussion. However, this would violate the so-called **Cartwright Conjecture** that bedeviled earlier U.S. experiences—namely, that a lack of public communication is inimical to deterrence. For deterrence to work, one must **communicate** not only a technical capability but also the credible will to use it. If efforts are conducted clandestinely, even in conjunction with others, this indicates a lack of resolve by the exercising states. This, in turn, could be perceived as weakness by the state suffering compellence and therefore invite further escalation attempts. The only logical move to forestall further escalation following a compellence act is to indicate willingness to stand by these measures and implications—and therefore politically demonstrate willingness to match escalation, if necessary. Few European nations want to walk that road alone.

Stumbling Forward: Europe Reaches for a Unified Capability

Europe is faced with two overriding cybersecurity concerns. First, it must field a credible deterrence-by-punishment strategy that can be meaningfully and demonstrably employed in all-out conflict, including against a resurgent Russia. Second, it must have the ability to engage in cyber compellence and actively counter and push back against hybrid warfare tactics. Previously, these capabilities, to the extent they existed at all, were provided (and at best, shared) only by the United States—a cyber umbrella that is comprehensively less well integrated across NATO than the U.S. nuclear umbrella has been. The transformation of the cyber domain into a permanent domain of conflict and the rapid changes in the geopolitical landscape make it essential for Europe to field its own offensive cyber capabilities—and to do so very soon.

CONSIDERATIONS ON "EURO EYES" AND THE EU CYBER FORCE

Europe has seen a widening discussion on the need to acquire independent cyber and counter-hybrid capabilities—often within the context of joint intelligence instruments. In November 2023, then-President of the European Council Charles Michel publicly floated the idea of a European cyber force in a **speech** made at a European Defence Agency event. This force would help Europe "take a position of leadership in cyber responsive operations and information superiority," and "be equipped with offensive capabilities."

Around the same time, Sauli Niinistö, former Finnish president and special adviser to the European Commission president, released a **report** proposing changes to European intelligence sharing. He argued that the European Union should have a fully-fledged intelligence cooperation service supporting all EU institutions and member states. It would not "emulate the tasks of Member States' national foreign intelligence and domestic security services," nor would it "interfere with their prerogative on national security." Instead, it would reinforce the existing EU intelligence fusion center—the **Single Intelligence Analysis Capacity (SIAC)**, which currently includes both the EU Intelligence and Situation Centre and EU military intelligence. The report has been interpreted as advocating a "**Euro Eyes**" version of the fabled U.S.-led Five Eyes intelligence alliance.

Attempts to find a **minimum consensus** led to the early 2025 announcement that the European Commission would set up a Cyber Defence Coordination Centre (CDCC) to facilitate enhanced situational cyber awareness and intelligence sharing. However, the expansion of both the SIAC and the CDCC would be in the European External Action Service (EEAS), headed by the High Representative for Foreign Affairs and Security Policy Kaja Kallas. As Commission President von der Leyen has **made clear**, it is important to strengthen the intelligence capability of the Commission (a separate body from the EEAS). In November 2025, she went so far as to propose setting up her own "intelligence cell" directly in the Commission's Secretariat-General. The **pushback** was public and fierce. Currently, neither this fusion cell nor the expanded SIAC nor the CDCC (which has been starved of funding within the EEAS) has been fully implemented. All of these measures, it should be noted, would hardly have delivered on a Euro Eyes concept, let alone a counter-hybrid operations center.

The most forward-leaning suggestion emerged in November 2025. In response to escalating hybrid warfare attacks against Italy, Italian Defense Minister Guido Crosetto advocated for **two organizations**: a national deterrence body (Arma Cyber) and a dedicated counter-hybrid compellence body at the EU level.[14] The national Arma Cyber would initially field 1,200–1,500 personnel and eventually expand to 5,000, including reservists. It would engage in the full spectrum of activities in cyberspace—including strategic cyber operations and other measures below the threshold of war. It appears similar to the UK joint **National Cyber Force**. Meanwhile, the EU-level compellence body—proposed as the **Center for Countering Hybrid Warfare**—would share best practices and intelligence and engage in command and control of European counter-hybrid operations. This center appears intended to effectively coordinate a proactive EU cyber response against hybrid threats.

14. Italy has experienced a sustained pattern of overt coercive cyber and hybrid activity alongside more subtle and ambiguous forms of pressure. Pro-Russian hacktivist groups including Killnet and NoName057(16) have repeatedly launched DDoS attacks against Italian ministries, parliament, law enforcement bodies, health authorities, transport agencies, ports, airports, and banks. Alongside these visible actions, Italy has faced more subtle forms of coercion, intimidation, and framing. These include unexplained data leaks involving personal and financial records and circulation of the compromised credentials of high-profile individuals.

The debate in Europe on building an **autonomous cyber capability** has often been seen as intractable, characterized by conflicting requirements and political views. The 27 EU member states possess a wide range of technical capabilities and **geopolitical interests**, including varying commitment to European solidarity in general and resistance to Russian aims in particular. Moreover, cooperating with non-EU members including the United Kingdom presents an additional challenge. Lastly, NATO alone likely represents an ineffective solution, given the complications associated with **non-Article 5 counter-hybrid compellence activities** that lack the full consent of the entire alliance.

Clearly, European leaders perceive the need for changes to EU hybrid warfare responses, and new thinking is urgently needed. In December 2025, the European Commission published a d**efense white paper** stating the need for Europe "to develop together with Member States a voluntary support scheme for offensive cyber capabilities as credible deterrence." How this would be accomplished, however, remained unanswered.

THE EUROPEAN CYBER OPERATIONS GROUP: A FRAMEWORK

For Europe to meet the consistent challenges of ongoing hybrid attacks and provide meaningful contributions to the evolving NATO cyber umbrella in conventional defense, a small group of like-minded European nations could deepen cooperation under a cyber coalition of the willing. This new ECOG would fully leverage existing offensive cyber operations capabilities within militaries and intelligence agencies, cooperating to develop them further and coordinating to deliver joint strategic effects in wartime and below the threshold of war.

Mission

ECOG would have two principal missions:

- support the deployment of a NATO cyber umbrella by developing and coordinating collective offensive cyber operations missions that can be integrated into general NATO war planning activities; and
- respond to hybrid attacks against European interests by executing cyber countermeasures in peacetime.

ECOG would contribute to activities of conventional military deterrence and engage in compellence to impose costs for "below the threshold" hostile acts. As a single body, ECOG would share political responsibility for its actions, enabling joint communication and limiting attribution to individual states while not implicating other nations in the European Union or NATO. ECOG would therefore be an operational group and an important tool for strategic communication—and thus deterrence.

Organization

ECOG would constitute a stand-alone, invite-only political initiative, which could later transition to an EU, NATO, or other affiliation. An existing framework that could be adapted for this purpose is the French-led **European Intervention Initiative**, which was introduced by French President Emmanuel Macron in 2017, or the UK-led Joint Expeditionary Force, focusing on military collaboration with Nordic countries. An intelligence-only framework, such as the purported "**Maximator**" group of European intelligence agencies or a cyber equivalent of it (including Sweden and the UK) could form the base. However, on its own, an intelligence grouping would be insufficient due to the importance of strategic communication and political ownership. As noted previously, to engage in effective deterrence, it is

essential to overcome the Cartwright Conjecture and clearly communicate both will and capability. A covert alliance will likely fail on both accounts, and by implying a weakness of political will (by insisting on "hiding in the shadows") it may even invite stronger retaliation and further escalation. A key feature of ECOG would be the ability to deny direct attribution (and therefore retribution) to individual states while providing a unified front in joint activities.

Figure 2: European Cyber Operations Group: The "Corkscrew Governance Framework"

Source: Author's model.

Further, depending on circumstances, ECOG would need to be able to draw on the political support of NATO and EU leaderships. A single organizational spokesperson would be essential to fulfill the critical strategic communication function and delineate group activities from individual endeavors. The current EU counterterrorism coordinator role may be an example, although governments may agree on a rotating position as well. Finally, public communication on ECOG actions could also play a role in buttressing public support—an inability to fight back against an aggressor is a key part of the psychological attrition intended in hybrid war. ECOG action, when clearly limited and supported by international law, could thus help buttress European psychological resilience as well.

Method of Operation

ECOG would employ a corkscrew governance framework to increase outreach and case-by-case collaboration, depending on the mission set and purpose. This allows for varying levels of external engagement and interaction depending on the ambition and objective. The highest levels of the corkscrew—specific acts of political support by NATO and/or EU leadership, or even direct mission requests from the same—are likely to be leveraged only in cases of the broadest alignment with non-ECOG members.

The first element is individual partner organizations. Ideally, each partner nation would be represented by a U.S. Cyber National Mission Force or UK National Cyber Force equivalent. ECOG would likely form several task forces with thematic/regional needs. Key common resources would be a cyber common operational picture, deconfliction of intelligence and operational preparation of the environment activities, and resource sharing (e.g., a "cyber foundry" supply chain, shared computing facilities, or signals intelligence activities). Participation in all task forces would be case by case, with decisions to actively deploy offensive cyber capabilities or publicly communicate made by the respective governments. Direct cooperation between and among these organizations would depend on the assessed requirements of the necessary secure communication infrastructure and could range from a pure hybrid structure to a localized institution with permanent liaison personnel. The most important elements would likely be the ability to field peer or near-peer capabilities, political alignment on geopolitical threats, and, above all, the highest level of mutual trust. As such, ECOG would be unlikely to include more than half a dozen European nations and would likely be limited to an existing informal cyber intelligence alliance.

The second element is the SCEPVA approach. The **NATO framework** for joint offensive cyber operations, SCEPVA, provides a common language with which to understand and define cyber effects and missions. For both principal ECOG missions (i.e., deterrence and counter-hybrid compellence), SCEPVA would provide the basic communication frame for deterrence missions and would be key to helping unfold the NATO cyber umbrella. Close cooperation with NATO partners (especially the United States), as well as Supreme Headquarters Allied Powers Europe, would be crucial.

The third element is bespoke cooperation with NATO and EU institutions. The participating nations would be able to directly draw upon resources—and, critically, funding instruments—that NATO and the European Union currently maintain. Further, some aspects of the compellence mission could profit from civilian organization cooperation, such as with EUROPOL's European Cybercrime Centre.

The fourth element is wider political support by EU political leadership and/or NATO. While ECOG would be outside the direct command of either organization, demand signals could emanate from both. This applies equally to both missions but is particularly important in conducting a counter-hybrid compellence operation. It would be crucial for the top leadership of either or both organizations to provide political support to ECOG, especially after a mission has been carried out, to reinforce the wider deterrence value of these actions.

Enabling Factors

Executing ECOG missions will require substantial cooperation and joint investment in enablers. As such, providing adequate support for ECOG operations represents a crucial task for such a group. Providing such support requires effort across three pillars: enabling strategic investment, modernizing procurement processes, and developing an elite workforce.

Enable strategic investment. ECOG's constituent partners will need to invest heavily in critical areas to effectively support the group's operations. These areas include: (1) intelligence gathering and processing, (2) high-performance computing (HPC) infrastructure, (3) secure communications, (4) common cyber operational picture assessments, (5) joint cyber foundries, (6) test ranges for cyber capabilities, (7) sharing tactics, techniques, and procedures, and (8) human skills development.

This investment should be targeted to overcome existing weaknesses. For example, HPC is **crucial** for intelligence analysis and codebreaking, yet Europe **lags** the United States and China. Likewise, significant investments targeting new cybersecurity and digital technologies will be vital to effectively grow the European defense industrial base and meet the requirements for a highly secure information and communication technologies supply chain.

The new **5 percent GDP target** for EU defense spending could directly support ECOG-related investments, primarily through the 1.5 percent earmarked for defense-adjacent security, including cybersecurity and critical infrastructure protection. To facilitate and properly align this investment, ECOG should leverage existing financial frameworks. The mammoth €150 billion **Security Action for Europe (SAFE)** instrument is designed to jump-start defense production. Notably, SAFE is **open** to all European Free Trade Association members, including the United Kingdom and Switzerland. The **European Defence Fund** provides EU grants for collaborative defense research and capability development, with a 2021–27 budget of roughly €7.3 billion. The **NATO Innovation Fund** is a stand-alone, for-profit venture capital fund that focuses on investing in deep tech startups across dual-use technologies and other issues with defense, security, and resilience applications, including AI, biotechnology, quantum computing, space, energy, novel materials, and autonomy. Each existing framework could efficiently funnel capital into ECOG research and capability development. Moreover, Europe should create and leverage bespoke investment frameworks specifically oriented around ECOG mission sets.

Modernize procurement processes. To translate improved investment frameworks into effective capability acquisition and deployment, the EGOC should embrace and modernize existing procurement and technology adoption processes. Strong procurement processes already exist within NATO: The **Rapid Adoption Action Plan (RAAP)**, endorsed at the 2025 Hague Summit, compresses technology integration cycles from decades to just 24 months. It encourages "**New Defence**" thinking, bringing together innovative dual-use startups and established defense firms to foster innovation. The plan utilizes the NATO Support and Procurement Agency and the Defence Innovation Accelerator for the North Atlantic **Rapid Adoption Service** to provide streamlined contracting vehicles for multinational consortia. The NATO Innovation Fund supports RAAP by **bridging the gap** between deep tech startups and ministries of defense through bridge loans and venture capital, linking investment frameworks and often-opaque government procurement processes.

Additionally, the EU leverages innovative procurement processes to advance capability adoption. The **European Defence Industry Reinforcement Through Common Procurement Act (EDIRPA)** is a short-term EU instrument designed to strengthen the European defense industry by incentivizing joint procurement among member states. The **European Defence Industry Programme** represents the European Union's longer-term industrial readiness and procurement framework, designed to improve the European defense ecosystem by translating short-term emergency measures such as EDIRPA into a more durable EU approach to industrial capacity, joint procurement, and market mechanisms.

Together, NATO and EU procurement processes provide opportunities for ECOG. If ECOG partners modernize existing frameworks for cyber-specific procurement, facilitating pathways for operators to acquire critical enablers such as HPC and cybersecurity technologies, they will likely convert substantial investment into strategic gains.

Develope an elite workforce. Europe must undertake significant measures to develop skilled human operators, as the greatest shortfall in European cyber capabilities is manpower quality.

Mitigating this deficiency is already a **major priority** across the European Union, as demonstrated by numerous publicly and privately funded initiatives. For instance, **hacking competitions**—sometimes with military support—are actively fostering offensive skills while also presenting a proven tool for recruitment. Despite these efforts, recruiting, integrating, and retaining technical specialists will certainly impact European cyber capabilities, and creative thinking is increasingly necessary for governments to sustainably field the best talent. The United States is intimately familiar with this issue: It faces an estimated shortfall of **500,000 cyber workers**. The U.S. Armed Forces **likewise struggle** to recruit, train, and retain skilled cyber operators, leading to calls for a stand-alone cyber service.

The European private market also faces a shortage of skilled cyber workers. Indeed, companies with the capacity to pay high salaries often **struggle** to attract enough talented employees. Limited budgets and other challenges **exacerbate** this issue for governments and militaries. ECOG partners could mitigate this by prioritizing smaller numbers of high-quality technical specialists with special pay conditions over greater quantities of less qualified operators. As an example, highly prolific Russian hacking groups reportedly leveraged only a **dozen coders** in their 2016 cyberattack on the Democratic National Committee. The focus on highly capable talent will likely increase as the integration of AI into operations shifts the focus of activities further.

Conclusion

In December 2025, Britain's new MI6 Chief Blaise Metreweli **remarked**, "We are now operating in a space between peace and war." Russia's comprehensive hybrid warfare campaign against Europe may be as precursor for a wider open conflict or may be intended to seek victory outright. Whatever the case, a lack of forceful countermeasures to these activities is likely to invite further aggression. Resilience measures and targeted sanctions are necessary but insufficient on their own.

As Russia continues to adapt and rearm and as U.S. support wavers, current circumstances demand urgent action. Europe cannot wait for consensus or operate solely within existing institutions ill-suited to the contemporary environment. Europe must credibly deliver an offensive cyber capacity in wartime, engage in cyber countermeasures against hybrid warfare activities, and authoritatively communicate both to adversaries.

> *Europe must credibly deliver an offensive cyber capacity in wartime, engage in cyber countermeasures against hybrid warfare activities, and authoritatively communicate both to adversaries.*

The practical path forward is a coalition of the willing jointly acting below the threshold of war in peacetime while reinforcing NATO and conventional military efforts in wartime, underpinned by a crucial strategic communication mission. The proposed Europe Cyber Operations Group fits that

path. Operating under a corkscrew governance framework and supported by applicable investments, procurement processes, and talent systems, ECOG would develop Europe's cyber umbrella while enabling responses to hybrid threats. ECOG would be able to draw upon the best of both NATO and EU frameworks, without their limitations and without forcing other governments to support their activities.

Under the ECOG framework, Europe can confront the dual threat posed by the cyber and information spaces and closely coordinate to affect its adversaries' strategic calculus and compel restraint. As Italian Defense Minister Crosetto remarked, perception is key to hybrid warfare. But perception of ability and will to act are also key dimensions of deterrence. For both, speed is a good indicator of decisiveness. Europe needs to illustrate its decisiveness—before time runs out. ■

Alexander Klimburg *is a Europe-based nonresident senior associate for the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.*

The author would like to thank Max Bergmann and Peter Dohr, as well as Matt Pearl and Lauryn Williams, for their assistance in shaping this piece.

This report is made possible by support from Google.org.