

EQUIPO EUROPA

V EDITION

FORUM ON THE FUTURE OF THE EU

European Security in a Changing World

Forum on the Future of the EU

EUROPEAN SECURITY in a Changing World

INDEX

FOREWORD
By Enrico Letta __ 02

INTRODUCTION
Of the policy proposals document. __ 05

EU AND SECURITY GOVERNANCE
Introductory Chapter 1 __ 09

EU EXTERNAL ACTION AND GEOPOLITICS
Introductory Chapter 2 __ 31

DEFENCE AND MILITARY CAPABILITIES
Nucleus Chapter 1 __ 57

ECONOMIC SECURITY
Nucleus Chapter 2 __ 89

HYBRID THREATS AND INTERNAL SECURITY
Focal Chapter 1 __ 111

TECHNOLOGY AND FUTURE SECURITY
Focal Chapter 2 __ 133

CLIMATE, HEALTH AND HUMAN SECURITY
Focal Chapter 3 __ 155

CONCLUSION
Of the Policy Proposals Document __ 172

FOREWORD: *BUILDING EUROPE'S CAPACITY TO ACT*



Enrico Letta

Dean School of Politics, Economics and Global Affairs IE University

For decades, European integration developed within an implicit division of responsibilities. It advanced most readily in fields in which security considerations appeared limited, while matters closely associated with national sovereignty remained largely under national control. The Single Market, Europe's most successful integration project, emerged from this political understanding. Finance, energy and telecommunications consequently remained only partially integrated, since their strategic importance was thought to justify the retention of national authority.

For a considerable period, this division of responsibilities appeared sustainable. It supported growth, high living standards and prosperity, while Europe's security seemed assured by a stable strategic environment and the protection afforded by the transatlantic alliance. In the unipolar order that followed the end of the Second World War, the assumption that security should remain primarily a national responsibility was rarely contested. **However, the conditions that sustained this model have since changed profoundly.** Three closely connected, yet analytically distinct, developments explain why it now requires fundamental revision.

The most immediate development is the deterioration of Europe's security environment. Russia's war against Ukraine and the intensification of strategic competition have made the continent's security an urgent concern. At the same time, the American security guarantee can no longer be assumed to be fully dependable. **European countries must therefore assume greater responsibility for their own protection.** This entails a substantial shift in the capabilities they develop and in the resources

they are willing to mobilise. Incremental adjustment will be insufficient.

A deeper transformation concerns the scale at which power is exercised. Demographic and economic trends are reducing the relative weight of individual European countries, each of which is becoming smaller in relation to the principal centres of global power. Globalisation is also entering a new phase of continentalisation, in which power is increasingly organised around large and integrated economic spaces. Geopolitical influence depends on the capacity to combine market size, industrial capability, technological ecosystems and investment resources within a coherent framework supported by effective public action. As this combination becomes more important, national fragmentation becomes more costly. Acting individually, European countries cannot mobilise such resources on the scale required to guarantee their security. **The assumption that national governments can secure their countries' future primarily through national means has therefore lost much of its force.** A substantive reassessment of the EU's role is unavoidable and can develop in a complementary relationship with NATO.

The third development concerns the foundations of security itself. In an environment shaped by hybrid warfare, Europe's security rests on economic resilience alongside the instruments traditionally associated with defence. Industrial capacity, technological leadership, investment capability, reliable supply chains, productivity and competitiveness have all acquired strategic significance. The economic sectors that remained at the margins of the Single Market are central to these foundations. This reveals a paradox within Europe's inherited arrangements. **Sectors retained under national control because of their strategic importance now require deeper European integration in order to serve that same strategic purpose.** In a world increasingly organised at continental scale, national fragmentation weakens the security it was intended to safeguard.

Taken together, these developments require a thorough reconsideration of Europe's approach to security across several areas. The first concerns governance. **A credible European defence project depends on decision making that can take account of the strategic consequences of choices made across policy areas.** The EU's institutions and policies have largely developed along sectoral lines, with distinct mandates and specialised procedures. Yet the consequences of today's choices routinely extend beyond those boundaries. An industrial policy decision may determine the availability of a critical defence capability, while an energy or telecommunications decision may create lasting strategic dependencies. When such choices are assessed through separate policy frameworks, their security implications may receive insufficient weight. European governance must therefore allow the various consequences of a decision to be considered together, so that sectoral objectives are pursued with a fuller understanding of their strategic effects.

Within defence itself, the immediate priority lies in strengthening capabilities through practical cooperation. Fundamental debates over decision making structures and chains of command would require treaty change and absorb considerable political energy, while offering limited prospects of substantive results in the short term. **Greater integration of Europe's defence industrial base provides a more immediate route to effectiveness.** Economies of scale, reduced duplication and closer coordination of investment would enable available resources to generate stronger collective capabilities. When countries pursue overlapping programmes in isolation, they incur substantial additional costs without a corresponding improvement in Europe's capacity for self defence. Overcoming this fragmentation should therefore be a central objective of European defence cooperation.

Perhaps the most consequential task is to bring strategic economic sectors fully within the European integration project. **Europe's security and geopolitical influence will increasingly depend on the extent to which its economic capacities are organised at European scale.** Defence capabilities require sustained investment, technologically advanced industrial ecosystems, secure and resilient infrastructure, and the ability to reduce critical dependencies. Each of these conditions rests in part on the quality of Europe's financial system, the resilience and affordability of its energy system, and the integrity of its digital and telecommunications networks. **The One Europe, One Market Roadmap provides a common framework for this endeavour and places it within a broader strategic perspective,** treating the integration of finance, energy and telecommunications as an essential condition for Europe's capacity to act. A more integrated financial market would make it easier to mobilise Europe's considerable savings towards productive investment, innovation and the scaling up of European firms. A genuinely integrated energy market would strengthen resilience, lower prices and reduce exposure to external pressure. Greater integration in telecommunications would support the

deployment of secure digital infrastructure, the development of technological ecosystems and the protection of critical networks. **The Roadmap may therefore prove to be among the most consequential European initiatives of the past decade.** Its success will help determine whether the EU can convert its combined economic resources into an effective and durable capacity for strategic action.

This transformation must also rest on a durable social foundation. **The measures undertaken must deliver tangible improvements in living standards and opportunities across European society.** Many citizens continue to bear the consequences of fifteen years of successive crises. Further demands that impose unsustainable sacrifices would deepen their insecurity and weaken the public consent on which a sustained security effort depends. Should greater strategic ambition fail to generate broadly shared prosperity, Europe would risk a social crisis with direct consequences for its security. A cohesive society can pursue common objectives and commit itself to challenges whose resolution lies beyond the immediate present. A society absorbed by the insecurity of everyday life will struggle to sustain such a collective effort.

The scale of these challenges is considerable, yet there are grounds for cautious confidence. **In matters of security, the ability to understand a changing environment and to adjust accordingly is itself a strategic asset. Europe has begun to demonstrate that capacity.** In 2019, well before Russia's full scale invasion of Ukraine, Ursula von der Leyen announced her ambition for a geopolitical Commission. The objective was to give Europe a more active role in fields extending beyond economic integration, including through the coordination of strategic action in areas where the EU could not act directly. As the importance of economic scale became clearer, so did the limits of an approach centred primarily on extending the range of European activity. The ambition to act in new domains depended on economic foundations that remained fragmented. The EU was able to adjust its approach accordingly. The **One Europe, One Market** Roadmap reflects this evolution by placing the instruments of economic integration within a wider strategic framework. The speed with which this understanding has taken hold is significant. **Within a few years, arguments often treated as technical have moved to the centre of the European agenda and have informed an interinstitutional programme.** This evolution matters in its own right. Europe has not always displayed this capacity. During the sovereign debt crisis, policymaking remained attached to inherited doctrines long after events had exposed their limitations. Reality changed more rapidly than the intellectual frameworks through which it was interpreted. Adaptation came only after years of economic hardship and political conflict, by which time the delay had deepened the crisis and widened divisions among Member States. That experience demonstrated the costs of allowing inherited assumptions to constrain the response to a changing reality. Recent years suggest a greater capacity to learn under pressure. The pandemic, Russia's invasion of Ukraine, the energy crisis and the intensification of strategic competition have repeatedly compelled European institutions to reconsider established assumptions. The resulting responses have varied in ambition and advanced at different speeds. Nevertheless, it must be recognized that European institutions have become quicker to recognise fundamental changes, revise their analysis and reorder their priorities.

The Roadmap gives concrete expression to this evolution. An understanding of Europe's geopolitical role that would have appeared unconventional only a few years ago has acquired institutional form, a defined timetable and mechanisms of accountability. This remains an intermediate achievement, since the Roadmap will ultimately be judged by the results it delivers. Yet a shared diagnosis is indispensable to coherent action. The progress made in reaching it raises the stakes of implementation. Europe's institutions must now show that they can translate a revised understanding of their strategic needs into effective policy.

Enrico Letta

Dean School of Politics, Economics and Global Affairs IE University



INTRODUCTION *OF THE POLICY PROPOSALS DOCUMENT*

On 30 August 1954, the French National Assembly rejected the treaty that sought to establish the European Defence Community. Nine years after the end of the Second World War, the prospect of a European army had proved politically impossible. The proposal belonged to an extraordinary moment in European history, when the devastation of war had opened possibilities that would previously have been almost inconceivable. Its failure did not bring European integration to an end. Three years later, the Treaties of Rome laid the foundations for a common market, and Europe continued its construction by other means. Defence remained largely in national hands, under the protection of the Atlantic Alliance. Economic integration, rather than military union, became the principal path towards European unity.

That choice shaped what the European project would become. The European Communities, and later the European Union, developed an exceptional capacity to establish common rules, integrate economies and manage relations between states that had repeatedly fought one another. In historical terms, this was a remarkable reversal. For centuries, European states had built their institutions partly through war, which demanded armies, taxes and ever larger administrations. European integration followed almost the opposite path: it sought to make war between its members inconceivable by binding them together through law, institutions and shared interests. A common defence was not part of that design, nor did it need to be, since it remained the responsibility of the Alliance. It was a division of labour suited to its time.

For several decades, this arrangement served Europe well. American security guarantees provided the military protection that European integration itself did not seek to reproduce. Meanwhile, the common market expanded, former dictatorships became democracies, and the division of the continent began to disappear. The events of 1989 seemed to offer confirmation of a larger historical hope: that a Europe once defined by rivalry might increasingly be organised through political freedom, economic interdependence and cooperation. The enlargement of the Union carried that promise eastwards. For a generation of Europeans, peace, prosperity and integration gradually ceased to appear as improbable achievements and became the ordinary conditions of political life.

History, however, does not necessarily preserve the circumstances that make a particular political settlement successful. Russia's invasion of Ukraine in February 2022 brought large-scale interstate war back to Europe. The disruption of energy supplies revealed how commercial relationships could become instruments of political pressure. Competition over critical technologies such as semiconductors, and over access to critical raw materials, exposed similar vulnerabilities in sectors upon which Europe's prosperity increasingly depends. Since 2025, renewed uncertainty over the future of transatlantic security cooperation has further sharpened questions that Europeans had long been

able to postpone. These developments have different origins, but together they have unsettled the assumption that economic integration and international interdependence would progressively reduce the importance of "raw" power.

The problem is not that Europe's economic achievements have suddenly lost their value. Quite the contrary. They have become too important to remain disconnected from the means of protecting them. A common market of considerable weight does not automatically provide the military capabilities necessary for collective defence. Regulatory authority does not guarantee technological leadership, any more than economic openness guarantees secure access to essential resources. Europe's institutions have become highly effective at organising common interests, but their ability to defend those interests has developed unevenly. **The question left unanswered in 1954 has returned in a different form: how can a Europe built to overcome the politics of force acquire the capacity to protect itself in a world where force still matters?**

This question now runs through much of the European debate. The reports on competitiveness and preparedness published in 2024 approached Europe's predicament from different directions, but revealed a common concern. Economic prosperity, technological capabilities, industrial production and collective security cannot be sustained independently of one another. The initiatives launched in 2025 to strengthen defence investment, joint procurement and European preparedness represent attempts to address this imbalance. Their real test lies less in the ambitions they announce than in the capacity to fulfil them. Europe must translate its economic resources into effective capabilities, overcome fragmentation between national systems and determine which responsibilities can best be exercised collectively. The distance between recognising a shared problem and developing the political means to solve it remains considerable.

There is no reason to assume that this process must lead to a European state, or that every new challenge requires greater centralisation. The European Union was built upon a different relationship between authority and sovereignty, and that remains part of its political character. Decisions about common defence, economic dependencies or critical infrastructure involve competing national priorities, public resources and questions of democratic accountability. Greater autonomy may require developing European capabilities in some areas, while preserving international cooperation in others. Security, moreover, cannot become an end that justifies every means. The purpose of strengthening Europe's capacity to act is to preserve the political order that made cooperation possible in the first place.

For those of us who have grown up within that order, the historical distance can be deceptive. Open borders, peaceful relations between neighbouring states and the freedoms associated with European citizenship may appear permanent precisely because we have rarely known anything else. The Europeans who began the process of integration could make no such assumption. They understood, from experience, that peace and political freedom were neither natural nor irreversible. Our circumstances are different, but the underlying lesson remains. Europe's future is not guaranteed by its past achievements, nor is its decline predetermined by its present difficulties. It will depend, as it has before, on political choices whose consequences may extend far beyond the generation making them. Peace and freedom endured in Europe because there were those prepared to defend them: preserving them will demand the same resolve from our own generation.

It is with this conviction that Equipo Europa presents the Policy Proposals Document accompanying the fifth edition of the Forum on the Future of the European Union, held in Madrid from 20 to 22 November 2026 under the theme *European Security in a Changing World*. Developed since May by more than forty young contributors, its seven policy briefs address different aspects of a common problem: the relationship between Europe's political ambitions, the capacities available to realise them and the vulnerabilities that increasingly test its institutions.

The document follows this reasoning in three parts.

The first examines **the conditions under which Europe can act collectively**. *EU Security Architecture and Governance* considers the institutions and responsibilities through which European security is organised, while *EU External Action and Geopolitics* explores the Union's position in an international order increasingly shaped by strategic competition.

The second turns to **the material foundations of European action**. *Defence and Military Capabilities* addresses military preparedness and cooperation, while *Economic Security* examines the dependencies and productive capacities upon which Europe's freedom of action increasingly rests.

The third considers **the changing nature of the threats European societies must confron**t. *Hybrid Threats and Internal Security, Technology and Future Security*, and Climate, Health and Human Security explore vulnerabilities that cross borders and blur the distinction between external security and domestic resilience.

The central and focused briefs conclude with policy proposals intended to translate these analyses into possible courses of action. They are not presented as definitive answers, nor do they presume that every challenge calls for further integration. Their purpose is to contribute to a debate in which Europe must decide not only what it wishes to achieve, but what it is prepared, institutionally and politically, to do.

Seventy-two years after the rejection of the European Defence Community, Europe is again confronting questions about defence, sovereignty and common political authority. The answer cannot simply be to revive the ambitions of 1954. The Union that exists today is immeasurably different from the Europe of the six founding states, and so is the world around it. But the historical question remains recognisable. Europeans once found a way to replace rivalry with cooperation, creating institutions that transformed their continent. They must now determine how those institutions can acquire the capacity to preserve what they have achieved. The future of Europe will depend not on escaping the realities of power, but on finding a way to confront them without losing sight of the political purpose for which Europe was built.

Delia Dinca

President of Equipo Europa



Santiago Slullitel

Director of the V Edition of Forum on the Future of the EU



EQUIPO EUROPA

INTRODUCTORY CHAPTER 1

EU AND SECURITY GOVERNANCE

THE EU SECURITY ARCHITECTURE: GOVERNANCE IN A POST 2026 LANDSCAPE.

Authors: Henriqueta Henriques, Helena López Roncero, Mario Martín Ortega, Pablo Musulen Lachica, Daniel Pérez Castro, Nerea Pérez Romo, Mariola Requena Buzón, Iván Segura Domene.
Reviewers: Santiago Slullitel and María Villaverde Temes.

Forum on the Future of the EU
EUROPEAN SECURITY in a Changing World

EXECUTIVE SUMMARY

This Policy Brief examines the legal, political and institutional architecture underpinning the European Union's Common Foreign and Security Policy (CFSP) and its Common Security and Defence Policy (CSDP). It draws a crucial analytical distinction between European Security — the broader continental order grounded in international law, the UN Charter and the Helsinki Final Act — and EU Security, understood as the specific governance structures, legal competences and defence capabilities through which the 27 Member States protect their citizens and territory. As an introductory diagnostic brief, its purpose is threefold: to map how the EU's security governance currently functions, to analyse where its security instruments suffer structural paralysis during moments of crisis, and to identify legal pathways capable of reforming that architecture.

The analysis is relevant to European security because the continent has entered a period of renewed power politics, marked by the return of war to Europe, the weaponisation of economic and energy interdependence, and an expanding, increasingly complex threat landscape spanning hybrid warfare, disinformation and contested global commons. In this context, the EU has recognised the need to "speak the language of power" and to build genuine strategic autonomy as a credible security provider.

Yet the brief identifies four interlocking challenges that constrain the EU's capacity to act decisively. First, the unanimity obstacle embedded in the Treaties, which allows a single Member State to obstruct collective decisions on sanctions, missions or joint positions. Second, veto weaponisation, exemplified by the repeated use of dissent as diplomatic leverage on matters unrelated to the decision at hand. Third, the "shadow of the veto", whereby the mere threat of obstruction pushes policy toward the lowest common denominator before any formal vote is even cast. Fourth, institutional fragmentation and a split of competences between the intergovernmental Council, the High Representative, the EEAS and the supranational Commission, which generates coordination friction even where political will exists.

Keywords

Common Foreign and Security Policy (CFSP); Common Security and Defence Policy (CSDP); Institutional Bottlenecks; Qualified Majority Voting (QMV); Unanimity; Veto Weaponisation.

INTRODUCTION

DEFINING THE "SECURITY" PARADIGM

The contemporary European security landscape is no longer defined by the predictable rules of the post-Cold War era, but by a volatile, contested multipolar world where interdependence has been actively weaponized.

In this context, the European Union does not rely on a traditional, strictly military definition of security. Instead, the organization operates under a "comprehensive concept of security." Under this paradigm, **the EU defines security as the ability to guarantee the protection of its citizens and territory, operating on the premise that internal and external security are inextricably intertwined**[1]. It is an indivisible construct where traditional defence is combined with the promotion of human security and the mitigation of root causes of instability. To understand how the European Union addresses security today, it is essential to trace the evolution of its strategic posture from its 2016 Global Strategy to the 2022 Strategic Compass[2].

European Security vs. EU Security: An Indivisible Link

While the overarching theme of this Forum addresses European Security—referring to the broader continental order based on international law, the UN Charter, and the Helsinki Final Act—this specific Policy Brief focuses on EU Security. The distinction is crucial: Europe is a continent, whereas the European Union is a distinct political organization of 27 Member States. EU security specifically relates to the governance, institutional architecture, and defence capabilities (such as the Common Security and Defence Policy) designed to protect the Union's citizens and territory. However, the EU recognizes that these two concepts are inextricably linked. European security is indivisible; any challenge to the broader continental security order, such as the return of war to Europe, fundamentally threatens the security of the EU itself[3].

The Comprehensive and Dual Nature of EU Security

Historically, the European Union has prided itself on its soft power—championing job opportunities, inclusive societies, human rights, and development. However, **the EU explicitly recognizes that the idea of Europe as an exclusively "civilian power" no longer aligns with an evolving reality**. The foundational security paradigm of the EU dictates that soft and hard power must go hand in hand. This dual approach means that the EU's definition of security spans across multiple domains, involving the resilience of Member States and societies by building inclusive governance and economic convergence, while simultaneously maintaining the military and civilian capabilities necessary to deploy operations under the Common Security and Defence Policy (CSDP)[4].

1 European Union, A Global Strategy for the European Union's Foreign and Security Policy (Brussels, 2016), 9, 14.

2 European Union, A Strategic Compass for Security and Defence (Brussels, 2022), 5-14; European Union, A Global Strategy for the European Union's Foreign and Security Policy (Brussels, 2016), 14.

3 European Union, A Strategic Compass for Security and Defence (Brussels, 2022), 14-15.

4 European Union, A Global Strategy for the European Union's Foreign and Security Policy (Brussels, 2016), 14-23.

A Geopolitical Awakening: The Paradigm Shift

While the 2016 strategy laid the groundwork for a globally engaged Europe, the 2022 Strategic Compass marks a **critical paradigm shift, described as Europe's "geopolitical awakening**". The return of war in Europe, specifically Russia's unprovoked and unjustified military aggression against Ukraine, shattered the European security order and proved that the continent is living in an era of raw power politics. **The current security paradigm acknowledges that multilateralism and soft power alone are insufficient in a highly confrontational system**. The EU has formally recognized that to ensure dialogue, diplomacy, and multilateralism succeed, it must put power behind them—or, as the organization frames it, it must learn to "speak the language of power"[5].

Consequently, the EU defines its security mandate through the urgent need to make a "quantum leap forward" in its capacity and willingness to act, aiming to become a stronger, more autonomous security provider[6].

The Expanding Threat Landscape

Because the EU's definition of security is comprehensive, it addresses **an expanding and complex threat landscape**. Today, the security paradigm is shaped by a dangerous mix of fragile states, revisionist powers, and authoritarian regimes, expanding into new domains:

- **Weaponisation of Interdependence:** the EU recognizes economic and energy coercion as direct security threats. Interdependence, once seen as a tool for peace, has become conflictual, with energy flows, financial sanctions, and even vaccines being used as instruments of political competition.

- **Hybrid Threats and Cyber warfare**: state and non-state actors increasingly utilize hybrid tactics, including cyberattacks against critical infrastructure, direct interference in democratic elections, and the instrumentalization of irregular migration.

- **Foreign Information Manipulation:** the battle of narratives and disinformation campaigns are now treated as core threats that destabilize societies and require dedicated toolboxes to counter.

- **Climate Change as a Threat-Multiplier:** the EU incorporates environmental degradation and climate change into its security definition, recognizing them as catalysts for resource scarcity, social inequality, and violent conflict globally.

- **Contested Global Commons:** access to the high seas, outer space, and the digital sphere is increasingly contested, requiring the EU to project security across all these strategic domains[7].

Structure and Purpose of this Policy Brief

To navigate this complex, fragmented, and volatile world, the European Union requires a robust security architecture. Following the methodological guidelines of a Policy Brief, this document will address exactly what the problem is, why it matters, and what should be done about it. In the subsequent sections, this brief will analyse the policy instruments, legal frameworks, and institutional bottlenecks that define the EU's current security governance. It will evaluate whether the current decision-making processes allow for rapid crisis response and assess the strategic autonomy of the EU's defence capabilities. Ultimately, this brief will provide a comprehensive diagnosis of the European Union's structural vulnerabilities, serving as a foundational roadmap to understand the institutional reforms required to strengthen this architecture for the future.

5 Josep Borrell, "Foreword," in A Strategic Compass for Security and Defence (Brussels: European Union, 2022), 6.
6 European Union, A Strategic Compass for Security and Defence (Brussels, 2022), 4-15.
7 European Union, A Strategic Compass for Security and Defence (Brussels, 2022), 10-22.

1 THE LEGAL AND COMPETENCE FRAMEWORK

1.1 WHAT ARE THE EXISTING LEGAL FRAMEWORKS?

The legal architecture of European defence operates under a differentiated regime from other EU policy areas. Under the Treaties (Treaty on European Union and Treaty on the Functioning of the European Union), **defence falls within the scope of the EU's External Action**, regulated through the Common Foreign and Security Policy[8] and, within it, the CSDP. This domain operates under a special intergovernmental framework, whose political direction and external execution rest primarily with the High Representative of the Union for Foreign Affairs and Security Policy and the Council of the EU. However, this institutional balance is complemented on the industrial and internal market front by the European Commissioner for Defence and Space, Andrius Kubilius. While the High Representative commands operational CSDP missions and leads diplomatic consensus under Council oversight, the Defence Commissioner focuses on strengthening the European Defence Technological and Industrial Base[9] and managing financial instruments such as the European Defence Fund[10]. Legally, the CSDP is not codified in a single instrument but articulated through Council decisions and EEAS guidelines, enabled by primary law to define lines of action and mandates for civilian and military missions. Alongside this hard law coexists a body of non-binding but strategically significant soft law instruments—most notably the White Paper on the Future of European Defence, alongside roadmaps and action plans—designed to assess capability investment gaps, foster joint cross-border procurement, and guide the immediate planning of resources.

Figure 1: Infographic on the division of security responsibilities within the EU



Source: Own-elaboration

As EU law has evolved, so too have its defence policies and legal frameworks. To provide a general legal and political overview of Security and Defence, the following is organised into two groups: **primary legal frameworks** (the basis of the Union's competence to adopt policies in this area) and **political and development frameworks**, covering primarily Council decisions and other soft law instruments, which illustrate how this field has developed in practice and where things stand today.

Primary Legal Frameworks (competence base and hierarchy)

Treaty on European Union: The foundational pillar. Title V, Chapter 2, Section 2, Articles 42 to 46[11] establish the legal basis of the CSDP, enable Permanent Structured Cooperation[12] and enshrine the mutual assistance clause in its Article 42(7). Article 42(1) establishes that the CSDP "shall be an integral part of the common foreign and security policy." Under Articles 42(4) and 26, decisions are adopted by unanimity in the Council, while the High Representative assumes the execution, coordination, and political representation of the CSDP, assisted by the EEAS and military/civilian planning bodies.

Treaty on the Functioning of the European Union: Complements the Treaty of European Union. Article 2.4[13] delimits external competences, Article 215[14] provides the legal basis for restrictive sanctions regimes, and Articles 209–211[15], which are es-

8 The abbreviated form CFSP will be used from now on.
9 The abbreviated form EDTIB will be used from now on.
10 The abbreviated form EDF will be used from now on.
11 Treaty on European Union (Consolidated Version), Official Journal of the European Union C 202 (7 June 2016), Title V, Ch. 2, Sec. 2, arts. 42-46
12 The abbreviated form PESCO will be used from now on.
13 Treaty on the Functioning of the European Union (Consolidated Version), Official Journal of the European Union C 202 (7 June 2016), art. 2(4).
14 Treaty on the Functioning of the European Union (Consolidated Version), Official Journal of the European Union C 202 (7 June 2016), art. 215.
15 Treaty on the Functioning of the European Union (Consolidated Version), Official Journal of the European Union C 202 (7 June 2016), arts. 209-211.

sential for integrated missions combining civilian and security components.

Political and Development Frameworks for Security and Defence Policy

The operationalisation of the CSDP is in constant evolution and has depended on Council decisions that have created permanent structures and financial instruments. The following are the most significant milestones in the development of the CSDP.

Figure 2: Chronology of the Most Significant Milestones in Regulatory and Institutional Development in the Context of Security in the EU



Source: Own-elaboration

1.2 WHAT ARE THE COMPETENCES? WHICH INSTITUTIONS HAVE THESE COMPETENCES?

In accordance with Article 5 (2) of TEU[16], the EU operates under the **principle of conferral**, meaning **it can only act within the limits of the powers assigned to it by the Treaties**. Any power not explicitly granted remains entirely with the Member States. Security and defence do not fall under the categories of exclusive or shared competences of the Union, instead, according to Article 2 (4) of TFEU[17], the EU has solely the competence to define and implement a Common Foreign and Security Policy (CFSP)[18].

The exercise of these powers is governed by **two fundamental constitutional principles** set out in Article 5 (1) of the TEU[19], being **subsidiarity and proportionality**. Under Article 5 (3) of the TEU[20], the principle of subsidiarity dictates that in areas of non-exclusive competence, the Union shall act only if the objectives cannot be sufficiently achieved by the Member States, but can be better achieved at Union level due to the scale or effects of the operation. The principle of proportionality is established by Article 5 (4) of the TEU[21], which mandates that the content and form of Union action must not exceed what is necessary to achieve the objectives of the Treaties.

This restrictive distribution of power is most visible in the legal framework governing the CFSP and the CSDP[22], outlined in Article 24 (1) of the TEU[23]. This article establishes that the CFSP is subject to procedures of a predominantly intergovernmental nature, explicitly excluding the adoption of legislative acts and limiting the judicial control of the Court of Justice of the European Union (CJEU). Supranational tools, such as regulations and directives, cannot be used to harmonise security policy. This protection of the State sovereignty is reinforced by Article 4 (2) of the TEU[24], which declares that national security remains the exclusive responsibility of each Member State.

Within this framework, the competence to set strategic goals belongs exclusively to intergovernmental institutions. According to Article 22 (1)[25] and Article 26 (1) of the TEU[26], the European Council holds the power to identify the Union's strategic interests and define the general guidelines for the CFSP. However, the operational efficiency of this power is restricted by Article 31 (1) of the TEU[27], which requires unanimity for decisions within this sphere.

Operating beneath these guidelines, the Council of the European Union (specifically the Foreign Affairs Council) holds the competence to formulate the CFSP and adopt the decisions necessary for its implementation, as mandated by Article 26 (2) of the TEU[28]. For crisis management and deployments, Article 42 (4) of the TEU[29] grants the Council the competence to decide, by unanimity, on the launch of civilian and military missions. Although preparatory bodies like the Political and Security

16 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 5 (2).
17 Treaty on the Functioning of the European Union, Official Journal of the European Union C 326, October 26, art. 2 (4).
18 The abbreviated form CFSP will be used from now on.
19 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 5 (1).
20 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 5 (3).
21 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 5 (4)).
22 The abbreviated form CSDP will be used from now on.
23 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 24 (1).
24 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 4 (2).
25 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 22 (1).
26 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 26 (1).
27 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 31 (1).
28 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 26 (2).
29 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 42 (4).

Committee (PSC), established under Article 38 of the TEU[30], exercise strategic direction, the system remains dependent on unanimous consent. Since the Member States retain operational control over their military forces, it weakens the chain of command and hinders permanent readiness.

In contrast, the competences for initiative and implementation are split. Under Articles 18 and 27 (1) of the TEU[31], the High Representative conducts and executes the CFSP and CSDP on behalf of the Council. Article 30 (1) of the TEU provides the High Representative with a right of initiative to submit proposals to the Council. To support these duties, the EEAS operates under the functional competence regulated by Article 27 (3) of the TEU[32]. However, because the High Representative must simultaneously serve as the Council's agent and as a Vice-President of the European Commission, this institutional dualism can generate structural conflicts.

At the same time, the European Commission has steadily expanded its influence in the security sector through supranational competences. Article 17 of the TEU[33] grants the Commission a monopoly on legislative initiatives and the competence to execute the general budget of the Union, a power detailed in Article 317 of the TFEU[34]. By combining these provisions with Article 173 of the TFEU[35] on industrial competitiveness and Article 182 of the TFEU on research and technological development, the Commission has gained substantial powers to legislate, finance, and manage defence industrial instruments, such as the European Defence Fund, shaping the European Defence Technological and Industrial Base. Consequently, the Union effectively separates its security policy into two fields, allowing the Commission to drive defence integration economically and technologically, while leaving military deployment under intergovernmental control.

Regarding democratic scrutiny, the European Parliament plays a limited role. Under Article 36 of the TEU[36], it holds a consultative role regarding its competences in CFSP and CSDP, legally entitling it to formulate recommendations to the Council or the High Representative. Its main leverage remains indirect, exercising political control by approving the budget for civilian or industrial defence programs managed by the Commission.

This structure also includes bodies for technical support and advisory oversight. The EDA, established under Article 42 (3) and regulated by Article 45 of the TEU[37], has specific competences to support the Council and Member States in identifying operational needs and implementing PESCO, described in Article 46 of the TEU[38], which allows a core group of states to enter into binding commitments to develop joint military capabilities.

Operating as the Union's diplomatic corps, the EEAS holds the operational competence to assist the High Representative in conducting the CFSP and CSDP, ensuring the consistency of the EU's external action. Under Article 27 (3) of the TEU[39], this functionally autonomous body is responsible for the daily implementation of crisis management missions, diplomatic coordination via EU Delegations, and intelligence aggregation. However, because the EEAS lacks independent decision-making power and acts only as a supportive body, its institutional capacity remains entirely dependent on the strategic consensus of the Member States.

1.3 WHAT ARE THE EU POLICY INSTRUMENTS?

EU policy instruments are composed of the legal, financial and strategic tools the European Union uses to achieve its objectives. A policy instrument is a means of public intervention. It refers to any strategy, programme or law developed by public authorities and implemented to improve a specific territorial situation. An instrument can also refer to a strategy or legislative framework with no specific funding (for example, the Smart Specialisation Strategy) as long as this strategy or legislative framework comply with the above definition (i.e, developed by public authorities and implemented to improve a specific territorial situation). Beyond the EU's cohesion policy programmes, local, regional or national public authorities implement their own policy instruments, which are categorized into primary legislative tools, financial mechanisms and specific foreign or economic policies.

30 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 38.
31 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 18 and 27 (1).
32 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 27 (3).
33 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 17.
34 Treaty on the Functioning of the European Union, Official Journal of the European Union C 326, October 26, art. 317.
35 Treaty on the Functioning of the European Union, Official Journal of the European Union C 326, October 26, art. 173.
36 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 36.
37 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 42 (3) and 45.
38 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 46.
39 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 27 (3).

Legal Instruments

The European legal instruments refer to the instruments available to the European institutions to carry out their tasks. These instruments are listed in Article 288 of the **TFEU** (Chapter 2 - Legal acts of the Union, adoption procedures and other provisions, Section 1 - The legal acts of the Union) and are composed by the following sections:

- **Regulations:** a regulation is a binding legislative act in its entirety and directly applicable in all Member States without the need for national transposition. When the EU's regulation on ending roaming charges while travelling within the EU expired in 2022, the Parliament and the Council adopted a new regulation both to improve the clarity of the previous regulation and make sure a common approach on roaming charges is applied for another ten years.

- **Directives:** a directive is a legislative act that sets out a goal that EU countries must achieve. However, it is up to the individual countries to think of their own laws on how to reach these goals. An example is the EU single-use plastics directive, which reduces the impact of certain single-use plastics on the environment, for example by reducing or even banning the use of single-use plastics such as plates, straws and cups for beverages.

- **Decisions:** a decision is binding on those to whom it is addressed (e.g. an EU country or an individual company) and is directly applicable. For example, the Council issued a decision on allowing Croatia to adopt the euro on 1 January 2023. The decision related to the country only.

- **Recommendations:** a recommendation is not binding. When the Commission issued a recommendation that EU countries' media service providers improve their ownership transparency and safeguard their editorial independence, this did not have any legal consequences. A recommendation allows the institutions to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed.

- **Opinions:** an opinion is an instrument that allows the institutions to make a statement in a non-binding fashion, in other words without imposing any legal obligation on those to whom it is addressed. An opinion is not binding. It can be issued by the main EU institutions (Commission, Council, Parliament), the Committee of the Regions and the European Economic and Social Committee. While laws are being made, the committees give opinions from their specific regional or economic and social viewpoint. For example, the European Economic and Social Committee issued an opinion on the Commission's Next GenerationEU's small and medium-sized enterprises strategy.

1.4 FINANCIAL INSTRUMENTS

The EU allocates significant funding to support economic development, regional cohesion, and crisis response. There are various types of financial instruments such as equity and debt, loan guarantees and venture capital and capacity building and risk sharing facilities.

For instance, the European Union offers loans to various kinds of enterprises for the purpose of funding research and development initiatives. Additionally, it provides guarantees which assist recipients in securing loans more easily or under more favorable terms from financial institutions such as banks. The EU can also engage financially in a project by acquiring shares in it. Financial tools may also be paired with grants.

Financial tools are executed in collaboration with both public and private entities, including banks, venture capitalists, or angel investors. These financial bodies establish the specific conditions for financing, which includes the amount, length of the loan, interest rates, and applicable fees.

Those applying for funding through EU financial tools must permit the intermediary financial organization to perform necessary due diligence, which involves on-site audits and evaluations. Noncompliance with this requirement could lead to delays or rejections of funding.

- **Funding under shared management with Member States:** financial tools can be offered by the EU via financial intermediaries located in Member States (shared management) to assist its initiatives and strategies. This form of funding can be advantageous for start-ups, small enterprises, and larger corporations alike.

- **Funding under partnership with the European Investment Bank:** the European Investment Bank (EIB) provides financial products such as loans, guarantees, equity investments, and advisory support. Known as the "lending branch" of the European Union, it collaborates closely with

various EU institutions to implement EU policies across more than 140 nations globally. The EIB Group also oversees the execution of 75% of the InvestEU initiative, which leverages the successful framework of the Investment Plan for Europe (known as the Juncker Plan). This initiative combines the European Fund for Strategic Investments with 13 existing EU financial tools under a single entity. By utilizing guarantees obtained from the EU budget to attract additional investors, the InvestEU Fund enhances the EU's capacity to facilitate investments.

The European Investment Fund[40], a component of the EIB Group, aids small and medium-sized enterprises[41] throughout Europe in obtaining financing. Via the EIF, SMEs engage in their operations relying on either their own funds or those supplied by the European Investment Bank, the European Commission, EU Member States, or other external organizations.

- **Funding under NextGenerationEU:** Under NextGenerationEU – the temporary recovery tool comprising €806.900 million (at current price levels) and a new feature of the EU budget for 2021-2027 – the European Commission oversees the management of these funds, which are executed via the Member States. In order to secure the necessary financing for NextGenerationEU, the Commission engages in borrowing from the capital markets on behalf of the EU.

1.5 STRATEGIC INSTRUMENTS

The European Union uses a variety of strategic instruments to achieve its geopolitical, economic, industrial, and defence objectives. These tools allow the EU to manage trade, stimulate industrial competitiveness, ensure supply-chain resilience, and project its regulatory power globally These key strategic instruments utilized by the EU include:

- I**ndustrial and Technology frameworks**: the Strategic Technologies for Europe Platform (STEP) boosts the competitiveness of the EU's industry by concentrating on the advancement of essential technologies for a sustainable and competitive future. It evaluates innovative strategic approaches and fortifies the industrial policy of the EU. Specifically, the field of clean and resource-efficient technologies is one of the primary areas of emphasis within the STEP Programme.

- **Defence and Security:** the European Defence Fund (EDF) assists enterprises throughout Member States in creating competitive and cooperative defence initiatives that provides cutting-edge and compatible defence technologies and materials. It provides help and guidance to participants during the whole process of research and development. The Fund possesses a financial plan of almost €7.3 billion for the years 2021-2027, which includes €2.7 billion designated for joint defence research and €5. 3 billion for collaborative capability development efforts that supplement national investments. The monetary assistance is mainly offered through grants that can cover up to 100% of the allowable expenses based on the activities undertaken, as well as an incentive system that takes into account SMEs, mid-sized companies, and links to a PESCO initiative.

In addition, the Security Action for Europe[42] is the EU's latest financial tool aimed at offering monetary assistance to Member Nations to accelerate military preparedness by enabling immediate and significant investments that support the European defence sector, concentrating on addressing essential capability shortages. SAFE offers as much as €150 billion in competitively valued loans with extended repayment terms to Member States seeking financial support for investment in defence capabilities. These loans are intended to support urgent and significant procurement initiatives, guaranteeing that Europe's defence sector can supply the essential equipment at crucial times.

- **Economic Security and Trade:** trade defence instruments, including anti-dumping regulations and the Anti-Coercion Instrument, protect the EU against economic blackmail. As an example, the Comprehensive Economic and Trade Agreement[43] between the EU and Canada, was agreed for reducing tariffs, fostering trade and enforcing marketing standards. The EU also imposes sanctions to influence behaviors of other countries, entities, or individuals, often for political reasons, such as the sanctions against Russia in response to the war in Ukraine, limiting access to EU markets and financial systems. Moreover, instruments such as the Solidarity and Emergency Aid Reserve[44] can be used to

40 The abbreviated form EIF will be used from now on.
41 The abbreviated form SMEs will be used from now on.
42 The abbreviated form SAFE will be used from now on.
43 The abbreviated form CETA will be used from now on.
44 The abbreviated form SEAR will be used from now on.

assist Member States and accession nations in managing emergency situations brought on by significant natural catastrophes or public health crises. Additionally, it can assist non-EU nations with new demands arising from conflicts, the worldwide refugee crisis, or intensifying natural disasters as a result of climate change.

2 ANALYSIS OF SYSTEMIC FAILURES. INSTITUTIONAL BOTTLENECKS IN EU FOREIGN AND SECURITY POLICY

2.1 AN UNION UNDER PRESSURE

The European Union's architecture of peace has long been celebrated as one of the most ambitious exercises in multilateral governance in modern history. Yet as geopolitical shocks multiply — from Russia's full-scale invasion of Ukraine to the shifting posture of the United States under successive administrations — the structural limitations of the EU's decision-making framework have been thrown into sharp relief. **The central question confronting policymakers, scholars, and citizens alike is whether the Union's institutional design, built for deliberation and consensus, is fit for an era that demands speed, coherence, and strategic will.**

The EU's expansion to a potential membership of 35 or more states adds further urgency to these concerns. An enlarged Union would face a compounded risk of institutional paralysis, particularly in domains that still operate under unanimity rules — most critically, the CFSP. As Csaky and Grant observe, the addition of eight to ten new members with diverging interests 'could risk institutional paralysis' in areas where cohesion is most urgently required[45].

This paper maps the key structural bottlenecks within the EU's security governance model, examining both the unanimity requirement and the broader coordination failures that generate friction in crisis response. It then reflects on what legal and institutional reforms might enable a transition from a reactive, crisis-driven Union to one permanently configured for strategic readiness.

2.2 THE UNANIMITY OBSTACLE: VETO POWER AS STRUCTURAL PARALYSIS

The unanimity requirement sits at the heart of the EU's foreign and security policy dysfunction. Under the Treaty on European Union, **all decisions within the CFSP** — including sanctions, crisis management missions, and joint foreign policy positions — **require the consent of all member states**. In a bloc of 27, this creates an architecture in which a single dissenting government can hold the collective hostage[46].

The practical consequences of this arrangement have become increasingly visible. Between 2011 and 2025, a total of 45 vetoes were recorded in the EU's decision-making processes, with one-third of them occurring in just the last year and a half[47]. Hungary alone accounts for 19 of these vetoes, repeatedly blocking or threatening to block joint statements on Ukraine, the extension of Russian sanctions, and security assistance measures. Hungary's Former Prime Minister Viktor Orbán deployed the veto as an instrument of leverage — extracting concessions on unrelated budgetary matters — rather than as a principled objection to the policy in question. This pattern exposes a **fundamental vulnerability: unanimity rules can be weaponized by individual member states pursuing narrow national or partisan interests at the expense of collective European security.**

It is important to note, however, that the veto dynamic is not uniformly obstructionist. The EU Council Monitor — a database maintained by the German Institute for International and Security Affairs — recorded that over 80 per cent of Council decisions between 2010 and 2024 were made by consensus or quasi-consensus[48]. This figure, while superficially reassuring, conceals the nature of that consensus: it is often the product of pre-negotiation, informal deal-making, and the anticipatory moderation of proposals to avoid triggering a veto. In other words, the shadow of the veto shapes policy before any formal vote is cast[49].

45 Zselyke Csaky and Charles Grant, "Does EU Enlargement Require Voting Reform?," CER Insight (Centre for European Reform, May 9, 2025), https://www.cer.eu/sites/default/files/ZC_CG_enlargement_9.5.25.pdf.

46 Ibid.

47 Csaky and Grant, "Does EU Enlargement Require Voting Reform?" 4.

48 German Institute for International and Security Affairs (SWP), EU Council Monitor, cited in Csaky and Grant, "Does EU Enlargement Require Voting Reform?" 3.

49 Ana Juncos and Karolina Pomorska, "Crisis Windows and Reversible Empowerment in the EU's Common Foreign and Security Policy," Journal of European Public Policy 31, no. 7 (2024): 4, https://doi.org/10.1080/07036337.2024.2379421.

SAME RULES, DIVERGENT OUTCOMES: VETOES VS. CONSENSUS IN COUNCIL DECISION-MAKING

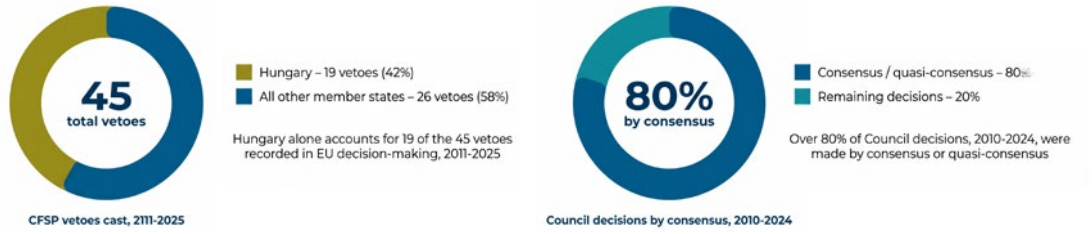


Figure 2: Vetoes vs Consensus in EU Council Decision-Making (2010-2025)
Source: Own-elaboration

Within the CFSP, decisions operate under the **'shadow of the veto**' — a dynamic in which the mere threat of non-cooperation drives member states toward the lowest common denominator. As Juncos and Pomorska document, this cyclical pattern means that even when crises generate a temporary surge of coordinated EU action, positions subsequently diverge as urgency fades, sanctions scope narrows, and strategic ambition retreats to what the most reluctant member state will tolerate[50].

The potential remedy most frequently discussed is the extension of Qualified Majority Voting (QMV) to foreign and security policy. Under QMV, a decision requires the support of 55 per cent of member states representing 65 per cent of the EU's total population. The so-called 'Friends of QMV' group — currently comprising twelve member states including Germany, France, and Italy — has expressed support for extending this mechanism to CFSP.[51] However, QMV is not a panacea. It shifts the blocking threshold from one state to a coalition of states, reducing but not eliminating the risk of deadlock. Moreover, several member states with significant strategic interests — such as Cyprus over Turkey-related foreign policy, or Sweden and the Netherlands over tax-adjacent sovereignty — flatly refuse to relinquish their veto.

2.3 INSTITUTIONAL BOTTLENECKS: COORDINATION FAILURES AND FUNDING FRICTION

Beyond the unanimity rule, the EU's security architecture suffers from deep coordination deficits. The institutional landscape for external action is fragmented across multiple bodies: the European External Action Service (EEAS), the European Commission, the Council's Political and Security Committee, and individual member state foreign ministries — all operating with distinct mandates, reporting lines, and strategic cultures. This fragmentation generates what practitioners describe as institutional friction: the accumulated drag of duplicated bureaucracies, contested competences, and communication failures that slow coordinated response even when political will nominally exists.

The CFSP budget illustrates this tension. Under the 2021–2027 Multiannual Financial Framework (MFF), Heading 6 — Neighbourhood and the World — was allocated €98.4 billion, and Heading 5 — Security and Defence — €13.1 billion (in 2018 prices)[52]. These are substantial sums, yet their effective deployment has been hampered by the architecture through which they flow. Unanimity is required not only for CFSP decisions but also for the adoption of the MFF itself and for the EU's own resources framework. Disputes over budget scope and expenditure priorities have resulted in delayed disbursements and reduced operational flexibility at precisely the moments when it is most needed[53].

The case of **military assistance to Ukraine illustrates this friction in practice**. Member states, frustrated with the pace and scope of EU-level coordination, frequently bypassed EU structures in favor of bilateral agreements[54]. Poland, for instance, supplied substantial military assistance outside EU frameworks. While this reflected laudable national initiative, it simultaneously undermined the strategic coherence and political visibility of Euro-

50 Juncos and Pomorska, "Crisis Windows," 4.

51 Csaky and Grant, "Does EU Enlargement Require Voting Reform?" 5-6.

52 European Parliament Research Service, "Annual Report on Implementation of the CFSP, 2023," EPRS, 2024, https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757598/EPRS_ATA(2024)757598_EN.pdf.

53 European Parliament Research Service, "Annual Report on Implementation of the CFSP, 2023."

54 Ana Juncos and Karolina Pomorska, "Crisis Windows and Reversible Empowerment in the EU's Common Foreign and Security Policy," Journal of European Public Policy 31, no. 7 (2024): 4, https://doi.org/10.1080/07036337.2024.2379421.

pean solidarity. The European Peace Facility Fund — intended as a collective off-budget instrument for military assistance — was itself repeatedly constrained by Hungarian threats of non-cooperation, forcing workarounds that added time, cost, and reputational damage to the EU's external profile.

The civilian dimension of the CSDP has also suffered from **chronic structural deficits:** shortages of qualified personnel, difficulties in recruitment and deployment, and insufficient mechanisms for coordination between CSDP structures and Commission-managed instruments[55]. Efforts to address these shortcomings — including the Civilian CSDP Compact and the development of National Implementation Plans — represent genuine progress but have not yet achieved the level of interoperability and operational readiness that modern crisis environments demand.

2.4 PATHWAYS TO REFORM: FROM REACTIVE TO PERMANENT READINESS

The challenge of institutional reform in the EU is compounded by the very unanimity requirements that constrain its operational capacity. Treaty change — the most comprehensive route to structural reform — itself requires unanimous agreement among all member states, followed by ratification processes that may include national referendums. The failure of the Constitutional Treaty in 2005 and the prolonged ratification crisis of the Lisbon Treaty serve as cautionary precedents[56].

Within the existing treaty framework, however, several mechanisms offer pathways to incrementally improved performance. Passerelle clauses allow the European Council to authorize a shift from unanimity to QMV in defined policy areas — without requiring treaty change. Their activation itself requires unanimity, which is why they have been used only once to date (for visas and border controls in 2004). Nevertheless, a phased approach — selectively activating passerelles in less politically sensitive areas first — could build momentum toward wider adoption in CFSP and taxation[57].

Constructive abstention, already provided for in Article 31(1) TEU, offers another avenue. It allows member states to opt out of a CFSP decision without blocking it — enabling the Union to act while accommodating principled national reservations. Its use in relation to Ukraine assistance (Austria, Ireland, and Malta's abstention on lethal weapons supply; Hungary's abstention on EUMAM Ukraine) demonstrates that the mechanism functions, but its broader adoption requires a shift in political culture that treats abstention as a legitimate rather than a reputationally costly choice[58].

A more structural reform agenda would include a '**sovereignty safety net**' — as proposed by the Franco-German working group on institutional reform — which would permit member states to object to QMV decisions that touch vital national interests, subject to a secondary QMV vote on transferring the matter to the European Council for high-level resolution. **This mechanism would reduce the risk of large member states systematically dominating smaller ones while preventing minority capture of the collective decision-making process.**

The EU's current governance model does, to a significant degree, paralyze its key security instruments during crises. The unanimity rule in CFSP creates structural opportunities for individual member states to obstruct collective action for reasons unrelated to the policy at hand. Coordination failures between institutional actors and friction in funding distribution compound these delays. The result is a Union that oscillates between temporary surges of crisis-driven cohesion and a reversion to lowest-common-denominator inertia once immediate urgency subsides.

Moving from reactive posture to permanent readiness requires a dual strategy: exploiting existing treaty flexibilities — passerelle clauses, constructive abstention, legal basis selection — to expand effective decision-making capacity in the short term, while building the political consensus necessary for deeper institutional reform over time. Neither path is easy, and neither alone is sufficient. **What is clear is that the geopolitical environment no longer affords the EU the luxury of deliberative inaction.** The costs of institutional paralysis — measured in lives, credibility, and strategic influence — are no longer theoretical.

55 Csaky and Grant, "Does EU Enlargement Require Voting Reform?" 3.

56 Irakli Machaidze, "Unanimity-Driven Foreign Policy and the EU's Limitations as an Effective Global Actor" (MA thesis, Central European University, 2025), https://www.etd.ceu.edu/2025/machaidze_irakli.pdf.

57 Csaky and Grant, "Does EU Enlargement Require Voting Reform?" 4–5.

58 Csaky and Grant, "Does EU Enlargement Require Voting Reform?" 6.

3 POLICY-MAKING METHODS AND CRISIS REACTIVITY

When a crisis breaks, what determines whether the European Union can act is not only the instruments it has built, such as sanctions regimes, military missions, or financing facilities, but the rules that govern whether a decision to use them can be reached at all.

This section sets out the **formal architecture of decision-making** in the CFSP and its defence dimension, the CSDP, and how that architecture has performed when confronted with the security crises that have defined the period since 2022, with the purpose of establishing, as a basis for the legal reform options, where the EU's security governance model creates friction, and where it does not.

An analysis of this governance model reveals a fundamental tension at its core. While the EU has demonstrated a remarkable capacity to develop forward-looking security instruments, its political decision-making process remains constrained by an intergovernmental logic that prioritises the sovereign equality of member states over collective action. This tension is not merely procedural but deeply political, reflecting what some scholars describe as an "adaptive degradation" of the EU's security governance system, where external crisis-driven institutional innovations often deviate from initial governance objectives. The system's resilience in responding to security challenges has been continuously weakened by the inherent friction between the logic of security and the logic of development, leading to a gradual erosion of governance effectiveness.

3.1 HOW CFSP DECISIONS ARE MADE?

Unlike most areas of EU competence, which follow the so-called Community method, where Commission proposes legislation, the Council votes by qualified majority and the European Parliament shares decision/making power, CFSP operates on a distinctly intergovernmental basis[59].

Under Article 22(1) TEU[60], the right to propose action in CFSP does not belong to the European Commission but is instead shared among Member States, the High Representative for Foreign Affairs and Security Policy (HR/VP), and the High Representative acting jointly with the Commission's support[61]. The Commission's influence over CFSP is therefore channelled almost entirely through the HR/VP, whose dual role as Vice-President of the Commission and chair of the Foreign Affairs Council was designed to bridge the diplomatic and supranational tracks of EU external action and to replace the fragmented pre-Lisbon set of instruments of common strategies, joint actions and common positions with a single legal instrument, the CFSP "decision".

The **default decision rule is unanimity**. Article 24 TEU[62] establishes that the European Council and the Council define and implement CFSP acting unanimously, except where the treaties provide otherwise, and Article 31(1) TEU[63] repeats the principle for individual measures. In practice, all twenty-seven member states must agree before a sanctions package can be adopted, a CSDP mission launched, or a common position on a third country defined.

The treaties do carve out four narrow exceptions to this rule, though each comes with its own built-in limitation. **Constructive abstention allows a state to formally step aside from a decision**, accepting that it binds the Union without being obliged to implement it itself, provided that no more than a third of member states do so at once.[64] A small set of technical matters concerning the European Defence Agency (EDA) can already be decided by qualified majority voting (QMV) in the Council. A third mechanism, sometimes known as flexible implementation, allows the Council to use QMV in four specific situations: when adopting a decision implementing a strategic line that the European Council has already agreed unanimously; when implementing any other CFSP decision or action; when appointing a special representative; or when acting on a proposal from the HR/VP made at the European Council's specific request.

Even here, the mechanism carries its own emergency brake: any single state may still invoke "**vital and stated reasons of national policy**" to stop the

59 Massay-Kosubek, Katherina "Intergovernmental decision-making procedures" European Parliament, 2025, https://www.europarl.europa.eu/ftu/pdf/es/FTU_1.2.4.pdf

60 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 22 (1).

61 European Studies Hub, University of Portsmouth, "Decision Making in Common Foreign and Security Policy", 2017. https://hum.port.ac.uk/europeanstudieshub/learning/module-2-understanding-eu-policy-making/decision-making-in-common-foreign-and-security-policy/

62 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 24.

63 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 31 (1).

64 OSW Team, "The EU Debate on Qualified Majority Voting in the Common Foreign and Security Policy: Reform and Enlargement," October 12, 2023), Appendix 1. https://www.osw.waw.pl/en/publikacje/osw-commentary/2023-10-12/eu-debate-qualified-majority-voting-common-foreign-and

vote, after which the High Representative must search for a compromise or refer the issue back to the European Council for a unanimous decision. Finally, the passerelle clause in Article 31(3)[65] TEU would allow the European Council, acting unanimously, to authorise QMV for a defined set of foreign-policy decisions excluding anything with military or defence implications.

The European Parliament and the Commission, the EU's two most supranational institutions, hold comparatively limited formal power here. The Parliament is informed and consulted by the Presidency on CFSP's main aspects, and may put questions or recommendations to the Council and the HR/VP, but these can be set aside; its principal point of leverage remains the EU budget. The Court of Justice of the European Union, for its part, has no general jurisdiction to enforce CFSP decisions against a non-complying member state.

Around this voting architecture sits a network of supporting bodies. The European Council sets strategic priorities and can be convened in extraordinary session by its President if international events so require, the Council and the Political and Security Committee (PSC) prepare and adopt day-to-day measures; and the European External Action Service, through its Intelligence Analysis Centre (IntCen) and the Single Intelligence Analysis Capacity (SIAC) it shares with the EU Military Staff, feeds collective threat assessments into the process, although member states retain full discretion over what national intelligence they choose to contribute[66].

The relationship between this voting architecture and the EU's intelligence-support structures illustrates a related, non-legal source of friction in the CFSP method. Tasking of the Union's joint analytical capacity is led by the HR/VP and the EEAS bureaucracy rather than by member states directly: the directors of IntCen and its military counterpart prepare a list of "Prioritised Intelligence Requirements," which is then formally agreed, roughly twice a year, by a steering board chaired by the HR/VP. This bureaucratic structure appears to have grown faster over time as the time between an initial request for information to national agencies and a finished EU assessment, once around three weeks, can today often be measured in days, a reminder that **not every constraint on EU crisis reactivity stems from the unanimity rule itself.**

3.2 WHY DOES CONSENSUS SLOW DOWN? A THEORETICAL LENS

Foreign policy analysis offers a useful vocabulary for understanding why a body bound by unanimity tends to produce different outcomes than one that can outvote a reluctant minority. A useful starting point for understanding this dynamic is Graham Allison's well-known distinction between two models of decision-making: the rational actor model and the bureaucratic politics model[67]. The rational actor model assumes a single decision-maker who identifies the available options and selects the one that best serves a defined objective. The bureaucratic politics model, by contrast, holds that outcomes are rarely the product of such unified calculation; they emerge instead from a process of bargaining among multiple actors, each with their own organisational interests, priorities and constraints. Among twenty-seven sovereign delegations, it is this second dynamic that tends to prevail. Each member state arrives at the negotiating table with its own assessment of the threat, its own domestic political pressures, and its own network of bilateral relationships, and a measure can typically advance only once it satisfies the most reluctant participant rather than the one that would produce the optimal collective outcome.

Foreign policy scholars Steven Redd and Alex Mintz identify a related pathology that is particularly relevant to large and heterogeneous decision-making bodies. Groupthink, a concept widely discussed in the organisational literature, describes what happens when a cohesive group suppresses internal dissent in order to preserve the appearance of unity. Redd and Mintz argue that the opposite problem, which they term polythink, is equally damaging and arguably more common in bodies like the Council. Polythink arises when a plurality of competing national positions makes it structurally difficult for the group to converge on any coherent collective position, producing decisions that are either excessively cautious, internally contradictory, or shaped by whichever national stance happens to represent the lowest common denominator among participants rather than the most effective response to the problem at hand[68]. Both dynamics

65 Treaty on European Union, Official Journal of the European Union C 326, October 26, art. 31 (3).

66 Björn Fägersten, "Intelligence and Decision-Making within the Common Foreign and Security Policy," October 2015, https://sieps.se/media/cfnds5me/intelligence-and-decision-making-within-the-common-foreign-and-security-policy-2015_22epa.pdf

67 Jones, Christopher M, "Bureaucratic Politics and Organizational Process Models", Oxford Research Encyclopedia of International Studies, November 20, 2017 https://doi.org/10.1093/acrefore/9780190846626.013.2

68 Steven B. Redd and Alex Mintz, "Policy Perspectives on National Security and Foreign Policy Decision Making", 2013.https://moodle2.units.it/pluginfile.php/799484/mod_resource/content/1/REDD%20MINTZ%20PolicyPerspectivesonNationalSecurityandForeignPolicyDecisionMaking.pdf

point to the same structural conclusion: **unanimity does not only slow decisions down, it also shapes their substance, since any single state can trade its consent for a diluted formulation, a carve-out, or an indefinite delay.**

A third lens, poliheuristic theory, offers a more granular account of how an individual government might arrive at the decision to block consensus in the first place. The theory was also developed by Alex Mintz, and proposes that policymakers process a choice in two stages: first, they screen out any alternative that scores unacceptably on a single "noncompensatory" dimension regardless of how favourably that alternative scores on other dimensions such as military effectiveness or economic benefit; only the alternatives that survive this initial screen then go through a more conventional cost-benefit calculation[69]. Applied to CFSP, this suggests that a national veto is not always the product of a careful weighing of European security interests against domestic ones. It can instead reflect an earlier, near-automatic step in which an option perceived as politically costly at home is removed from consideration before any substantive negotiation over its security merits has even begun, a dynamic that procedural reform alone may struggle to address, since it operates upstream of the vote itself.

3.3 CRISIS REACTIVITY IN PRACTICE

The clearest test of this architecture is empirical rather than theoretical: **how has it performed when a crisis required a fast answer?** The record is mixed, and arguably reveals a growing gap between the EU's operational capacity and its political capacity to use it. On the operational side, the Union has shown it can build forward-looking capability outside the constraints of day-to-day voting. The 2022 Strategic Compass for Security and Defence created the EU Rapid Deployment Capacity (RDC), a modular force of up to 5,000 troops spanning land, air, maritime, cyber and space domains, designed to allow the Union to respond to an external crisis quickly and without waiting for a wider coalition to be assembled[70]. By 2026, EU officials reported that most of the Compass's objectives had been met, although the instrument's actual use still depends on the same Council unanimity that governs every other CSDP decision. Analysing the RDC's predecessor, the EU Battlegroups, created in 2004 but never deployed in two decades of existence, find that procedural flexibility tools such as Article 44 TEU, which allow willing coalitions of member states to plan or conduct a mission, leave the underlying unanimity rule in the Council untouched and do little to lower the likelihood that an individual state will veto the use of forces it has itself pledged[71]. **The Union has, in short, invested heavily in the operational means of rapid response without fully resolving the political precondition for using them.**

The EU's struggle to operationalise its rapid response capabilities is emblematic of a deeper governance dilemma. The creation of the RDC, for instance, was a significant institutional innovation. However, its deployment requires a unanimous Council decision, a hurdle that has historically proven insurmountable for its predecessor, the EU Battlegroups. This suggests that the EU's security governance is characterised by a pattern of "goal alienation," where institutional reforms lock in a path that may not effectively address the core political constraints. As one analysis notes, **the EU is good at creating military instruments but struggles to muster the political will to use them.**

Unanimity, however, is not inherently slow: it tends to be slow specifically where consensus is contested. The clearest illustration comes from the economic rather than the military track. CFSP sanctions decisions also require unanimity, yet in the days immediately following Russia's full-scale invasion of Ukraine on 24 February 2022, the Council moved with striking speed: within days it had immobilised some €210 billion of the Central Bank of Russia's assets, and within roughly a week had cut seven major Russian banks off from the SWIFT messaging system entirely[72].

That a unanimity-bound institution could agree on measures of this scale within days, while the same institution has needed twenty successive sanctions packages over four years to keep adjusting that same Russia regime, and has seen individual packages delayed by national objections over unrelated bilateral disputes, suggests that the binding constraint is less the voting rule itself than the depth of shared threat perception among member states at a given moment, a factor that varies across policy areas and over time.

69 Mintz, Alex. "How Do Leaders Make Decisions?: A Poliheuristic Perspective." The Journal of Conflict Resolution 48, no. 1, 2004. http://www.jstor.org/stable/3176265

70 European External Action Service, "A Strategic Compass for Security and Defence."https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

71 Christoph O. Meyer, Ton Van Osch, and Yf Reykers, "From EU Battlegroups to Rapid Deployment Capacity: Learning the Right Lessons?," January 2024 https://academic.oup.com/ia/article/100/1/181/7506708

72 Council of the European Union, "Timeline — Packages of Sanctions against Russia since February 2022," Consilium, accessed June 18, 2026.

Intelligence-sharing offers a related, partial counterexample. During the height of the fighting in eastern Ukraine in 2014, an assessment produced jointly by IntCen and contributing member states was presented to national delegations and created what one Brussels-based diplomat described as a shared baseline understanding, making it harder for traditionally cautious states to question the basic facts before the Council[73].

Where the EU's collective machinery can generate a common picture of a crisis before member states take fixed national positions, it appears to narrow, though not eliminate, space for disagreement once a decision is actually tabled.

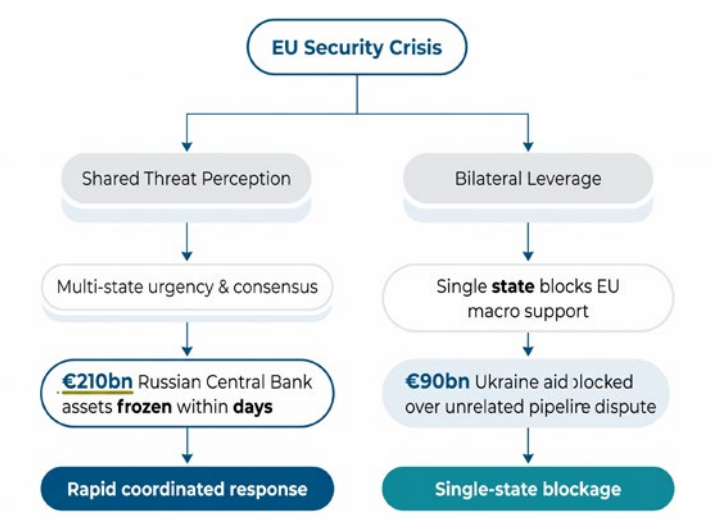
On the political side, the years since Russia's full-scale invasion of Ukraine in 2022 have produced repeated and highly visible instances of single-state blockage, bringing the unanimity rule's practical costs into sharp relief. Hungary alone has accounted for 19 of the 45 vetoes cast by EU member states in recent years, more than any other country, and as recently as March 2026 blocked a previously agreed €90 billion loan to Ukraine. The stated grounds for that veto were unrelated to the loan itself: Hungary objected to the continued operation of the Druzhba oil pipeline, a bilateral dispute with no direct bearing on the financial instrument being voted upon. The episode illustrated a broader pattern in which **the veto power is deployed not merely to protect a state's interests** in the matter under discussion, **but as general diplomatic leverage across unrelated policy files.**

3.4 EXTERNAL SHOCK / SECURITY CRISIS

This pattern has driven the most concrete governance reform debate currently before the Union. Since 2023, Germany has led a so-called **Group of Friends, a coalition of member states that advocates for expanding the use of qualified majority voting** within the framework of the existing treaties, without requiring treaty revision. In parallel, a Franco-German expert working group has proposed a more structured approach: combining an expanded passerelle clause with what it terms a sovereignty safety net, a set of procedural guarantees designed to reassure smaller and medium-sized member states that their vital interests would not be overridden under a more majority-based system. Several Central, Northern and South-Eastern European member states have nonetheless responded with scepticism, arguing that moving away from unanimity risks concentrating decision-making influence among the Union's largest members and would deprive smaller states of the leverage they currently exercise over decisions that directly affect their core national interests. At the institutional level, the Conference on the Future of Europe concluded in 2022 that the Union's unanimity-based procedures warranted revision, and the European Parliament reinforced that position by adopting a resolution specifically on the use of passerelle clauses in July 2023.

Figure 3: Divergent Crisis Response Dynamics in EU Decision-Making

Source: Own-elaboration



73 Björn Fägersten, "Intelligence and Decision-Making within the Common Foreign and Security Policy," European Policy Analysis, no. 2015:22, October 2015. https://sieps.se/media/cfnds5me/intelligence-and-decision-making-within-the-common-foreign-and-security-policy-2015_22epa.pdf.

The political landscape shifted further in April 2026, when the defeat of Hungary's Viktor Orbán, the EU's most frequent user of the veto, removed one of the most consistent obstacles to consensus on Ukraine-related measures, prompting renewed calls from Commission President Ursula von der Leyen to use the resulting political momentum to extend qualified majority voting into foreign policy. This momentum remains contested rather than settled. **Some member states continue to regard unanimity as an essential safeguard of national sovereignty** over security matters of vital national interest, fearing that majority voting could subordinate smaller states' positions to those of the largest; others argue that continued reliance on a single-state veto leaves the Union exposed to manipulation by any government willing to use it as diplomatic leverage, and that no functioning democratic body governs its core decisions by requiring the consent of every single member.

This **disagreement is not merely about voting thresholds: it reflects an unresolved tension** between the sovereign equality of member states and the Union's collective capacity to act, a tension the sections that follow examine through concrete proposals for legal and institutional reform, and for which procedural adjustment alone is unlikely to be enough.

The debate over QMV is, therefore, not just a technical one about voting rules; it is **a fundamental struggle over the nature of the EU as a security actor**. The reluctance of some member states, particularly smaller ones, to move away from unanimity reflects a deep-seated concern that their core national interests could be outvoted, a fear that is often framed as a defence of sovereignty. This highlights a persistent obstacle: without a genuine common strategic culture, a shared understanding of threats and appropriate responses, a shift to majority voting may simply transpose intergovernmental bargaining into a different procedural framework, without necessarily fostering more decisive or effective action.

Conclusion

The European Union's security architecture stands at a critical crossroads. The return of high-intensity conflict to the European continent, the rise of hybrid threats, and an increasingly fragmented geopolitical environment have demonstrated that **security can no longer be treated as a peripheral policy area, but as a core element of the European integration project.** Throughout this Policy Brief, it has been shown that while the EU has developed an increasingly sophisticated set of legal, financial, and strategic instruments under the CFSP and the CSDP —such as the European Defence Fund, SAFE, and the Rapid Deployment Capacity—, its capacity to act continues to be constrained by structural weaknesses embedded in its governance model.

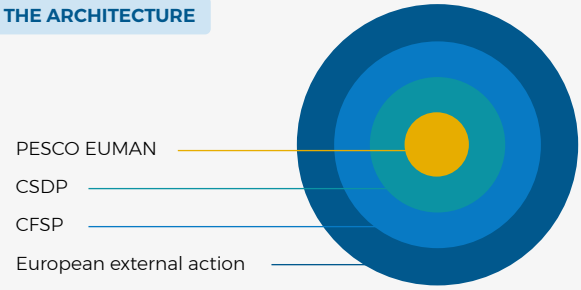
The principal bottleneck constraining collective action remains the unanimity rule embedded in Articles 24 and 31(1) TEU. In a Union of 27 Member States, this requirement enables individual governments to weaponise the veto as diplomatic leverage over unrelated policy files, forcing collective action down to the lowest common denominator under the constant "shadow of the veto". This political inertia is further compounded by a structural split in competences: while the European Commission exercises supranational legislative and financial powers to shape the defense industry under Articles 173 and 182 TFEU, military deployment and strategic direction remain strictly intergovernmental under the Council and High Representative, creating coordination drag even when political alignment exists.

To transition from systemic reactivity to permanent strategic readiness, the Union must pursue a dual-track reform strategy. In the immediate term, policymakers must fully exploit underutilised Treaty flexibilities, such as activating Article 44 TEU to delegate CSDP mission execution to coalitions of willing Member States, expanding constructive abstention (Art. 31(1) TEU), and selectively applying passerelle clauses (Art. 31(3) TEU). For long-term structural resilience, introducing Qualified Majority Voting alongside a procedural "sovereignty safety net" would mitigate minority capture while safeguarding vital national interests. Ultimately, procedural reforms alone are insufficient; closing the gap between operational capability and political execution will require the steady cultivation of a genuine, shared strategic culture across all Member States.

THE EU SECURITY ARCHITECTURE: GOVERNANCE IN A POST-2026 LANDSCAPE

Infographic — Forum on the Future of the EU 2026

THE ARCHITECTURE



Defence has **no legislative act** — only Council decisions & soft-law guidelines govern it, executed by the **High Representative** and the **EEAS.**

THE CORE BOTTLENECK: UNANIMITY

48
vetoes cast in CFSP decisions, 2011–2025

21
of those vetoes cast by a single state: Hungary

1/27
One dissenting government can hold the collective hostage — sanctions, missions & joint positions all need 100% agreement.

BUILDING THE TOOLBOX: CSDP MILESTONES

2001	2004	2005	2010	2017	2021
EUMS Military planning	**EDA** Capability forum	**EULEX Kosovo** Rule of law	**EEAS** Diplomatic arm	**PESCO** Joint cooperation	**EPF** Defence financing

SAME RULE, DIFFERENT SPEED

When threat perception is shared

Within days of Russia's Feb. 2022 invasion, the Council unanimously froze €210bn of Central Bank assets and cut 7 banks from SWIFT.

When one state has leverage

In March 2026, Hungary blocked a €90bn Ukraine loan over an unrelated pipeline dispute — proof the veto is used as generic leverage.

PATHWAYS TO REFORM

Constructive Abstention
Step aside without blocking (Art. 31 TEU)

QMV Extension
55% states / 65% population threshold

Passerelle Clause
Council shifts to QMV - no treaty change

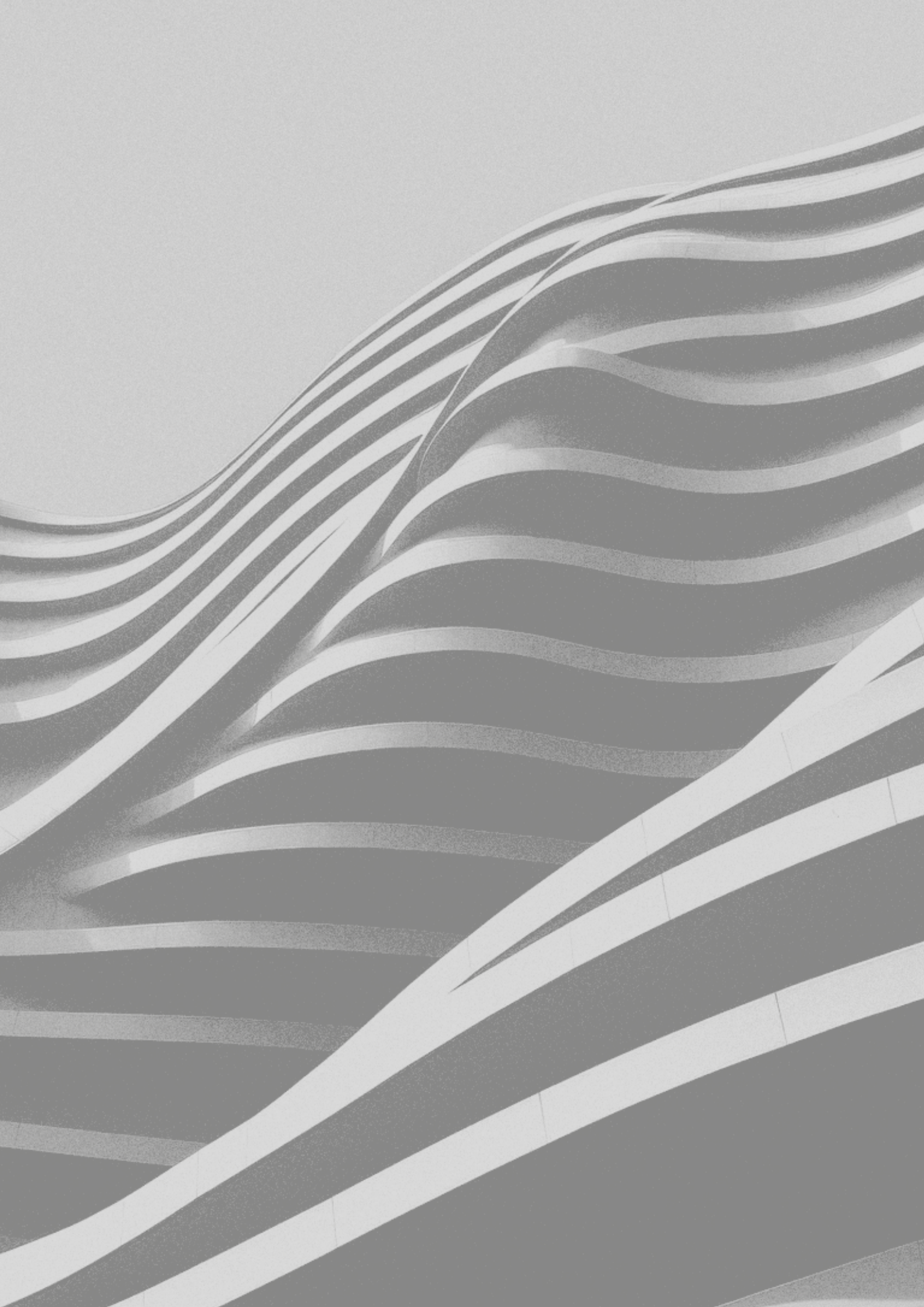
Sovereignty Safety Net
Vital-interest objection + secondary vote

From *reactive crisis-response to permanent strategic readiness:* the EU must combine existing treaty flexibilities with the political will for deeper reform.

Figure 0: Own elaboration, based on TEU/TFEU, EEAS Strategic Compass (2022) and Csaky & Grant (2025).

Glossary of abbreviations

CETA	Comprehensive Economic and Trade Agreement
CFSP	Common Foreign and Security Policy
CJEU	Court of Justice of the European Union
CSDP	Common Security and Defence Policy
EDA	European Defence Agency
EDF	European Defence Fund
EDTIB	European Defence Technological and Industrial Base
EEAS	European External Action Service
EIB	European Investment Bank
EIF	European Investment Fund
HR/VP	High Representative for Foreign Affairs and Security Policy (also Vice-President of the European Commission)
IntCen	(EU) Intelligence Analysis Centre
MFF	Multiannual Financial Framework
PESCO	Permanent Structured Cooperation
PSC	Political and Security Committee
QMV	Qualified Majority Voting
RDC	Rapid Deployment Capacity
SAFE	Security Action for Europe
SEAR	Solidarity and Emergency Aid Reserve
SIAC	Single Intelligence Analysis Capacity
SME	Small and Medium-sized Enterprise
STEP	Strategic Technologies for Europe Platform
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union



EQUIPO EUROPA



INTRODUCTORY CHAPTER 2

EU EXTERNAL ACTION AND GEOPOLITICS

STRATEGIC INTERESTS AND ALLIANCES IN A CHANGING SECURITY LANDSCAPE

Authors: Adrián Morcillo Pazos, Júlia Bagués Busuldo, Montse Aubeyzón Silva, Beatriz Sobral, Marta Praticò, Lungu Tudor Matei, Emma Díez Oricheta.
Reviewers: María Villaverde Temes.

Forum on the Future of the EU

EUROPEAN SECURITY in a Changing World

EXECUTIVE SUMMARY

The European Union (EU) is facing a very different security environment from the one it was designed for. Russia's invasion of Ukraine, growing competition between the United States of America (USA) and China, the consequences of the COVID-19 pandemic and increasing pressure on global supply chains have shown that economic interdependence alone is no longer enough to guarantee security. Today, issues such as energy, technology, critical raw materials and connectivity have become central to European foreign and security policy.

This policy brief explores how the EU can strengthen its role as a geopolitical actor while remaining committed to multilateralism and the rules-based international order. It argues that Open Strategic Autonomy (OSA) should not be understood as isolation or protectionism, but as the ability to reduce critical dependencies, increase resilience and protect European interests without abandoning international cooperation.

The analysis identifies the EU's main strategic priorities, including defence, economic security, technological leadership and the protection of the international order. It then examines how these priorities shape the EU's relations with USA, China and Russia, before turning to strategic partnerships in Africa, Latin America, the Indo-Pacific, the Middle East and the Arctic - regions that, despite their differences, have all become increasingly important for Europe's security, whether through critical resources, trade routes, energy, technology or political influence.

The paper also argues that strategic partnerships and enlargement form part of the same geopolitical strategy. Candidate countries such as Ukraine, Moldova and the Western Balkans are no longer discussed only in terms of accession criteria, but as part of the EU's long-term security and stability.

Ultimately, Europe's ability to act as a credible geopolitical actor will depend not only on military capabilities, but also on its capacity to build reliable partnerships, reduce strategic vulnerabilities and turn its economic and diplomatic strengths into coherent external action.

Keywords

Open Strategic Autonomy; European Security; Strategic Partnerships; EU Enlargement; Geopolitics; Economic Security.

INTRODUCTION

DEFINING THE EU'S ROLE AND ITS TRANSITION FROM AN ECONOMIC ACTOR TO A GEOPOLITICAL ACTOR

The EU was born from the conviction that power could be constrained by rules, and that war could be made not only unthinkable, but materially impossible through interdependence. The Schuman Declaration of 1950 expressed this logic with unusual clarity: **peace in Europe would not be secured by balance-of-power politics, but by binding the strategic interests of former rivals so closely together that conflict would lose both its political purpose and its material foundation**[1]. For decades, this idea shaped the European project internally and externally. The EU came to understand itself not as a traditional great power, but as a normative actor whose influence derived from regulation, multilateralism and the attraction of its economic model[2]. Over time, this was complemented by a distinct form of power, through which the EU used markets, standards and institutional innovation to project influence beyond its borders[3].

Yet the world for which this model was designed has become far less stable. As Josep Borrell argued, Europe has entered an age of geopolitics in which it must learn the "language of power" without abandoning its commitment to multilateralism, openness and international law[4]. The COVID-19 pandemic exposed Europe's dependence on external suppliers for essential goods, while Russia's full-scale invasion of Ukraine demonstrated that energy ties could be transformed into instruments of coercion rather than guarantees of peace[5]. At the same time, the intensification of USA-China rivalry and the politicisation of technology have shown that trade, technology and finance are increasingly used as tools of international competition[6]. Disruptions to maritime routes and growing competition over critical raw materials have further demonstrated that economic openness can generate strategic vulnerability when it is not accompanied by resilience and strategic capacity[7].

Russia's invasion of Ukraine was the clearest turning point in this transformation. It forced the EU to confront the return of large-scale war to the European continent, the limits of economic interdependence as a stabilising force, and Europe's persistent dependence on the North Atlantic Treaty Organization (NATO) and USA military ca-

1 Robert Schuman, "The Schuman Declaration," May 9, 1950. https://european-union.europa.eu/principles-countries-history/history-eu/1945-59/schuman-declaration-may-1950_en

2 Broeders, D., F. Cristiano, and M. Kaminska. "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions." JCMS: Journal of Common Market Studies (2023): 1–20. https://doi.org/10.1111/jcms.13462

3 Sarah Bauerle Danzman and Sophie Meunier, "The EU's Geoeconomic Turn: From Policy Laggard to Institutional Innovator," JCMS: Journal of Common Market Studies 62, no. 4 (2024): 1098–1115, https://doi.org/10.1111/jcms.13599

4 Josep Borrell, "Hearing of Josep Borrell, Vice-President-Designate of the European Commission, High Representative of the Union for Foreign Affairs and Security Policy: A Stronger Europe in the World," European Parliament, October 7, 2019, 4–5, https://www.europarl.europa.eu/resources/library/media/20191008RES63704/20191008RES63704.pdf

5 Niklas Helwig, "EU Strategic Autonomy after the Russian Invasion of Ukraine: Europe's Capacity to Act in Times of War," JCMS: Journal of Common Market Studies 61 (2023): 57–67, https://doi.org/10.1111/jcms.13527; Sarah Bauerle Danzman and Sophie Meunier, "The EU's Geoeconomic Turn: From Policy Laggard to Institutional Innovator," JCMS: Journal of Common Market Studies 62, no. 4 (2024): 1098–1115, https://doi.org/10.1111/jcms.13599

6 Josep Borrell, "Hearing of Josep Borrell, Vice-President-Designate of the European Commission, High Representative of the Union for Foreign Affairs and Security Policy: A Stronger Europe in the World"; D. Broeders, F. Cristiano, and M. Kaminska, "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions," JCMS: Journal of Common Market Studies (2023): 1–20, https://doi.org/10.1111/jcms.13462

7 Victoria Sainz, "The Red Sea Shipping Crisis (2024-2025): Houthi Attacks and Global Trade Disruption," Atlas Institute for International Affairs, March 27, 2025, https://atlasinstitute.org/the-red-sea-shipping-crisis-2024-2025-houthi-attacks-and-global-trade-disruption; Council of the European Union, "Maritime Security: Council Updates Mandates of EU Naval Operations ASPIDES and ATALANTA," press release, March 30, 2026, https://www.consilium.europa.eu/en/press/press-releases/2026/03/30/maritime-security-council-updates-mandates-of-eu-naval-operations-aspides-and-atalanta

pabilities[8]. However, the war also revealed the EU's capacity to act geopolitically through sanctions, financial assistance, energy diversification, and defence support mechanisms such as the European Peace Facility[9]. **Ukraine therefore exposed both the weakness and the potential of the EU as a strategic actor**: it showed that Europe remains dependent in hard security, but also that it possesses powerful legal, financial and economic instruments when political unity is achieved[10]. Furthermore, USA remains Europe's indispensable security partner, but recent shifts in American politics have made European dependence on Washington appear less predictable than before[11].

OSA has emerged as the EU's attempt to respond to this dilemma[12]. Charles Michel, then President of the European Council, framed it **as a generational priority**, linking it to EU's need to strengthen its independence and capacity to shape its own future. It does not mean isolation or protectionism. Rather, it reflects the ambition **to remain "as open as possible" while becoming "as autonomous as necessary"** in areas where dependence threatens EU's capacity to act[13]. OSA has not disappeared despite limited progress in defence integration; rather, it has become a broader Europeanised framework shaping EU policy across trade, industry, competition, digital governance, finance and security[14].

This ambition cannot be achieved through relations with great powers alone. Africa emerges not merely as a development partner, but as a central space where European security, climate policy, migration dynamics, institutional partnerships and external competition converge with their own agency, priorities and negotiating power[15]. In this wider regional landscape, Latin America and the Caribbean (LAC) also reveal a complementary potential. As Equipo Europa's 2025 report argues, the EU-LAC relationship stands at a crucial moment in a more multipolar world, after years in which the partnership had often been neglected. The region appears not only as a like-minded partner, but as a strategic arena for supply-chain diversification, critical raw materials, renewable energy, food security, democratic cooperation and the green and digital transitions[16].

The same logic applies to the Indo-Pacific, which can no longer be treated as distant from European security, since semiconductor supply chains, maritime routes, tensions around Taiwan and partnerships with India, Japan, South Korea and the Association of Southeast Asian Nations (ASEAN) connect regional stability directly to Europe's economic resilience and technological autonomy[17]. The Middle East and North Africa (MENA) performs a different but equally important role by linking Europe to energy flows, migration routes, maritime chokepoints, counterterrorism, Gulf partnerships and cross-regional connectivity projects such as the India-Middle East-Europe Economic Corridor[18]. The Arctic, finally, shows how climate change is transforming a once peripheral region into a strategic frontier of resource competition, maritime access, Russian militarisation, Chinese interest and renewed attention to Greenland[19]. This scenario demonstrates **the importance of understanding geographies as active sources of European resilience.**

This policy brief argues that OSA should be understood as the organising principle of the EU's emerging geopolitical role, offering a framework for turning vulnerability into capacity through coherence and strategic planning. It first identifies EU's core strategic interests, before examining how relations with USA, China and Russia's war against Ukraine reveal the limits and instruments of European autonomy. The brief then turns to the regional dimension of this agenda, analysing Africa, Latin

8 N. Helwig, "EU Strategic Autonomy after the Russian Invasion of Ukraine," 57–67; Council of the European Union, A Strategic Compass for Security and Defence: For a European Union that Protects Its Citizens, Values and Interests and Contributes to International Peace and Security (Brussels: Council of the European Union, 2022). https://www.consilium.europa.eu/en/policies/strategic-compass/

9 N. Helwig, "EU Strategic Autonomy after the Russian Invasion of Ukraine," 57–67.

10 N. Helwig, "EU Strategic Autonomy after the Russian Invasion of Ukraine," 57–67; Sarah Bauerle Danzman and Sophie Meunier, "The EU's Geoeconomic Turn: From Policy Laggard to Institutional Innovator," JCMS: Journal of Common Market Studies 62, no. 4 (2024): 1098–1115, https://doi.org/10.1111/jcms.13599

11 Johannes Nordin, Strategic Autonomy, Anyone? Charting Europe's Shifting Security Debates and 2024–2029 Priorities, Special Paper (Stockholm: Institute for Security and Development Policy, March 2025), 22–23, https://www.isdp.eu/wp-content/uploads/2025/03/Special-Paper-Johannes.pdf

12 Govaere, I. "On EU values and the open strategic autonomy paradox: Revisiting the EU as a global actor." Common Market Law Review 63 (2026): 147. https://doi.org/10.54648/cola2026011; Miró, J. "Responding to the global disorder: The EU's quest for open strategic autonomy." Global Society 37, no. 3 (2023): 315. https://doi.org/10.1080/13600826.2022.2110042.

13 L. Schmitz and T. Seidl, "As Open as Possible, as Autonomous as Necessary: Understanding the Rise of Open Strategic Autonomy in EU Trade Policy," JCMS: Journal of Common Market Studies 61, no. 3 (2023): 834–852, https://doi.org/10.1111/jcms.13428

14 J. Miró, "Responding to the Global Disorder: The EU's Quest for Open Strategic Autonomy," Global Society 37, no. 3 (2023): 315–335, https://doi.org/10.1080/13600826.2022.2110042

15 John K. Akokpari, "The European Union and Africa: The Political Economy of an Asymmetrical Partnership," in The ACP Group and the EU Development Partnership: Beyond the North-South Debate, ed. Annita Montoute and Kudrat Virk (Cham: Palgrave Macmillan, 2017), 55–78

16 José Antonio Sanahuja, "The European Union and Latin America in a Changing Global Order" (Madrid: Fundación Carolina, 2023); Equipo Europa, Forum on the Future of the EU 2025: Deepening Partnerships: EU-LATAM (Equipo Europa, 2025).

17 European Commission, The EU Strategy for Cooperation in the Indo-Pacific (Brussels: European Commission, 2021). https://www.eeas.europa.eu/sites/default/files/jointcommunication_2021_24_1_en.pdf

18 Gedaliah Afterman and Peter Hefele, Rethinking Europe's Middle East Strategy in a Changing World (Brussels: Wilfried Martens Centre for European Studies, August 2025), Maximilian Mayer, Gedaliah Afterman, N. Janardhan, and Mohammed Baharoon, Connectivity and "Reglobalization": India-Middle East-Europe Economic Corridor and Its Potential Digital Future (Abu Dhabi: Anwar Gargash Diplomatic Academy, 2025), https://www.agda.ac.ae/docs/default-source/2025/publications/imec-march-2025-update.pdf?sfvrsn=4be3633b_3.

19 Gabija Leclerc, EU Arctic Policy Update, Briefing PE 789.336, European Parliamentary Research Service (Brussels: European Parliament, June 2026), 2–3, https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/789336/EPRS_BRI(2026)789336_EN.pdf; López Coca, P., and Morcillo Pazos, A., "Comparativa de las políticas de la UE y de China en el Ártico. Nuevos retos en el Ártico tras la guerra de Ucrania," Quaderns IEE 1, no. 2 (2022): 87–114, https://doi.org/10.5565/rev/quadernsiee.33

America, the Indo-Pacific, MENA, and the Arctic as spaces where security, economic resilience, critical resources, technology, connectivity and political influence increasingly overlap. In doing so, the analysis also offers a starting point for asking what the EU can offer these regions in return, so that Strategic Autonomy (SA) becomes the basis for more reciprocal and sustainable partnerships. Finally, it considers enlargement as part of the same geopolitical shift, showing **how the EU's internal transformation is increasingly linked to its capacity to shape stability in its wider neighbourhood.**

1 GLOBAL STRATEGIC INTERESTS

Building on the EU's transition from a predominantly normative to an increasingly geopolitical actor outlined in Section I, this section maps the principal strategic interests that now define EU's engagement with the international system. These interests are not isolated policy objectives but form an interconnected architecture in which security, economic resilience, technological autonomy, and the defence of a rules-based order are mutually dependent.

1.1 OSA: THE FRAMING CONCEPT

The concept anchoring the EU's articulation of its global interests is OSA. Drawing on language first used in the EU Global Strategy of 2016 - which enshrined the ambition of SA - and formalised as a compound concept in the Commission's 2021 Trade Policy Review, **OSA encapsulates EU's aspiration to remain as open as possible to trade, to alliances, and to multilateral engagement, whilst developing the capacity to act independently when necessary**[20]. It reflects, in the words of one analysis, a new doctrine of qualified openness. The EU wants to be "as open as possible" but must also be "as autonomous as necessary"[21]. This framing has functioned as a coalition magnet - broad enough to unite diverse factions within EU institutions behind a shared direction - whilst justifying concrete departures from the previously dominant free-trade orthodoxy[22]. From its origins in trade policy, OSA has since expanded into industrial policy, energy, digital governance, and security and defence[23].

The **deliberate ambiguity of OSA has been both its strength and its limitation**: broad enough to sustain consensus among member states with divergent strategic cultures, it has also complicated the task of translating the concept into coherent and enforceable policy across domains.

The concept is not without its tensions: it presents an OSA paradox. By reducing economic dependencies - decoupling from Russian energy, limiting reliance on Chinese supply chains - the EU simultaneously weakens the trade leverage that previously gave it influence over those actor[24]. The instruments designed to protect EU strategic interests can, if pursued in isolation, reduce EU's capacity as a global actor.

1.2 SECURITY AND DEFENCE

The most fundamental strategic interest is the security of the EU's territory, citizens, and neighbourhood. Progress in developing autonomous military capabilities was for decades hampered by NATO's primacy, divergent national threat perceptions, and persistent member-state disagreements over the scope of European security integration[25]. SA in this domain remained **an aspiration rather than a political reality**[26]. The adoption of the EU's Strategic Compass in March 2022 represented a meaningful step in translating ambitions into concrete capability targets and counter-hybrid commitments, even if its early implementation was rapidly overtaken by events; subsequent progress has been substantial, with the EU Rapid Deployment Capacity becoming operational in May 2025 and most Compass objectives fulfilled by 2026 according to European External Action Service (EEAS) annual reporting.

Russia's full-scale invasion of Ukraine in 2022 altered this landscape. The invasion demonstrated that economic interdependence alone cannot de-

20 Govaere, I. "On EU values and the open strategic autonomy paradox: Revisiting the EU as a global actor." Common Market Law Review 63 (2026): 147. https://doi.org/10.54648/cola2026011; Miró, J. "Responding to the global disorder. The EU's quest for open strategic autonomy." Global Society 37, no. 3 (2023): 315. https://doi.org/10.1080/13600826.2022.2110042.

21 Schmitz, L. and Seidl, T. "As open as possible, as autonomous as necessary: Understanding the rise of open strategic autonomy in EU trade policy." JCMS: Journal of Common Market Studies 61, no. 3 (2023): 834. https://doi.org/10.1111/jcms.13428.

22 Schmitz and Seidl, "As Open as Possible," 847–848.

23 Michaels, E. and Sus, M. "(Not) Coming of age? Unpacking the European Union's quest for strategic autonomy in security and defence." European Security 33, no. 3 (2024): 384. https://doi.org/10.1080/09662839.2024.2376603; Miró, "Responding to the global disorder," 317–318.

24 Govaere, "On EU Values," 150–151.

25 Michaels and Sus, "(Not) Coming of Age?," 389–390.

26 Michaels and Sus, "(Not) Coming of Age?," 392.

ter conflict[27]. The EU's response - activating the European Peace Facility, coordinating sanctions, and launching a military training mission on EU soil - pointed to **a growing capacity for collective action**[28]. It also exposed deep dependence on American capabilities and persistent divergences among member states over EU's long-term security role[29]. The EU's genuine comparative advantage lies not in replicating NATO but in its legislative and financial instruments - the European Defence Fund, Permanent Structured Cooperation (PESCO), and economic statecraft - deployed in coordination with, rather than in competition to, the Alliance[30].

Most recently, the March 2025 Readiness 2030 initiative mobilised up to €800 billion[31] in coordinated defence investment across member states, marking the most significant collective EU defence spending commitment to date.

1.3 ECONOMIC SECURITY: ENERGY, SUPPLY CHAINS, AND CRITICAL RAW MATERIALS

The **COVID-19 pandemic exposed Europe's fragility in global supply chains**, and Russia's subsequent weaponisation of energy exports demonstrated that economic interdependence could become a direct tool of geopolitical coercion[32]. The EU had allowed economic dependencies to form without adequately accounting for the political risks they carried[33]. The RePowerEU plan, launched in May 2022, marked the first concerted attempt to treat energy dependency as a geopolitical rather than merely a commercial problem, accelerating diversification towards renewables and liquefied natural gas imports.

The European Strategy for Economic Security of June 2023 identified **four risk categories**: the resilience of supply chains, including energy security; the physical and cyber security of critical infrastructure; technology security and technology leakage; and the weaponisation of economic dependencies or economic coercion by third countries[34]. Of particular concern is Europe's near-total dependence on China for rare earth elements - including 100% of heavy rare earths and 97% of natural graphite - as well as its structural vulnerability in lithium, where China controls approximately 60% of global processing and refining capacity despite primary extraction being concentrated in Australia, Chile and Argentina. **These materials are indispensable for the green transition**[35]. The EU's response - "de-risking" rather than decoupling - seeks to diversify strategic supply chains without severing economic ties entirely[36], operationalised through

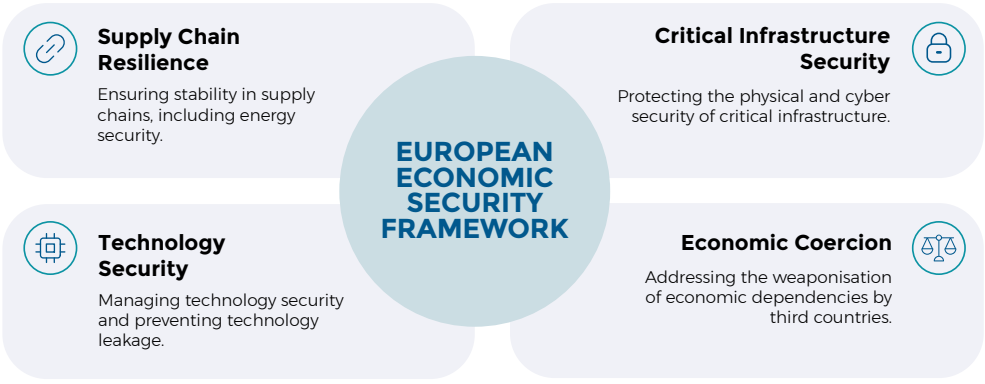


Figure 0: European Economic Security Framework

Source: own-elaboration, generated using AI

27 N. Helwig, "EU Strategic Autonomy after the Russian Invasion of Ukraine," 57–67.

28 N. Helwig, "EU Strategic Autonomy after the Russian Invasion of Ukraine," 57–67.

29 Michaels and Sus, "(Not) Coming of Age?," 393–395.

30 Michaels and Sus, "(Not) Coming of Age?," 396; N. Helwig, "EU Strategic Autonomy after the Russian Invasion of Ukraine," 57–67.

31 European Commission. "White Paper for European Defence - Readiness 2030." November 19, 2025. https://commission.europa.eu/topics/defence/future-european-defence_en.

32 Govaere, "On EU values," 144; Iacob, C.-G. "The strategic repositioning of the European Union in the new global geopolitical context." The Romanian Economic Journal 26, no. 86 (2023): 91.

33 Danzman, S. B. and Meunier, S. "The EU's geoeconomic turn: From policy laggard to institutional innovator." JCMS: Journal of Common Market Studies 62, no. 4 (2024): 1098. https://doi.org/10.1111/jcms.13599.

34 Iacob, "The Strategic Repositioning," 94–95.

35 Iacob, "The Strategic Repositioning," 97.

36 Iacob, "The Strategic Repositioning," 97–98; N. Helwig, "EU Strategic Autonomy after the Russian Invasion of Ukraine," 57–67.

the Critical Raw Materials Act, investment screening, and the Global Gateway initiative.

1.4 TECHNOLOGICAL SOVEREIGNTY

The EU's interest in technological sovereignty - the capacity to make autonomous choices based on its own values, respecting its own rules[37] - has translated into major legislative initiatives.These include the EU Chips Act, the AI Act, and the Digital Services and Digital Markets Acts, alongside the GAIA-X initiative - a federated data governance and trust-framework project that has faced significant implementation challenges and evolved away from its original ambition of a sovereign European cloud infrastructure[38]. In contrast to USA, which has favoured a more permissive, innovation-led approach to digital governance, **the EU has consciously chosen regulation as its primary instrument of technological positioning** - a choice that reflects its comparative strengths as a rule-maker rather than a technology producer.

The EU's regulatory power constitutes a genuine strategic asset: through the "Brussels Effect", European standards are frequently adopted globally, extending EU influence without coercive means[39]. However, this regulatory ambition carries its own risks. An excessive emphasis on digital sovereignty could generate strategic fragmentation among member states, ultimately weakening the very normative coherence that gives the EU its global standard-setting power[40].

1.5 MULTILATERALISM AND THE RULES-BASED INTERNATIONAL ORDER

A fourth strategic interest, often overshadowed but no less fundamental, is the EU's stake in a functioning multilateral order. **The EU's global influence is structurally dependent on a world organised around rules and institutions**. Democratic governance is, however, in retreat globally[41], and the EU's own difficulties in responding coherently to violations of international law have weakened its credibility as a principled actor[42]. The EU's mixed record in United Nations General Assembly votes following Russia's invasion of Ukraine - achieving broad condemnation but struggling to secure concrete penalties from major Global South partners - illustrates the limits of its multilateral leverage when confronted with genuine great power competition.

A strategy that increasingly limits cooperation to a shrinking circle of like-minded partners prevents the EU from leveraging trade to promote liberal democracy precisely where it might be needed most[43], risking a reduction of the EU to a regional rather than a global force. Upholding a rules-based order is, ultimately, the precondition for exercising all the other interests outlined above.

1.6 TOWARDS A COHERENT ARCHITECTURE OF INTERESTS

The four strategic interests examined here - security, economic resilience, technological sovereignty, and multilateralism - are interconnected but generate real trade-offs. Managing these tensions requires, as the ENGAGE research consortium has argued, that the EU become far more strategically selective in where it engages and what instruments it deploys, rather than attempting to address every challenge simultaneously[44]. The sections that follow examine how these interests are expressed in practice across the EU's key relationships and regions.

Figure 1: EU Strategic Interests



Source: own-elaboration, generated using AI.

37 Broeders, D., Cristiano, F. and Kaminska, M. "In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions." JCMS: Journal of Common Market Studies (2023): 7. https://doi.org/10.1111/jcms.13462.

38 Broeders, Cristiano, and Kaminska, "In Search of Digital Sovereignty," 7–13.

39 Broeders, Cristiano, and Kaminska, "In Search of Digital Sovereignty," 3; Govaere, "On EU Values," 142.

40 Broeders, Cristiano, and Kaminska, "In Search of Digital Sovereignty," 14–15.

41 Govaere, "On EU Values," 145–146.

42 Bouris, D., Fisher-Onar, N. and Huber, D. V. "Towards allyship in diversity? Critical perspectives on the European Union's global role." JCMS: Journal of Common Market Studies 63, no. 5 (2025): 1393–1394. https://doi.org/10.1111/jcms.13763.

43 Govaere, "On EU Values," 151.

44 Sus, M., Adebahr, C. and Saz-Carranza, A. "10 recommendations to make the European Union a stronger global actor." ENGAGE White Paper. June 2024, 2.

2 CHALLENGES WITH GREAT POWERS

2.1 RELATIONS WITH THE USA AND CHINA

The relationship between the EU and USA remains central to Europe's security architecture, yet the debate on SA reflects a growing concern over Europe's defence dependence.

In this context, SA should not be understood as a breaking away from the USA, but rather as the strengthening of European defence capabilities, while still working within NATO, and in order to enhance its ability to act within the alliance. This reflects a broader push to strengthen the transatlantic partnership, particularly given concerns about a shift in USA strategic focus towards Asia.

2.2 USA

The **EU and USA maintain the world's largest bilateral trade and investment relationship**, illustrating a high degree of economic interdependence that simultaneously strengthens the partnership and constrains the EU's capacity to fully detach itself from American influence. Together, the EU and USA account for approximately 43% of global Gross Domestic Product (GDP)[45].

Between 2017 and 2019, Donald Trump's policies, characterised above all by a strong aversion to multilateralism, the intensification of trade conflicts, and the widespread use of extraterritorial sanctions, surprised most EU leaders[46]. SA emerged as a pursuit of autonomy conceived as freedom from others, driven both by perceptions of USA unreliability and by the need to overcome the EU's internal lack of unity[47].

The EU and the USA **continue to cooperate closely on global security challenges**, including terrorism, nuclear proliferation and transnational crime. Nevertheless, Europe's reliance on USA military capabilities within NATO reinforces the debate on SA[48] and the need to develop stronger European defence capacities[49].

This highlights the structural nature of EU-USA interdependence, where European security remains closely tied to American military capabilities within NATO, limiting the EU's ability to act fully autonomously in defence matters[50].

2.3 CHINA

Over the past decade, China's political environment has become more closed and authoritarian. Furthermore, nationalism has grown and wider and more serious human rights violations occurred. Moreover, China's external behaviour has become more assertive and, sometimes, even confrontational[51].

Relations between the EU and China have progressively deteriorated since 2017. Since 2019, the economic competition and systemic rivalry have intensified[52], following the EU's characterisation of China as a cooperation and negotiating partner, as well as an economic competitor and a systemic rival[53]. Meanwhile, meaningful progress in EU-China negotiations has remained limited[54].

Besides its relations with the EU, China's relations with the USA and many of its neighbours have deteriorated and are marked by numerous points of tension[55].

In a context in which EU-China relations are constantly evolving, shaped by multiple sources of tension such as economic issues, human rights concerns, lack of equality for European companies operating in China, and geopolitical threats including the tensions in the Taiwan Strait and the South China Sea, **the EU proposed a "de-risking" strategy**. The strategy, still at an early stage of development, aims to manage the risks associated with economic and technological engagement

45 European Council. "EU relations with the United States." July 1, 2026. https://www.consilium.europa.eu/en/policies/united-states/.

46 Nordin, "Strategic Autonomy, Anyone?," 22-23.

47 Ibid.

48 European Council. "EU relations with the United States"

49 European External Action Service. "A Strategic Compass for Security and Defence." 2026. https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

50 NATO. Strategic Concept (2022). p. 6-7. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

51 Brinza, Andreea. "Study: EU-China relations: De-risking or de-coupling – the future of the EU strategy towards China". The Romanian Institute for the Study of the Asia-Pacific (26 March 2024). https://risap.eu/study-eu-china-relations-de-risking-or-de-coupling-%E2%88%92-the-future-of-the-eu-strategy-towards-china/.

52 Brinza, "Study: EU-China relations: De-risking or de-coupling – the future of the EU strategy towards China".

53 European External Action Service. "EU-China Relations". (6 December 2023). https://www.eeas.europa.eu/eeas/eu-china-relations_en.

54 Brinza, "Study: EU-China relations: De-risking or de-coupling – the future of the EU strategy towards China".

55 Ibid.

with China, mapping existing dependencies and identifying potential vulnerabilities[56].

Beyond geopolitical tensions, China's role as a major supplier in global value chains creates significant vulnerabilities for the EU, particularly in sectors such as critical raw materials, renewable energy technologies and digital infrastructure. This has led the EU to broaden the concept of SA to include economic security and technological sovereignty[57].

Currently, there is a broad consensus that the EU should avoid full decoupling from China and instead focus on targeted measures in areas of identified risk and dependency[58].

As a result, the EU seeks to manage its relationship with China through a strategy of de-risking[59], aiming to reduce critical dependencies while maintaining selective cooperation in areas of shared interest. **The concept of de-risking refers to the reduction of strategic vulnerabilities and excessive dependencies, while preserving economic engagement with China where possible, opposed to full decoupling.**

2.4 THE ROLE OF RUSSIA AND THE IMPACT OF THE WAR IN UKRAINE

Russia's war against Ukraine represents one of the most significant security challenges for the EU in the current international context. Unlike the EU's relations with USA and China, which are mainly shaped by alliance dependence, economic interdependence and systemic competition, relations with Russia have centred on the direct implications of the war for the European security order. Since February 2022, **the EU has defined Russia's full-scale invasion as a violation of international law and of Ukraine's sovereignty, independence and territorial integrity**[60].

The war has highlighted the limits of the EU's previous approach towards Russia, which combined economic interdependence, selective cooperation, sanctions after 2014 and support for conflict-management mechanisms. The annexation of Crimea and the destabilisation of eastern Ukraine had already challenged this model, but the full-scale invasion of 2022 has made clear that the EU can no longer rely solely on interdependence or dialogue as instruments of stability[61].

The EU's response has included a wide range of instruments. These include restrictive measures against Russia, financial and humanitarian assistance to Ukraine, support for refugees, energy diversification, reconstruction planning and defence-related assistance[62]. By April 2026, the EU had adopted 20 sanctions packages against Russia, aimed at increasing pressure on its war economy. In addition, the European Peace Facility, with a financial ceiling of more than €17 billion, has allocated €11.1 billion to military and defence-related support for Ukraine[63].

The war has also had **a direct impact on European economic and energy security**. One of the most visible changes has been the reduction of dependence on Russian gas. According to the Council of the EU, gas imports from Russia fell from 40% of total EU gas imports in 2021 to 15% in 2023. The European response has therefore not been limited to the military or diplomatic sphere, but **has also involved redefining economic vulnerabilities as security issues**[64].

Ukraine has become a central element of the EU's long-term geopolitical agenda. The Ukraine Facility provides €50 billion in stable and predictable support for the period 2024–2027, linking European assistance to recovery, reconstruction, reforms and Ukraine's path towards EU accession[65]. This is complemented by the €90 billion support loan for Ukraine approved in 2026, whose first disbursement amounted to €3.2 billion. The EU increasingly treats Ukraine not only as an emergency case, but also as part of the future European political and security landscape[66].

Furthermore, recent EU defence initiatives connect support for Ukraine with the broader strengthening of European defence readiness, as already dis-

56 Ibid.

57 European Commission. "Joint Communication to the European Parliament, the European Council and the Council on a European Economic Security Strategy." June 20, 2023. p. 7. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020

58 Ibid.

59 Brinza, "Study: EU-China relations: De-risking or de-coupling – the future of the EU strategy towards China".

60 Council of the European Union. EU response to Russia's war of aggression against Ukraine. https://www.consilium.europa.eu/en/policies/eu-response-russia-military-aggression-against-ukraine-archive/

61 Ibid.; Council of the European Union. A Strategic Compass for Security and Defence. https://www.consilium.europa.eu/en/policies/strategic-compass/.

62 Council of the European Union, European Peace Facility. https://www.consilium.europa.eu/en/policies/european-peace-facility/

63 Council of the European Union, Russia's war against Ukraine: EU sanctions. https://www.consilium.europa.eu/en/policies/sanctions-against-russia/

64 Council of the European Union. EU response to Russia's war of aggression against Ukraine. https://www.consilium.europa.eu/en/policies/eu-response-russia-military-aggression-against-ukraine-archive/

65 European Commission, Ukraine Facility. https://commission.europa.eu/topics/eu-solidarity-ukraine/eu-assistance-ukraine/ukraine-facility_en

66 European Commission, EU solidarity with Ukraine. https://commission.europa.eu/topics/eu-solidarity-ukraine_en

cussed in Section 1.2, closing capability gaps and reinforcing the European defence industry in response to the urgency of supporting Ukraine[67]. This reflects a broader shift in which **Ukraine's security and the EU's own security are increasingly understood as interconnected.**

The challenge that Russia poses to the EU is not limited to conventional military operations in Ukraine, it is also linked to energy security, cyber threats, disinformation, attacks on critical infrastructure, nuclear signalling, and attempts to exploit political divisions within European societies[68]. The EU's response to Russia is relevant not only to defence policy, but also to economic security, internal resilience, technology, energy, and democratic preparedness.

Overall, Russia's war against Ukraine has had a significant impact on the way the EU understands SA, and **it has become a central reference point for assessing whether the EU can translate its geopolitical ambitions into coherent and sustainable external action.**

3 REGIONAL POSITIONING: STRATEGIES IN AFRICA AND THE MIDDLE EAST

3.1 AFRICA

For decades, **EU-Africa relations have largely been structured around development cooperation, trade, political dialogue, and conditionality**. Rooted in a post-colonial legacy that has long shaped the terms of engagement, policies such as the European Neighbourhood Policy and the Africa-EU Partnership aimed to foster economic growth and stability. While this framework has contributed to long-term engagement, it is increasingly insufficient in a context marked by geopolitical competition, security instability, vulnerability, and the growing agency of African actors. Moreover, these frameworks have often remained shaped by aid-based logics, conditionality, and short-term policy horizons. Despite repeated attempts to strengthen cooperation, implementation has remained uneven, while regional integration has advanced only partially. A key criticism is that past EU approaches have not always sufficiently reflected Africa's political, economic, and social diversity,

Figure 2: Russia's War Impacts EU Security



Source: own-elaboration, generated using AI

67 European Commission, "White Paper for European Defence – Readiness 2030".

68 Council of the European Union, "Russia's War against Ukraine: EU Sanctions".

nor the importance of local ownership and African agency in shaping sustainable partnerships.

The EU should no longer approach Africa primarily as a recipient of aid but must treat African states and regional organisations as **strategic partners** in shaping a shared security and development agenda. Crucially, this also means recognising African actors not only as local implementers of European-designed frameworks but also as co-authors of international policy agendas, with their own priorities, interests, and negotiating power.

This shift is made more urgent by **the expanding presence of external actors across the continent**. China has strengthened its influence through infrastructure, investment, and connectivity projects, while Russia has increased its role through security cooperation, diplomatic engagement, and the exploitation of instability in fragile contexts. In an effort to step up, the EU should build on its comparative advantages: regulatory capacity, development finance, institutional partnerships, climate diplomacy, security training, and support for regional integration. However, these instruments must be deployed in a more coherent and politically strategic way[69].

The **Global Gateway represents a potentially important instrument** in this regard. Its Africa-Europe Investment Package aims to support green and digital transformation, sustainable growth, health systems, education, and infrastructure connectivity[70]. Yet its effectiveness will depend on whether it is perceived as a genuinely co-owned partnership or merely as a European response to China's Belt and Road Initiative. To avoid this risk, the EU should strengthen local ownership, increase transparency and align investment priorities with African regional agendas. In particular, Global Gateway should prioritise areas where African demand is strongest and where European comparative advantages are clearest: renewable energy transitions, digital infrastructure, transport corridors, and climate resilience. **Strategic partnerships cannot be built only through funding; they require trust, continuity, and recognition of African priorities**[71]. Equally important is that the EU makes the Global Gateway more politically visible, ensuring that African populations and governments perceive it as a meaningful and responsive commitment rather than a technical financing mechanism.

A more effective EU approach should also be **regionally differentiated**. Africa's political, economic, and security contexts are highly diverse, and a one-size-fits-all strategy risks being inefficient and weakening the EU's relevance. In North Africa, the EU's priorities are closely linked to energy, migration, Mediterranean stability, and connectivity. In the Sahel, the EU faces the challenge of recalibrating its engagement after years of instability, military takeovers, anti-Western sentiment, and the growing presence of alternative security partners. In West Africa and the Gulf of Guinea, maritime security, organised crime, trafficking, and democratic resilience are increasingly relevant to European security. In East Africa and the Horn, instability, climate pressures, food insecurity, and Red Sea dynamics connect local conflicts to wider geopolitical competition[72]. A regionally differentiated approach should draw on best practices already emerging from specific bilateral and multilateral engagements, learning from what has worked and **adapting frameworks to local political realities rather than applying uniform templates.**

For this reason, the **EU should frame Africa not only as a development partner but as a central component of European security.** Terrorism, organised crime, trafficking, climate change, and governance fragility do not remain confined to regional contexts; they shape migration dynamics, supply chains, energy routes, and Europe's wider strategic environment. At the same time, Africa should not be reduced to a security problem. An overly securitised approach would risk reinforcing mistrust and reproducing patterns of dependency. Instead, security cooperation should be embedded within broader political partnerships that include governance, climate adaptation, employment, education, digital transformation,

69 Council of the European Union, A Strategic Compass for Security and Defence: For a European Union that Protects Its Citizens, Values and Interests and Contributes to International Peace and Security (Brussels: Council of the European Union, 2022). https://www.consilium.europa.eu/en/policies/strategic-compass/

70 European Commission, "EU-Africa: Global Gateway Investment Package," International Partnerships, accessed June 10, 2026, https://international-partnerships.ec.europa.eu/policies/global-gateway/initiatives-sub-saharan-africa/eu-africa-global-gateway-investment-package_en.

71 Michele Collazzo, "The African Union–European Union Partnership at a Crossroads", IAI Commentaries 25, no. 59 (Rome: Istituto Affari Internazionali, November 2025), https://www.iai.it/it/pubblicazioni/c05/african-union-european-union-partnership-crossroads; Rossella Marangio, "Beyond Summits: The Africa-EU Partnership as a Priority", EUISS Brief (Paris: European Union Institute for Security Studies, March 4, 2026), https://www.iss.europa.eu/publications/briefs/beyond-summits-africa-eu-partnership-priority.

72 European External Action Service, "EU and North Africa," EEAS, August 11, 2025, https://www.eeas.europa.eu/eeas/eu-and-north-africa_en ; Angela Meyer, Loïc Simonet, and Johannes Späth, "The European Union and the Sahel: The Day After," Policy Analysis 1/2025 (Vienna: Austrian Institute for International Affairs, January 12, 2025; updated September 9, 2025), https://www.oiip.ac.at/en/publications/the-european-union-and-the-sahel-the-day-after/; Ivan U. Klyszcz and Rossella Marangio, "The Multi-Aligned Sahel: Reframing the EU's Role in a Crowded Region", EUISS Brief (Paris: European Union Institute for Security Studies, November 25, 2025), https://www.iss.europa.eu/publications/briefs/multi-aligned-sahel-reframing-eus-role-crowded-region; Rossella Marangio, "Deep Waters: The Maritime Security Landscape in the Gulf of Guinea," EUISS Brief (Paris: European Union Institute for Security Studies, January 9, 2025), https://www.iss.europa.eu/publications/briefs/deep-waters-maritime-security-landscape-gulf-guinea.

and regional economic integration[73]. Supporting local capacity-building and strengthening the legitimacy of African institutions must be seen as integral to European security interests, not as peripheral development concerns.

A credible EU strategy in Africa should therefore rest on **three priorities. First**, the EU should strengthen partnerships with African regional organisations, including the African Union and sub-regional bodies, to support conflict prevention, mediation, and regional integration[74]. **Second**, it should make Global Gateway more politically visible and more responsive to African priorities, particularly in renewable energy, transport corridors, digital infrastructure, and climate resilience[75]. **Third**, it should connect security cooperation with long-term state and societal resilience, ensuring that counterterrorism and border management are not separated from governance, development, and local legitimacy[76].

3.2 MENA: FROM CRISIS MANAGEMENT TO STRATEGIC ENGAGEMENT

MENA represents a different but equally crucial test for the EU's regional positioning. The region is directly connected to European security through energy flows, migration routes, maritime chokepoints, counterterrorism, conflict dynamics and strategic connectivity between Europe, Africa and Asia. Yet **the EU has often struggled to transform its economic and diplomatic weight into geopolitical influenc**e. Its role has frequently remained reactive, fragmented and constrained by internal divisions among Member States, particularly on the Israeli-Palestinian conflict, Iran, Syria and broader regional security questions[77].

The current regional environment makes this limitation increasingly costly. The crisis surrounding the Strait of Hormuz has become a major concern for the EU in 2026, given its implications for freedom of navigation, maritime security, energy supplies and global supply chains. At the same time, Iran's attacks and threats are increasingly extending beyond the region, with several European countries having been warned of possible retaliation[78]. Against this backdrop, the wars in Gaza and Lebanon, the fragility of ceasefires, tensions between Israel and Iran, instability in Syria, Houthi attacks affecting Red Sea shipping, and the broader recalibration of Gulf politics all underline the need for a more coherent and strategically focused EU Middle East policy[79].

The **EU's existing tools,** the European Neighbourhood Policy, the Union for the Mediterranean, the Middle East Peace Process framework, the regional strategy for Syria and Iraq, the position on Iran, and the Strategic Partnership with the Gulf, **provide important foundations. However, they remain too fragmented to produce a unified geopolitical posture**[80]. A more comprehensive EU strategy should connect crisis diplomacy with long-term strategic engagement. In the short term, the EU should maintain its support for a negotiated two-state solution, humanitarian assistance, Palestinian institutional reform, and stabilisation efforts in Lebanon, Syria and Gaza. However, this should be embedded within a wider regional strategy that also addresses energy diversification, maritime security, Gulf partnerships, digital infrastructure and connectivity. The Middle East should not be approached only as a space of conflict management but as a central corridor in the EU's broader geoeconomic and geopolitical positioning[81].

This is particularly relevant in the context of minilateralism and cross-regional connectivity. Initiatives such as the India-Middle East-Europe Economic Corridor (IMEC) show that t**he Middle East is increasingly becoming a bridge between**

73 Rossella Marangio, "Beyond Summits: The Africa-EU Partnership as a Priority," EUISS Brief (Paris: European Union Institute for Security Studies, March 4, 2026), https://www.iss.europa.eu/publications/briefs/beyond-summits-africa-eu-partnership-priority; European Commission, "EU-Africa: Global Gateway Investment Package," accessed June 10, 2026, https://international-partnerships.ec.europa.eu/policies/global-gateway/initiatives-sub-saharan-africa/eu-africa-global-gateway-investment-package_en; Arthur William Fodouop Kouam and Prisca Alphonus Chiefuna, "Rethinking European Union (EU)-Africa Relations in a Changing Global Landscape: Strategies for a Sustainable and Inclusive Partnership," presentation at the 8th International Conference on "Europe as a Global Actor," CEI-ISCTE, Lisbon, May 15–16, 2025, 13–14.

74 M. Collazzo, "The African Union–European Union Partnership at a Crossroads"; Rossella Marangio, "Beyond Summits: The Africa-EU Partnership as a Priority," EUISS Brief (Paris: European Union Institute for Security Studies, March 4, 2026), https://www.iss.europa.eu/publications/briefs/beyond-summits-africa-eu-partnership-priority.

75 European Commission, "EU-Africa: Global Gateway Investment Package"; Marangio, "Beyond Summits.

76 Ivan U. Klyszcz and Rossella Marangio, "The Multi-Aligned Sahel: Reframing the EU's Role in a Crowded Region," EUISS Brief (Paris: European Union Institute for Security Studies, November 25, 2025), https://www.iss.europa.eu/publications/briefs/multi-aligned-sahel-reframing-eus-role-crowded-region; Marangio, "Beyond Summits."

77 Christian Hanelt and Celine Plöger, Acting without Unanimity: How the EU Can Deliver in MENA: Lessons from the Middle East and North Africa on Turning Fragmentation into Strategic Leverage, Policy Brief (Gütersloh: Bertelsmann Stiftung, April 2026), https://www.bertelsmann-stiftung.de/en/unsere-projekte/projekte-startpunkt/building-european-resilience-and-security/project-news/acting-without-unanimity-how-the-eu-can-deliver-in-the-middle-east-and-north-africa-region.

78 Tim Ross et al., "Europe Braces as Iran Threatens to Attack," POLITICO Europe, March 4, 2026, https://www.politico.eu/article/iran-war-europe-braces-tehran-attack-retaliate-threat-missiles/.

79 Council of the European Union, "EU Position on the Situation in the Middle East," last reviewed July 2, 2026,https://www.consilium.europa.eu/en/policies/eu-position-situation-middle-east/.

80 Richard Youngs, "The EU's Dead-on-Arrival Pact for the Mediterranean," Carnegie Endowment for International Peace, September 18, 2025, https://carnegieendowment.org/research/2025/09/the-eus-dead-on-arrival-pact-for-the-mediterranean.

81 Gedaliah Afterman and Peter Hefele, Rethinking Europe's Middle East Strategy in a Changing World (Brussels: Wilfried Martens Centre for European Studies, August 2025).

Europe, the Gulf and Asia[82]. For the EU, IMEC is not only an infrastructure project; it is a potential instrument of SA. By supporting alternative trade routes, digital integration, energy cooperation and logistics resilience, the corridor can help Europe diversify its economic partnerships and reduce vulnerabilities linked to great-power competition and maritime disruption[83].

At the same time, **the EU must recognise that other actors are already shaping the regional order**. USA remains a key security actor but is often perceived as increasingly unpredictable. China has expanded its economic and diplomatic presence, especially in the Gulf, while avoiding major security responsibilities. **Russia continues to exploit regional instability where possible**, including through ties with actors in Syria, Iran and Libya. Türkiye has also positioned itself as a regional power broker, particularly in Syria and the Eastern Mediterranean[84]. Gulf states such as Saudi Arabia, the United Arab Emirates and Qatar are not passive partners, but increasingly autonomous middle powers able to shape regional and global diplomatic agendas[85].

In this context, **the EU's comparative advantage lies in its ability to combine diplomacy, investment, regulation, energy transition and security cooperation**. The Strategic Partnership with the Gulf should therefore be operationalised as a structured platform for strengthening European geopolitical resilience, including through regional security dialogue, green hydrogen cooperation, digital trade and connectivity, maritime security, crisis prevention and counter-terrorism[86]. Similarly, cooperation with Egypt, Jordan and other key partners should be linked to broader EU priorities on connectivity, migration governance, energy resilience and Mediterranean stability.

Maritime security is a particularly important area where regional instability directly affects European interests. The Red Sea crisis has demonstrated the vulnerability of global trade routes and the strategic importance of the Bab el-Mandeb Strait, the Gulf of Aden and the Suez route for European supply chains[87]. EU naval engagement, including EUNAVFOR ASPIDES, shows that it is capable of acting when commercial, security and geopolitical interests converge. ASPIDES was launched as a defensive maritime security operation under the Common Security and Defence Policy (CSDP) to safeguard freedom of navigation and protect merchant vessels in the Red Sea and surrounding waters[88]. However, **such operations should not remain isolated crisis responses**. They should be integrated into a broader EU maritime strategy connecting the Mediterranean, Red Sea, Gulf of Aden and Indian Ocean.

Overall, the EU's regional positioning in the Middle East should move beyond reactive diplomacy, including greater internal cohesion among Member States, clearer prioritisation of regional partnerships, and stronger integration between diplomatic, economic, energy and security tools[89]. Without this adjustment, the EU risks remaining financially engaged but politically marginal. With a more coherent approach, however, it can contribute to regional stabilisation while strengthening its own SA in a multipolar and increasingly contested international system.

82 Ibid; Express News Service, "New Economic Corridor to Connect Asia, Europe & US," The Sunday Standard, The New Indian Express, September 10, 2023, https://www.newindianexpress.com/thesundaystandard/2023/Sep/10/new-economic-corridor-to-connect-asia-europe-us-2613322.html ; Maximilian Mayer, Gedaliah Afterman, N. Janardhan, and Mohammed Baharoon, Connectivity and "Reglobalization": India-Middle East-Europe Economic Corridor and Its Potential Digital Future (Abu Dhabi: Anwar Gargash Diplomatic Academy, 2025), https://www.agda.ac.ae/docs/default-source/2025/publications/imec-march-2025-update.pdf?sfvrsn=4be3633b_3.

83 Afterman and Hefele, Rethinking Europe's Middle East Strategy.

84 Afterman and Hefele, Rethinking Europe's Middle East Strategy.

85 Ibid; Ahmed A. Shahbaz and Allan Hassaniyan, "The Growing Autonomy for GCC States' Foreign Policy and Structural Changes in the Balance of Power in the Region," Asian Journal of Middle Eastern and Islamic Studies 18, no. 4 (2024): 321–39, https://doi.org/10.1080/25765949.2025.2480007.

86 Beatrix Immenkamp, Roberto Bendini, and Perla Srour-Gandon, A Strategic Partnership with the Gulf: Old Ties, New Impetus, EPRS Briefing PE 739.228 (Brussels: European Parliamentary Research Service, December 2022), 1–7; Eszter Karacsony, "Strengthening EU Geopolitical Resilience Through Gulf Partnerships," ORF Middle East, June 3, 2025, https://orfme.org/research/eu-gulf-strategic-partnership-resilience/; European Council, "First European Union-Gulf Cooperation Council Summit – Joint Statement," 16 October 2024.

87 Victoria Sainz, "The Red Sea Shipping Crisis (2024–2025): Houthi Attacks and Global Trade Disruption," Atlas Institute for International Affairs, March 27, 2025, https://atlasinstitute.org/the-red-sea-shipping-crisis-2024-2025-houthi-attacks-and-global-trade-disruption/

88 Council of the European Union, "Maritime Security: Council Updates Mandates of EU Naval Operations ASPIDES and ATALANTA," press release, March 30, 2026, https://www.consilium.europa.eu/en/press/press-releases/2026/03/30/maritime-security-council-updates-mandates-of-eu-naval-operations-aspides-and-atalanta/.

89 Afterman and Hefele, Rethinking Europe's Middle East Strategy; Marius Strubenhoff, The European Union in the Middle East, cepAdhoc (Freiburg: Centre for European Policy Network, November 25, 2025), https://www.cep.eu/eu-topics/details/the-european-union-in-the-middle-east.html.

4 THE ARCTIC REGION: EMERGING SECURITY CHALLENGES, RESOURCE COMPETITION, AND GEOPOLITICAL INTERESTS IN THE HIGH NORTH

The **Arctic has ceased to be a cooperative environmental space and has become a contested geopolitical arena, and now the EU is caught in the middle without the institutional tools to respond effectively**. Following on the EEAS and Commission joint statement, the EU considers itself as a geopolitical power in the Arctic, actively pursuing strategic and day-to-day interests, both in the European Arctic and the broader region[90].

Three major pressures are converging simultaneously: USA, under President Trump's second term, has openly declared its ambition to bring Greenland under Washington's governmental control; Russia and China are deepening their security and economic partnership in the High North; and the progressive opening of Arctic Sea routes is accelerating the strategic value of the region for global trade and military positioning.

The EU's existing policy framework, anchored in the 2021 Joint Communication on a Stronger EU Engagement for a Peaceful, Sustainable and Prosperous Arctic, was designed for different times, ones premised on environmental diplomacy and peaceful multilateral cooperation. **That framework is now obsolete for contemporary challenges in matters of regional security and legislative order**. The expected 2026 Arctic Policy Update marks a pivotal moment for the EU as it transitions from environmental romanticism to strategic realism, or risks being sidelined in a region where its core interests in energy, critical minerals, trade routes, and security, are directly at stake[91].



Figure 3: The EU's Arctic Dilemma: Outdated Policy Meets New Realitie

Source: own-elaboration, generated using AI

4.1 THE CHANGING ARCTIC CONTEXT

The stakes of the Arctic have long been established by the interested parties. A 2009 USA Geological Survey estimated that the region holds 13% of the world's undiscovered oil and 30% of its natural gas[92]. By 2100, Arctic naval routes are projected to be fully navigable, transforming global shipping by offering a faster and cheaper alternative than existing corridors such as the Global South routes[93]. **These facts have attracted sustained interest from the world's major powers**.

Three external actors define the threat environment for the EU. Russia holds the strongest military and political presence in the region, with 24,140 kilometers of Arctic coastline[94], nuclear-powered icebreakers capable of year-round navigation, and a clear strategic interest in maintain-

90 European Commission and High Representative of the Union for Foreign Affairs and Security Policy. "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Stronger EU Engagement for a Peaceful, Sustainable and Prosperous Arctic." JOIN(2021) 27 final, October 13, 2021, 1–2. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021JC0027.

91 Gabija Leclerc, EU Arctic Policy Update, Briefing PE 789.336, European Parliamentary Research Service (Brussels: European Parliament, June 2026), 2–3, https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/789336/EPRS_BRI(2026)789336_EN.pdf.

92 Pincus R (2020) Three-way power dynamics in the Arctic. Strategic Studies Quarterly, 14(1): 40-63, Spring, https://www.jstor.org/stable/26891883, accessed June 20, 2026

93 Ranj Tofik, "Arctic Geopolitics: Strategic Stakes for China, Russia and the U.S.," Geopolitical Monitor, April 15, 2025, https://www.geopoliticalmonitor.com/arctic-geopolitics-strategic-stakes-for-china-russia-and-the-u-s/.

94 Ibid.

ing dominance over the Northern Sea Route (NSR). The so-called 1987 Murmansk speech of Mikhail Gorbachev describing the Arctic as a "peace and cooperation zone", can no longer be considered valid for the current overall Russian Arctic strategy[95]. China, despite lacking geographical proximity to the Arctic, declared the Polar Silk Road in 2018 as an extension of its Belt and Road Initiative and holds observer status at the Arctic Council since 2013; China's primary interest is securing faster, cheaper maritime trade routes that bypass nodes under foreign political influence, especially the American ones. USA, meanwhile, is pursuing an increasingly extractive and unilateral Arctic strategy, exemplified by Trump's Greenland ambitions and a sweeping expansion of its icebreaker fleet through the ICE Pact with Canada and Finland[96].

The EU faces a concerning institutional vulnerability for several reasons. Firstly, the EU is not a member of the Arctic Council, the primary regional negotiation forum. Secondly, the EU's CSDP does not fully extend to Overseas Countries and Territories (OCTs) such as Greenland, leaving critical legal gaps in the application of Article 42(7) of the Treaty on European Union (TEU)[97] - the Mutual Assistance Clause - and Article 222 of the Treaty on the Functioning of the European Union (TFEU)[98] - the Solidarity Clause. Furthermore, NATO's Article 5[99] collective defence mechanism was not designed to address threats originating from within the alliance itself, meaning that USA pressure on Greenland falls entirely outside established collective security frameworks, rendering the Article obsolete.

4.2 THE EU STAKES IN THE ARCTIC REGION

The **EU's exposure in the Arctic is substantial across five dimensions**: energy, environment, critical minerals, security and trade.

4.2.1 Energy

The EU imports between 30 and 40%of its Arctic fish and depends heavily on Arctic energy suppliers. Norway has become the EU's most important external gas supplier, accounting for 52.1% of all pipeline natural gas imported into the bloc, and its second largest oil supplier after USA[100]. This dependence, deepened by the rupture with Russia following the invasion of Ukraine, makes Arctic energy security an existential concern for the European economy.

4.2.2 Environment

The Arctic is warming at almost twice the global average rate, and its summer sea ice has decreased by more than 40% since 1979, physical changes that are directly accelerating the geopolitical competition the EU now faces. The 2021 Joint Communication placed the European Green Deal at the heart of EU Arctic engagement. Environmental leadership is not only a normative commitment, but a source of diplomatic leverage and regulatory influence that the EU must deploy strategically.

4.2.3 Critical Minerals

Greenland alone ranks eighth globally in rare earth element reserves, holding an estimated 1.5 million tons, and hosts two of the largest untapped critical mineral deposits on Earth: Kvanefjeld and Tanbreez[101]. These minerals are essential to the EU's green and digital transitions, sectors where the bloc remains deeply dependent on Chinese-controlled supply chains. The loss of meaningful access to Greenland's resources, whether through USA annexation or Chinese investment lock-in, would directly undermine Europe's SA agenda.

4.2.4 Security

The **Arctic's growing militarisation poses a direct security challenge for the EU**. Russia's sustained military build-up along the Arctic coastline, including the modernisation of Cold War-era bases and the deployment of advanced missile systems, has shifted the regional balance of power decisively. The Greenland–Iceland–United Kingdom (GIUK) gap, long a critical NATO chokepoint for monitoring submarine and naval movements between the Greenland Sea and the North Atlantic, has regained strategic centrality. Yet the EU's ability to contribute meaningfully to Arctic security is constrained by two structural gaps: the CSDP's incomplete coverage of OCTs such as Greenland, and the absence of a coordinated EU defence in-

95 Federico Aznar Fernández-Montesinos, "El Ártico como espacio de conflicto geopolítico," in Panorama geopolítico de los conflictos 2020 (Madrid: Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2020), 45-60, https://publicaciones.defensa.gob.es/panorama-geopolitico-de-los-conflictos-2020-revistas-ebook.html.

96 Mike Schuler, "Davie Defense Finalizes $3.5 Billion U.S. Coast Guard Arctic Security Cutter Deal," gCaptain, May 13, 2026, https://gcaptain.com/davie-finalizes-arctic-security-cutters-deal/.

97 Treaty on European Union, art. 42(7), 2016 O.J. (C 202) 13.

98 Treaty on the Functioning of the European Union, art. 222, 2016 O.J. (C 202) 47.

99 North Atlantic Treaty, art. 5, April 4, 1949, 34 U.N.T.S. 243.

100 Eurostat, "EU Imports of Energy Products - Latest Developments," Statistics Explained, European Commission, last modified March 25, 2026, accessed June 20, 2026, figs. 6–7, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=EU_imports_of_energy_products_-_latest_developments.

101 Meredith Schwartz and Gracelin Baskaran, "Greenland, Rare Earths, and Arctic Security," Center for Strategic and International Studies, January 8, 2026, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2026-01/260108_Schwartz_Greenland_Security.pdf.

dustrial and military capability. With the recent NATO accession of Nordic EU Member states, Finland and Sweden, the alliance's Arctic posture has strengthened, but EU-level security coordination in the region remains underdeveloped and dependent on bilateral arrangements that bypass Brussels entirely.

4.2.5 Trade

The Arctic's opening routes represent both an opportunity and a vulnerability. The GIUK gap is a critical naval chokepoint controlling access to major transatlantic trade routes. In late 2025, the "Istanbul Bridge" Chinese container ship completed the Northeast Passage from Zhejiang to Felixstowe in just 20 days, less than half the standard Suez Canal transit time, demonstrating that Arctic shipping has moved from theory to operational reality[102]. If the EU is absent from the governance of these routes, others will set the rules.

4.3 THE CURRENT EU POLICY REALITIES AND FURTHER RECOMMENDATIONS

4.3.1 Anchor the Greenland Partnership Strategically

The European Commission's proposed increase in financial support to Greenland under the 2028–2034 Multiannual Financial Framework (MFF), from EUR 225 million to EUR 530 million should be framed and operationalised as a geopolitical investment, not development aid[103]. **Funding priorities should be tied explicitly to critical mineral access agreements, infrastructure resilience, and environmental governance**, providing Nuuk with a credible European economic alternative to both Chinese capital inflows and USA political pressure.

4.3.2 Expand the EU's Regulatory Power through the Brussels Effect

The EU's most effective tool in the Arctic is not military but regulatory. The bloc should actively leverage its standard-setting power in environmental governance, resource extraction norms, and maritime safety to shape the behaviour of Arctic and non-Arctic actors alike. This approach should be deepened through engagement with Iceland, which is set to vote in a referendum on resuming frozen EU candidacy negotiations in August 2026.

4.3.3 Reform the CSDP to Seal the OCT Legal Gap

The exclusion of OCTs from the full scope of EU mutual defence obligations represents a critical structural vulnerability. The Council should mandate a formal legal review of the applicability of Article 42.7 TEU[104] and Article 222 TFEU[105] to OCT scenarios, with particular focus on Greenland. Where treaty amendment is not politically feasible in the short term, enhanced bilateral security **arrangements between Denmark and key EU partners, explicitly coordinated at EU level, should be established as an interim measure.**

4.3.4 Build a Coordinated EU Arctic Industrial and Defence Capability

The EU possesses the industrial and technological know-how to project credible defence capability in the Arctic. Finland's icebreaker shipbuilding expertise, demonstrated through its participation in the USA-led ICE Pact, represents a powerful competitive advantage for the European industry. Rather than allowing such capacity to be channelled exclusively through bilateral arrangements with third countries, the EU should develop a coordinated Arctic defence industrial framework under the European Defence Agency, pooling member state expertise in icebreaker construction, Arctic surveillance, and underwater naval technology.

4.3.5 Diversify Energy and Critical Mineral Supply Chains

The EU's structural dependence on single suppliers, such as Norway for gas, and China for rare earths, is a strategic liability. The upcoming Arctic Policy Update should include binding supply chain diversification targets for Arctic-sourced energy and critical minerals, supported by dedicated investment instruments under the EU Critical Raw Materials Act and the European Investment Bank. Partnership frameworks with Arctic states and territories should include explicit resource access provisions, integrated into the broader EU-SA agenda.

102 Heiner Kubny, "Through the Northeast Passage in Record Time," Polar Journal, November 3, 2025, https://polarjournal.net/through-the-northeast-passage-in-record-time/.
103 European External Action Service, "The EU in the Arctic," European Union, last modified January 28, 2026, accessed June 20, 2026, https://www.eeas.europa.eu/eeas/eu-arctic_en.
104 Treaty on European Union, art. 42(7), 2016 O.J. (C 202) 13.
105 Treaty on the Functioning of the European Union, art. 222, 2016 O.J. (C 202) 47.

4.3.6 Integrate Environmental Governance as a Strategic Instrument

The EU's environmental engagement in the Arctic must be embedded within its security and economic strategy, not treated as a parallel track. The 2021 Joint Communication placed the European Green Deal at the heart of EU Arctic engagement, and the 2026 update must build on that commitment. With the Arctic warming at almost twice the global average rate, the Commission should leverage its environmental leadership, Copernicus and Galileo satellite monitoring, black carbon reduction targets, and Horizon Europe research frameworks, as diplomatic currency with Arctic partners, while enforcing binding environmental and indigenous community standards on critical mineral extraction that competitors like China cannot easily match.

4.4 CRITICAL ASSESSMENT: THE EU STRATEGY IN THE ARCTIC REGION

The Arctic has ceased to be a peripheral environmental concern for the EU and has become a frontline of geopolitical competition. In this sense, the EU has the regulatory instruments, the financial leverage, and the member-state industrial expertise to be a meaningful Arctic actor. What it has lacked is institutional coherence and political urgency.

The convergence of USA unilateralism over Greenland, deepening Russo-Chinese cooperation, and the accelerating opening of Arctic Sea routes means **the window for the EU to shape the region's governance architecture is narrowing.** Positions are hardening, infrastructure is being built, and legal precedents are being set without European input.

A genuinely autonomous EU Arctic strategy requires moving beyond the comfort of environmental diplomacy and accepting the demands of hard geopolitical competition: secured resource access, credible defence commitments, reformed legal frameworks, and sustained financial engagement with Arctic partners. The cost of inaction is not the status quo, but it is a High North governed by others, on terms the EU will have had no part in setting.

5 OPPORTUNITIES AND NEW ALLIANCES: STRATEGIC PARTNERSHIPS AND ENLARGEMENT IN A GEOPOLITICAL EUROPE

The international environment has undergone significant changes over the last decades, especially when considering the events that have taken place since the beginning of 2020. Developments such as the COVID-19 pandemic, Russia's invasion of Ukraine and the growing competition between USA and China have forced the EU to reconsider some of the ideas that had guided its foreign policy since the end of the Cold War[106].

For a long time, the EU has been perceived primarily as an economic and normative power, strongly committed to political cooperation and development assistance. Its influence was largely based on trade, public diplomacy and the promotion of international norms aimed at preserving peace and security. However, in today's world, **security, economics and geopolitics are becoming increasingly interconnected.**

Europe is living in an age of geopolitics and must be able to learn the "language of power"[107] if it wants to remain an influential actor in an increasingly competitive world. However, this should not be understood as abandoning the EU's traditional commitment to multilateralism, openness and respect for international law. Rather, it means **recognising that economic dependencies, technological vulnerabilities and geopolitical rivalries can have direct consequences for European security** and that, therefore, a shift in the EU's strategic priorities has become necessary.

Russia's invasion of Ukraine represented a turning point that accelerated this process of strategic awareness. It highlighted that security in Europe cannot be taken for granted and that economic interdependence alone does not always guarantee either peace or stability. Furthermore, the conflict demonstrated how economic relations can be transformed into instruments of political pressure and how issues traditionally considered economic, such as energy supplies from external providers, may have significant geopolitical implications.

106 Council of the European Union, A Strategic Compass for Security and Defence.

107 Josep Borrell, "Europe in the Age of Geopolitics," speech before the European Parliament, Strasbourg, October 16, 2019.

Seen from this perspective, strategic partnerships and enlargement are not separate instruments, but complementary ones. Together, they enable the EU to shape its external environment, reduce its vulnerabilities and reinforce its own position. These two tools are central to the EU's ability to pursue its objectives and secure its position in a changing world, allowing it to create a more favourable environment for itself and its members while ensuring it is prepared for whatever comes next.

5.1 STRATEGIC PARTNERSHIPS: FROM INTERDEPENDENCE TO SECURITY

One of the main lessons of recent years is precisely the one mentioned above: **interdependence does not automatically generate security**[108]. Today's world is highly globalised, characterised by deep economic, technological and commercial connections[109]. However, rather than reducing risks, these connections can sometimes become sources of vulnerability when they are used for geopolitical purposes.

The COVID-19 pandemic was one of the first events to expose this reality, revealing Europe's dependence on external suppliers for certain strategic goods and raw materials. Shortly afterwards, the energy crisis triggered by Russia's invasion of Ukraine showed how areas traditionally viewed as purely economic, such as gas, oil or coal supplies, could be transformed into tools of political pressure. At the same time, growing concerns about China's dominant position in sectors such as rare earths, batteries, electric vehicles and telecommunications have reopened the debate on the risks associated with excessive dependence on external actors.

As a result, **the EU has increasingly started to rethink the relationship between economic openness and security**. The question is no longer whether Europe should remain actively engaged in the global economy, but how it can do so while reducing the vulnerabilities that may limit its ability to act independently. In this context, concepts such as ***de-risking*** have gained increasing relevance, as they seek to reduce strategic dependencies without completely disrupting international economic relations.

This debate is closely linked to the idea of OSA[110], which has become one of the most influential concepts in recent European discussions. **The aim is not to isolate Europe or move towards protectionism, but rather to ensure that openness does not become a source of vulnerability**. This approach can be seen in the European Economic Security Strategy of 2023, which identifies critical technologies, strategic supply chains and economic resilience as key elements for both the security and competitiveness of the EU.

In this context, strategic partnerships are no longer simply trade arrangements. They have become instruments through which the EU seeks to strengthen supply-chain resilience, secure access to critical resources, promote technological cooperation and increase its geopolitical influence.

As both Mario Draghi[111] and Enrico Letta[112] have argued in their 2024 reports, **Europe's economic competitiveness and its geopolitical relevance can no longer be separated**. An EU that loses technological leadership or industrial capacity may also lose its ability to defend its interests and values internationally.

5.2 LATIN AMERICA: A NATURAL PARTNER IN AN AGE OF STRATEGIC COMPETITION

Among the EU's strategic partners, Latin America has gained increasing relevance in recent years. Unlike other regions, where international relations are often shaped by geopolitical tensions or security concerns, **the relationship between the EU and Latin America has historically been built on a more positive foundation, characterised by strong historical and cultural ties**[113], as well as a broadly shared vision of the international order based on multilateralism, international cooperation and respect for international law[114]. These common principles[115] have generally facilitated a more

108 Mark Leonard, The Age of Unpeace: How Connectivity Causes Conflict (London: Penguin Random House, 2021), https://cdn.penguin.co.uk/dam-assets/books/9780552178273/9780552178273-sample.pdf.

109 Leonard, The Age of Unpeace.

110 European Commission, European Economic Security Strategy.

111 Mario Draghi, The Future of European Competitiveness (Brussels: European Commission, 2024). https://commission.europa.eu/topics/competitiveness/draghi-report_en

112 Enrico Letta, Much More Than a Market: Speed, Security, Solidarity (Brussels: European Commission, 2024). https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf

113 Timothy Garton Ash, Homelands: A Personal History of Europe (London: Bodley Head, 2023).

114 European Union and CELAC, EU-CELAC Summit Declaration (Brussels, 2023), https://ec.europa.eu/commission/presscorner/detail/en/statement_23_3924.

115 Sanahuja, "The European Union and Latin America in a Changing Global Order".

constructive political dialogue than the one the EU maintains with many other strategic regions.

However, Latin America's strategic importance goes far beyond shared values or political cooperation. In a context defined by the green and digital transitions, access to critical raw materials has become an increasingly important geopolitical issue[116]. The growing demand for minerals required for batteries, electric vehicles and renewable energy technologies has significantly increased European interest in the region, which is **seen as a key partner for achieving the EU's climate neutrality and green transition objectives.**

Countries such as Chile and Argentina possess some of the world's largest reserves of lithium and copper[117], both of which are essential for the energy transition. Meanwhile, Brazil plays a crucial role not only as an agricultural powerhouse but also in areas such as environmental protection, food security and regional stability[118]. From this perspective**, strengthening relations with Latin America is not only about economic interests**; it is also about increasing European resilience and diversifying dependencies in strategic sectors, particularly energy and critical supply chains, thereby reducing potential vulnerabilities linked to major powers such as China and, to a lesser extent, Russia.

This last point is particularly important given China's growing economic presence in the region[119] over the past two decades. **As Chinese investment and trade have expanded across Latin America, the EU faces the challenge of consolidating itself as a reliable long-term partner**, capable of offering investment, economic cooperation and institutional support without framing the relationship through a logic of geopolitical confrontation.

This growing importance helps explain why the EU-Mercosur Agreement has become such a relevant issue for both regions. After more than twenty years of negotiations, a political agreement was finally reached in December 2024, marking a major step towards the conclusion of the partnership. In January 2026, the Council authorised the signature of the agreements, and the Interim Trade Agreement (iTA) has been provisionally applied since 1 May 2026. If fully implemented, **the agreement would create one of the largest free trade areas in the world**, covering more than 700 million people. Beyond tariff reductions, it also includes provisions on services, public procurement, intellectual property and sustainable development, reflecting the broad and ambitious nature of the relationship between both blocs.

At the same time, the final stages of the agreement continue to reveal some of the challenges affecting EU-Latin America relations. Several European countries have raised concerns about environmental standards and the potential impact on their agricultural sectors, while Mercosur countries have criticised what they perceive as additional conditions imposed by the EU after the negotiations had been concluded. The nature of the current uncertainty, however, is different from that surrounding the agreement after the 2019 political deal. Rather than being centred on the conclusion of negotiations, it now concerns the agreement's institutional and legal future. In particular, the European Parliament has requested an opinion from the Court of Justice of the European Union (CJEU) on the compatibility of the agreement with the EU Treaties, adding a further legal dimension to the process.

For this reason, **the future of the agreement goes beyond trade itself.** Its implementation has become a test of whether both regions are able to translate long-standing political ambitions into concrete institutional action. At a time when protectionism is growing and geopolitical competition is becoming more intense, the implementation of the EU-Mercosur Agreement would send a strong signal in favour of open cooperation and rules-based international relations, while also demonstrating the capacity of the EU and Mercosur to overcome the political and legal obstacles that have shaped their relationship for decades.

5.3 THE INDO-PACIFIC: A STRATEGIC NECESSITY

If Latin America has been presented as an opportunity to diversify partnerships and reduce excessive dependencies, the Indo-Pacific has become a genuine strategic necessity for the EU. **The centre of gravity of the global economy is gradually shifting towards Asia**[120]. The region's importance,

116 European Commission, Regulation (EU) 2024/1252 Establishing a Framework for Ensuring a Secure and Sustainable Supply of Critical Raw Materials (Brussels, 2024), https://eur-lex.europa.eu/eli/reg/2024/1252/oj.

117 Andrés Malamud and Luis Schenoni, "Geopolitical Aspects of the EU-Mercosur Agreement" (Study requested by the AFET Committee, European Parliament, June 2025), https://www.europarl.europa.eu/RegData/etudes/STUD/2025/754478/EXPO_STU(2025)754478_EN.pdf.

118 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication to the European Parliament and the Council: A New Agenda for Relations between the EU and Latin America and the Caribbean," JOIN(2023) 17 final, June 7, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023JC0017.

119 Sanahuja, "The European Union and Latin America in a Changing Global Order."

120 Parag Khanna, The Future Is Asian: Commerce, Conflict, and Culture in the 21st Century (New York: Simon & Schuster, 2019).

however, goes well beyond economics. The Indo-Pacific contains some of the world's busiest maritime routes, is home to several major powers and has become the main stage for geopolitical competition in the twenty-first century.

This has direct implications for Europe. Rising tensions around Taiwan[121] have exposed how dependent the EU remains on Asian semiconductor production, a key component for industries ranging from automotive manufacturing to telecommunications and digital technologies. **Any disruption to trade routes in the South China Sea would also have an immediate impact on international trade and European supply chains**, something that became much easier to understand after the disruptions caused by the COVID-19 pandemic. The stability of the Indo-Pacific therefore matters to Europe far more today than it did only a decade ago.

The EU recognised this shift when it adopted its Indo-Pacific Strategy[122] in 2021 and began strengthening relations with several partners across the region. Japan and South Korea stand out because of their technological leadership and their role in sectors such as innovation and cybersecurity. India is becoming one of the most influential actors in the international system thanks to its growing economic and political weight[123]. ASEAN also plays an important role by promoting dialogue and cooperation in a region increasingly shaped by competition between major powers.

European engagement in the Indo-Pacific reflects a broader change in the way the EU understands security. Technology, supply chains, geopolitical competition and economic resilience are now closely connected. **What once seemed like a distant region has become a key area for protecting European interests and strengthening the EU's position in an increasingly competitive world.**

5.4 ENLARGEMENT AS A SECURITY POLICY

The Russian invasion of Ukraine has completely reshaped the debate on EU enlargement. Until a few years ago, enlargement had largely lost political momentum. After all, Croatia became the last country to join the EU in 2013, and the accession process was mostly seen as a technical matter linked to compliance with the 1993 Copenhagen criteria. Since Russia's invasion of Ukraine in February 2022, however, enlargement has returned to the centre of European discussions, this time with a much stronger focus on security and the EU's geopolitical position. **Enlargement can no longer be viewed solely through a bureaucratic or institutional lens, but increasingly as a question of strategic positioning**[124].

One clear sign of this shift is the fact that four countries have obtained candidate status since 2022: Ukraine, Moldova, Georgia and Bosnia and Herzegovina[125]. Today, the discussion goes far beyond the reforms required for accession. Instead, the debate is increasingly centred on how the EU can contribute to stability in its neighbourhood and strengthen its capacity to act in a more uncertain international environment. Ukraine's future accession would reinforce the EU's eastern flank while bringing in a country that has developed significant military and technological capabilities since the outbreak of the war. A similar argument can be made for Moldova and the Western Balkans, whose integration could help reduce the influence of external actors such as Russia and China while promoting greater political and economic stability in Europe's immediate neighbourhood.

At the same time, enlargement raises important challenges. A larger EU may find it more difficult to reach consensus, particularly in areas where unanimity is still required, such as the Common Foreign and Security Policy. Future accessions would also have budgetary implications, while unresolved disputes in candidate regions, including tensions between Serbia and Kosovo, continue to raise legitimate concerns.

Despite these challenges, the debate has changed considerably since 2022. Increasingly, the question is no longer whether candidate countries are ready for the EU, but whether the EU can afford the geopolitical consequences of leaving them outside. Seen from this perspective, enlargement is gradually becoming more than a policy of integration. In other words, **enlargement is no longer only about integration. It is also becoming a tool**

121 European External Action Service, Progress Report on the Implementation of the EU Strategy for Cooperation in the Indo-Pacific (Brussels: EEAS, 2024).

122 European Commission, The EU Strategy for Cooperation in the Indo-Pacific (Brussels: European Commission, 2021). https://www.eeas.europa.eu/sites/default/files/jointcommunication_2021_24_1_en.pdf

123 European External Action Service, EU-India Strategic Partnership: A Roadmap to 2025 (July 15, 2020), https://www.eeas.europa.eu/eeas/eu-india-strategic-partnership-roadmap-2025_en.

124 Ivan Krastev, intervention at the 25th Anniversary Conference of the Dutch Advisory Council on International Affairs, The Hague, 2023.

125 European Commission, 2024 Enlargement Package (Brussels: European Commission, October 30, 2024), https://enlargement.ec.europa.eu/news/commission-adopts-2024-enlargement-package-2024-10-30_en.

for strengthening Europe's security and shaping its geopolitical environment[126].

5.5 STRATEGIC ASSESSMENT

Current debates on strategic partnerships and the changing approach to enlargement reflect a broader transformation in the way the EU understands security. Recent crises have shown that military capabilities, while still important, are no longer enough on their own to guarantee stability and protect European interests[127]. Issues such as energy dependencies, technological vulnerabilities and disruptions to supply chains can have consequences that are just as significant, or sometimes even more significant, than many traditional security threats[128].

This helps explain why partnerships with regions such as Latin America and the Indo-Pacific, as well as the renewed interest in enlargement, have become increasingly important in the European agenda. Although these policies are different in nature, they all follow the same logic: **reducing vulnerabilities, increasing resilience and strengthening the EU's ability to act and manage crises in an increasingly competitive and uncertain international environment.**

In many ways, the main challenge facing the EU is no longer simply how to react to geopolitical changes, but how to define its own role within them. **The question is not only how Europe can protect its interests, but how it can do so autonomously without abandoning the values that have shaped the European project since its origins.**

126 Piotr Zerka, "Ukraine Means Enlargement Is Again the EU's Priority – But Not for the Reasons It Claims," Chatham House, February 19, 2024, https://www.chathamhouse.org/2024/02/ukraine-means-enlargement-again-eus-priority-not-reasons-it-claims.

127 Council of the European Union, A Strategic Compass for Security and Defence.

128 European Commission, European Economic Security Strategy.

Conclusion

If there is one idea this policy brief has tried to convey, **it is that Europe no longer gets to choose whether it acts geopolitically, only how.** The world that once allowed the EU to lead through rules and markets alone has given way to one shaped by war on its borders, great power rivalry, and dependencies it can no longer afford to ignore. OSA is the EU's answer to that shift: not a retreat from cooperation, but a way of protecting it.

What this analysis has offered is a map, not a destination. This brief has traced how the EU's relationships with USA, China and Russia are being redefined in real time, and why regions once seen as peripheral, Africa, Latin America, the Indo-Pacific, the Middle East, the Arctic, now sit at the centre of Europe's security calculations. Enlargement, too, has stopped being a technical process and become a geopolitical one, with Ukraine, Moldova and the Western Balkans woven into the EU's own security horizon.

None of this happens in a vacuum. The external posture described here is only as credible as the capabilities, institutions and resilience that sustain it, the very questions this Forum's other policy briefs go on to explore, from defence and economic security to technology, hybrid threats and human security. The role of this chapter, as one of the Forum's introductory contributions, has been to set the stage: to show why the EU's external action matters before the chapters that follow examine how it can be delivered.

Ultimately, the EU's credibility as a geopolitical actor will not be decided by any single instrument, but by whether it can align its external ambitions with the internal strength to back them. That is the thread connecting this brief to everything that follows.

EU External Action: Unveiling the Depths of Europe's Strategic Interests

Mapping the EU's strategic interests, great power relations and alliances in a changing security landscape

EU External Action

The EU's shift from an economic actor to a geopolitical one, shaped by Ukraine, great power rivalry and global instability



Open Strategic Autonomy

As open as possible, as autonomous as necessary — reducing critical dependencies in energy, technology and raw materials

Great Power Relations

Balancing cooperation and competition with the United States, China and Russia in an increasingly contested order

Africa & the Arctic

From migration and energy in Africa to emerging competition over resources and routes in the High North

Latin America & the Indo-Pacific

New strategic partnerships built on trade, connectivity and shared democratic values beyond Europe's traditional allies

Enlargement as Security

Ukraine, Moldova and the Western Balkans, assessed not only on accession criteria but as part of the EU's long-term stability strategy

Own Elaboration - Forum on the Future of the EU 2026

Glossary of abbreviations

ASEAN	Association of Southeast Asian Nations
CSDP	Common Security and Defence Policy
EEAS	European External Action Service
EU	European Union
GDP	Gross Domestic Product
GIUK	Greenland–Iceland–United Kingdom
IMEC	India–Middle East–Europe Economic Corridor
LAC	Latin America and the Caribbean
MENA	Middle East and North Africa
MFF	Multiannual Financial Framework
NATO	North Atlantic Treaty Organization
NSR	Northern Sea Route
OCTs	Overseas Countries and Territories
OSA	Open Strategic Autonomy
PESCO	Permanent Structured Cooperation
SA	Strategic Autonomy
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
USA	United States of America



EQUIPO EUROPA



NUCLEUS CHAPTER 1

DEFENCE AND MILITARY CAPABILITIES

TOWARDS STRATEGIC AUTONOMY: EU MILITARY CAPABILITIES AND DEFENCE INTEGRATION

Written with the contributions from the webinar featuring Félix Arteaga Martín.
Authors: Ángela Cordones Salas, Valeria Pérez López, Jaime Villamuera Bartolomé, Simón Conde Acevedo, Andreu Ahullana Judas and Álvaro Gálvez Lozoya.
Reviewers: María Villaverde Temes and Santiago Slullitel.

Forum on the Future of the EU

EUROPEAN SECURITY in a Changing World

EXECUTIVE SUMMARY

This policy brief examines how the European Union can transform its fragmented defence landscape into a coherent military capability framework capable of ensuring strategic autonomy while remaining complementary to NATO. It argues that although EU Member States have significantly increased defence spending following Russia's full-scale invasion of Ukraine, financial investment alone has not translated into an integrated, deployable, and resilient European defence capability. Instead, national procurement practices, duplicated weapons systems, limited interoperability, and uneven military capabilities continue to undermine collective effectiveness.

The topic is highly relevant for European security because the geopolitical environment has fundamentally changed. Russia's aggression against Ukraine, the rise of hybrid threats, cyber warfare, technological competition, and uncertainty regarding long-term transatlantic security require the EU to strengthen its ability to deter threats, sustain military operations, and protect critical infrastructure. A more integrated European defence also enhances NATO by addressing capability gaps and improving burden-sharing rather than duplicating Alliance structures.

The document identifies three interconnected challenges. First, **hardware gaps** include shortages in air and missile defence, ammunition, drones, strategic airlift, military mobility, and advanced capabilities such as AI, cyber, and space systems. Second, **institutional and governance challenges** stem from fragmented procurement, slow decision-making, restrictive fiscal frameworks, and insufficient incentives for collaborative defence investment, limiting the effectiveness of EU initiatives such as PESCO, the European Defence Fund, and joint procurement mechanisms. Third, **network and industrial challenges** arise from fragmented defence industries, dependence on non-EU suppliers, and the need to strengthen partnerships (particularly with Ukraine) while reducing strategic dependence on external actors.

The policy brief concludes that achieving strategic autonomy requires more than increased defence spending. The EU must coordinate capability development, streamline governance, strengthen its defence industrial base, promote joint procurement, improve interoperability, and deepen cooperation with NATO and strategic partners. Only by integrating military capabilities, institutions, and industrial policies can the EU build a credible, resilient, and operationally effective European defence framework capable of addressing future security challenges.

Keywords

Strategic Autonomy; European Defence Integration; Military Capabilities; Defence Industry; EU–NATO Cooperation; European security.

INTRODUCTION

One could argue that Europe's security landscape has changed more in the past four years than in the preceding three decades. Russia's full-scale invasion of Ukraine in February 2022 shattered the assumption that large-scale interstate war was no longer conceivable on European soil, forcing the EU to confront a question it had been delaying: **can a Union which was built primarily as an economic and regulatory project also become a credible security and defence actor?** European Commission President Ursula von der Leyen explicitly presented this shift at the 2026 Munich Security Conference, where she told delegates that **"Europe must become more independent. There is no other choice"**. Since 2022, EU Member States have responded with an unprecedented mobilisation of resources, soaring collective defence spending and the launching of ambitious initiatives such as the White Paper for European Defence, which are all aimed at translating financial commitment into military readiness.

Yet **spending more has not, by itself, made Europe safer or more capable.** Money has moved faster than the structures needed to spend it efficiently, and this brief examines why by tracing the problem from Member States' capabilities on the ground, through the institutions meant to coordinate them, to the industrial base behind them. Simultaneously, the brief also positions the EU's ambitions within its relationship to NATO, since it still is the cornerstone of collective defence for the large majority of its members, so that any move towards greater European capability is understood as reinforcing the Alliance rather than competing with it.

This brief is, hence, structured accordingly. Section 1 evaluates the current state of Member States' military capabilities, as well as identifying the operational and structural gaps that limit the EU's capacity for independent action. Section 2 examines the institutional architecture built to address these gaps; including PESCO, the CDP, CARD and the evolving EU-NATO relationship. Section 3 focuses on the industrial dimension, analysing why a fragmented European defence continues to constrain both competitiveness and sovereignty despite instruments such as SAFE, EDIP and EDIS. Finally, section 4 addresses the broader political question that comprises all of these debates: **is the logical endpoint of this process a "European Army"? What could the more realistic and intermediate scenarios look like?**

All of these sections encompass the brief's central argument. Closing Europe's capability gap cannot be achieved through a single reform, but must be done through an alignment of hardware investment, institutional design and external partnerships into one coherent strategy.

1 EU MEMBER STATES' MILITARY CAPABILITIES: EXISTING STRENGTHS AND CRITICAL GAPS

1.1 CURRENT MILITARY CAPABILITIES ACROSS EU MEMBER STATES

The contemporary landscape of European Union military capabilities presents a structural paradox defined by unprecedented financial mobilisation alongside deep-seated operational and systemic fragmentation. In the wake of the structurally altered European security paradigm following the 2022 invasion of Ukraine, aggregate defence expenditures across EU Member States have experienced a stark upward trajectory. According to data validated by the European Defence Agency[1], **collective EU defence spending reached a historic benchmark of €295 billion**, representing a continuous multi-year increase.

However, the strategic translation of these massive fiscal inputs into tangible, deployable, and combat-ready military output remains severely suboptimal[2]. The fundamental challenge confronting the EU's defence architecture is not merely quantitative, but qualitative, structural, and political. **The return on defence investment is systematically constrained by national protectionism in procurement, persistent duplication of weapon systems, and a historical lack of standardisation across the 27 national inventories**.

1.1.1 Asset Asymmetry and the Fragmentation Baseline

The structural baseline of current capabilities across the Union is characterised by profound geopolitical and operational asymmetry. A select tier of Member States retains conventional, high-end expeditionary and power-projection assets across all military domains (mechanised land forces, advanced blue-water naval surface combatants, and fourth-to-fifth-generation multi-role combat aircraft platforms). However, as noted by the Stockholm International Peace Research Institute[3]. These capabilities are predominantly configured around sovereign defence paradigms and national industrial preservation rather than a cohesive, unified European operational framework.

Conversely, a large cluster of Member States, particularly in Central and Eastern Europe, possesses highly specialised but small-scale forces. While these forces are increasingly modernised, they lack the critical mass and comprehensive logistical tail required for independent, sustained high-intensity combat operations.

This structural patchwork leads to an extraordinary proliferation of distinct platform types across the EU. The Coordinated Annual Review on Defence (CARD) has repeatedly warned that this lack of convergence prevents economies of scale, severely complicates cross-border joint training, and exponentially inflates life-cycle management and maintenance costs[4].

1.1.2 Institutional Architecture and the Roadmap to 2030

To bridge these gaps, **the European External Action Service (EEAS) emphasizes that modern military capability relies on a holistic ecosystem**: a combination of equipment, technology, trained personnel, logistical sustainability, and operational know-how. Under-investment has forced the EU to adopt a paradigm shift based on three pillars: invest more, invest together, and invest within Europe.

Through the Roadmap for Defence Readiness 2030 and the White Paper on European Defence, the EU has initiated structural frameworks to bypass unilateral capability building and establish collaborative procurement. **This institutional push is operationalised via two mechanisms**:

- **Capability Coalitions:** dynamic frameworks driven by Member States to pool financial and operational resources, identify joint priorities, and develop next-generation weapon systems in full alignment with NATO targets. Notably, these coalitions integrate battlefield insights and rapid innovation lessons directly from Ukrainian defence experiences.

1 European Defence Agency. *Coordinated Annual Review on Defence (CARD) Report*. Brussels: European Defence Agency, 2024. https://eda.europa.eu/docs/default-source/documents/card-report-2024.pdf.

2 Billon-Galland, Alice, and Erik Brattberg. Atlantic Council Defense Series: Navigating European Liability and Capability Gaps. Washington, DC: Atlantic Council, 2023. https://www.atlanticcouncil.org/content-series/atlantic-council-defense-series/navigating-european-liability-and-capability-gaps/.

3 Stockholm International Peace Research Institute. Trends in World Military Expenditure. Stockholm: SIPRI, 2025. https://www.sipri.org/sites/default/files/2026-04/2604_milex_2025.pdf.

4 European Defence Agency. Coordinated Annual Review on Defence (CARD) Report. Brussels: European Defence Agency, 2024. https://eda.europa.eu/docs/default-source/documents/card-report-2024.pdf.

- **European Readiness Flagships:** pan-European, mega-procurement projects designed to address urgent and non-negotiable strategic shortfalls collectively. These initial priorities include:
    - The European Air Shield: a multi-layered, fully integrated air and missile defence architecture interoperable with NATO C2 networks.
    - The European Space Shield: a comprehensive network of space capabilities to guarantee autonomous military communication, navigation, and satellite observation.
    - The European Drone Defence Initiative & Eastern Flank Watch: joint electronic warfare, counter-unmanned aerial vehicles (c-UAV), multi-domain surveillance, and precision strike systems explicitly positioned to secure the Union's eastern borders.

1.1.3 Existing Technological Strengths

On the upper end of the operational spectrum, the EU possesses world-class capabilities in specific technological and doctrinal domains:

- Aerospace Architecture: the continuous deployment and modernisation of advanced multi-role combat fleets constitute a critical pillar of European air power, providing robust air-defence, air-interdiction, and precision-strike capabilities aligned with NATO standards.
- Naval Warfare Systems: European shipyards continue to produce premier anti-submarine (ASW) and anti-air warfare (AAW) combatants, capable of securing sea lines of communication (SLOCs) and contributing to complex maritime security tasks globally.
- Mechanised Maneuver Warfare: certain European land forces maintain exceptional tactical proficiency in combined arms operations, anchored by robust armored and artillery assets.

Despite these localised strengths, the collective utility of these assets is severely undermined by the absence of a synchronised European command structure capable of seamlessly orchestrating these forces without extensive, ad-hoc political, legal, and technical reconciliation.

1.2 ASSESSMENT OF OPERATIONAL READINESS AND FORCE PROJECTION CAPACITY

An empirical assessment of the EU's operational readiness and force projection capacity reveals acute, systemic vulnerabilities when evaluated against the demanding requirements of high-intensity, peer-adversary conflict or protracted out-of-area crisis management. While European armed forces demonstrate high tactical competency in low-to-medium intensity, localised crisis-management deployments, their capacity to independently project power and sustain multi-domain operations at a strategic distance is severely compromised by long-standing, unaddressed capability gaps[5].

1.2.1 The Strategic Enabler Deficit

Force projection is fundamentally limited by a severe deficit in European-owned and operated strategic enablers. When evaluating the force generation requirements for EU battle groups or the broader goals of the EU Strategic Compass, Member States suffer from a critical shortfall in three foundational areas:

- **Strategic Airlift and Sealift:** the collective European inventory lacks sufficient heavy-payload, long-range transport assets required to rapidly deploy heavy mechanised brigades beyond immediate territorial borders without relying on commercial charters or allied assets.
- **Airborne Refueling (AAR):** the scarcity of dedicated, organic tanker fleets drastically limits the combat radius and persistence of European air assets, rendering sustained air campaigns heavily dependent on non-EU allied intervention.
- **Autonomous C4ISR Architecture:** while tactical intelligence is highly developed, space-based early warning systems, high-altitude long-endurance (HALE) unmanned aerial systems, and integrated cyber-intelligence platforms remain fragmented and quantitatively insufficient to provide comprehensive, independent situational awareness[6].

Without these force multipliers, the EU's ambition for "open strategic autonomy" remains an aspirational geopolitical concept rather than an operational reality.

5 Fiott, Daniel. "Strategic Autonomy and the EU's Capability Paradox." European Foreign Affairs Review 28, no. 2 (2023): 145–62. https://kluwerlawonline.com/JournalArticle/European+Foreign+Affairs+Review/28.2/EERR2023013.

6 Grand, Camille. The European Defense Calculus: Balancing C4ISR and Mass. Paris: Institut Montaigne, 2024. https://www.institutmontaigne.org/en/expressions/european-defense-calculus-balancing-c4isr-and-mass.

1.2.2 Logistics, Sustainment, and Material Services

Beyond initial deployment capacity, the core vulnerability of European military capabilities lies in operational sustainability and force readiness over time. Decades of post-Cold War defence divestment, underfunded readiness accounts, and reliance on "just-in-time" logistics have resulted in **critically depleted ammunition stockpiles, severe shortages of spare parts, and a fragile defence industrial base incapable of rapid surge production**[7].

The operational readiness of critical air and land platforms is frequently degraded by supply chain bottlenecks and a lack of cross-border logistical interchangeability among international partner fleets. In multinational programs, the inability to seamlessly pool and share material services, combined with distinct national maintenance protocols, creates friction that limits fleet availability and creates artificial bottlenecks during joint deployments. Furthermore, interoperability is hindered by the non-standardisation of secure communication systems, meaning that **units from different Member States often cannot exchange real-time tactical data on the battlefield.**

To transition from a fragmented defence posture into a credible force projection actor, the EU must aggressively leverage mechanisms like the Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF). As outlined in the European Defence Industrial Strategy (EDIS), future initiatives must focus on harmonizing readiness metrics, establishing joint logistical hubs, ensuring the absolute interchangeability of ammunition, and aligning multinational procurement programs directly with the operational blueprints of both the EU Strategic Compass and NATO's New Force Model[8].

1.3 IDENTIFICATION OF KEY CAPABILITY GAPS AND STRATEGIC SHORTFALLS

Europe's defence landscape has major gaps in three key areas which are mutually reinforced. The EU lacks the physical tools to fight and the strategic infrastructure to move and sustain forces across the continent (**hardware**). It lacks the institutional agility to act, since procurement rules, funding procedures and fiscal frameworks were all designed for peacetime and remain too slow, fragmented and nationally-dependent to respond to an active threat (**software**). Finally, it lacks the network of formal commitments needed to turn bilateral agreements into collective capabilities (network). Hardware without software produces armies that cannot be deployed. Software without hardware creates empty procedures. Both without a robust network of partnerships produce a Europe that is capable on paper and isolated in practice. Hence, transforming the EU's fragmented defence landscape into a coherent military capability framework requires addressing all three simultaneously as a single integrated effort.

1.3.1 Hardware

There are seven critical capability gaps[9] which can be understood from two distinct perspectives:

- The first four reflect the lessons drawn from Russia's 2022 full-scale invasion of Ukraine. Observed across four years of high-intensity conventional warfare, these gaps are operational and immediate[10]:

    1. **Air and missile defence:** to counter growing threats from hypersonic and ballistic missiles.
    2. **Artillery systems:** to enable sustained deep precision strike capabilities.
    3. **Ammunition and missiles:** to address critically drained stockpiles exposed by the tempo of modern warfare.
    4. **Drones and anti-drone systems:** to respond to the decisive role of unmanned systems on the contemporary battlefield.

- The latter three are **structural gaps**, which show that there are deficiencies in the foundational architecture that would allow the EU to project and sustain military force at the scale it is currently required[11]:

    1. **Military mobility:** the ability to move troops and materiel rapidly across the continent
    2. **AI, quantum, cyber and electronic warfare:** maintaining technological competitiveness in the next generation of conflict
    3. **Strategic enablers and critical infrastructure protection:** including strategic airlift,

7 European Commission. European Defence Industrial Strategy (EDIS). COM(2024) 150 final. Brussels: European Union, March 5, 2024. https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-our-common-defence-industrial-strategy_en.

8 European Parliament Research Service. EU-NATO *Cooperation: State of Play and Future Prospects. Brussels: European Parliament, 2024.*

9 European Commission, "White Paper for European Defence – Readiness 2030," March 2025. https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en.

10 European Commission, "White Paper for European Defence," 2025.

11 European Commission, "White Paper for European Defence," 2025.

air-to-air refuelling, maritime domain awareness and protection of space assets

Nonetheless, addressing these structural shortfalls requires a commitment level from Member States that is yet to be achieved. This could be contemplated through four conditions:

1. **A common understanding among Member States on shared investment priorities without outsourcing towards national priorities.**
2. **A stable and long-term commitment, moving beyond the current crisis-driven spending towards a durable and predictable defence investment[12].**
3. **A clear governance framework for each capability area, recognising that the appropriate institutional arrangement may differ between domains.**
4. **EU funding and incentives designed for continuity rather than crisis management, where the instruments outlast political cycles.**

These conditions have already been suggested in multiple reports[13], but the EU has historically struggled to meet all four at once. Closing the structural gaps identified above requires more than increased defence expenditure, as there should be a coherent institutional logic that links all countries to a collective outcome. In order for this to be achieved, there are three key proposals which are interdependent:

1. **Establishing a common understanding through a structured priority-setting process.**
2. **Redesigning EU funding as a structural and conditional instrument.**
3. **Anchoring long-term commitment through the funding conditionality itself.**

Firstly, rather than relying on unanimity (which has historically paralysed EU defence ambitions), Member States should **agree on a defined set of tangible capability targets through a lead nation model,** whereby coalitions of willing states drive progress in each priority area. This preserves

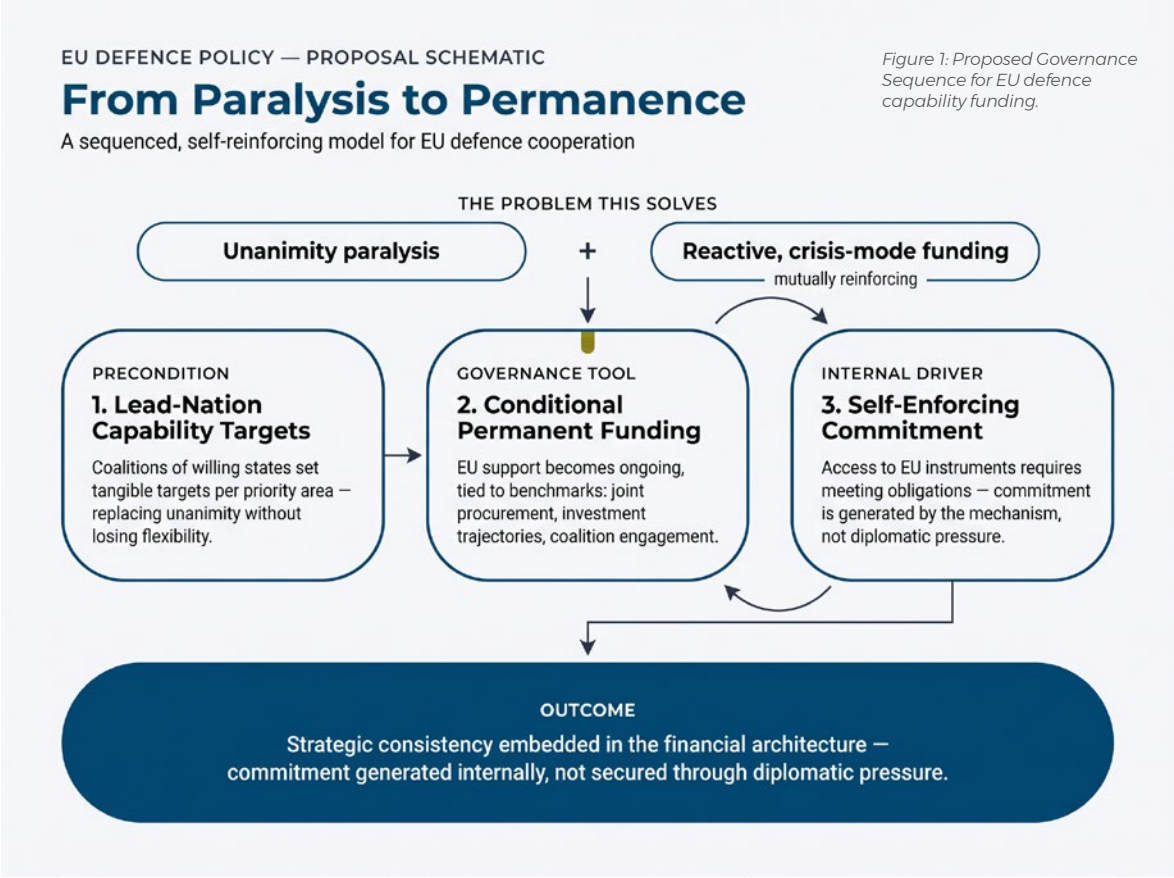


Figure 1: Proposed Governance Sequence for EU defence capability funding.

12 One mechanism to reinforce this could be making EU funding conditional on sustained national contributions, rather than rewarding one-off responses to specific threats.

13 European Commission, "White Paper for European Defence," 2025.

flexibility while avoiding veto problems related to consensus-based governance. This is the necessary precondition for the two mechanisms that follow.

Secondly, **current EU defence funding has operated largely in crisis mode**, characterised by being reactive and time-limited designed to patch immediate shortfalls instead of building lasting capacity. The proposal here is a permanent funding mechanism in which EU financial support is explicitly conditional on Member States meeting agreed contribution benchmarks: participation in joint procurement, sustained national investment trajectory or active engagement in capability coalitions. **This transforms funding from a subsidy into a governance tool.**

Finally, as an alternative to treating political commitment as a separate requirement to be secured through diplomatic pressure, the conditional funding mechanism generates commitment internally. In order for Member States to access EU instruments (such as financing), they must maintain their obligations and commitments. **This removes reliance on goodwill alone and embeds strategic consistency into the financial architecture.**

1.3.2 Software

Regarding the rules and procedure of the European Defence Strategy, these must be sped up. Rapid times require a decisive and simplified process that can easily respond to an enemy threat. The war in Ukraine has made this clear, essentially since EU Member States had ammunition stocks sufficient to resist a massive aggression for only a few days at most[14], and when the EU finally mobilised, the gap between political commitment and industrial reality was appalling. **The existing framework was designed for peacetime, and it performs accordingly.** What is needed, therefore, is a fundamental evaluation of the procedural architecture that governs how that spending is mobilised, approved and deployed.

This could take the form of a 'Defence Omnibus', which would simplify and speed up the procedure for the European Defence Funds Capabilities. This was **already proposed by the European Commission in 2025**, through a package of measures to simplify the legal and administrative framework in the defence sector, including an amendment to the EU Defence Procurement Directive that would simplify procedures, reduce administrative burdens and give Member States more flexibility[15]. Through the National Escape Clause, this framework could further allow Member States to temporarily deviate from the Stability and Growth Pact which, when activated, would enable flexibility regarding the fiscal rules. Still, this is only available for four years from 2025, and the annual excess must not exceed 1.5% of the country's GDP[16], giving Member States enough margin to innovate in their defence industry. Nevertheless, this approach raises two key problems:

- Firstly, if every Member State uses the National Escape Clause unilaterally, this will not necessarily create further cooperation among them, hence risking the creation of redundant, inefficient companies in the European market that are unable to compete at global scale.
    - Evidence already points in this direction, as collaborative defence procurement remains under 20%[17], despite defence expenditure having increased since 2020 by 62.87%[18].
    - The majority of defence acquisition by EU Member States still originates from non-EU suppliers, with 63% sourced from the US alone[19], demonstrating that more national spending does not automatically translate into a stronger European industrial base.
    - The solution must tie NEC activation to collective action, thus access to EU co-funding instruments such as SAFE loans and EDIP grants should be conditional on a minimum share of that additional spending being directed through joint procurement mechanisms, ensuring that fiscal flexibility at the national level becomes the entry point to integration rather than an alternative to it.

14 Besancenot, Damien, and Radu Vranceanu. "Explaining the Ammunition Shortage: The Show vs. Have Military Power Game." Defence and Peace Economics, February 5, 2025. https://www.tandfonline.com/doi/full/10.1080/10242694.2025.2460447.

15 Clapp, Sebastian. "Simplifying Intra-EU Transfers and Security and Defence Procurement." European Parliament Legislative Train, February 20, 2026. https://www.europarl.europa.eu/legislative-train/carriage/simplifying-intra-eu-transfers-and-security-and-defence-procurement/report?sid=10001.

16 Council of the European Union, "National Escape Clause for Defence Expenditure," last modified 2026, https://www.consilium.europa.eu/en/policies/national-escape-clause-for-defence-expenditure-nec/.

17 Tothova and Clapp, "EU Joint Defence Procurement," PE 785.665, March 2026. https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/785665/EPRS_BRI(2026)785665_EN.pdf.

18 Council of the European Union, "EU Defence in Numbers," last modified January 7, 2026, https://www.consilium.europa.eu/en/policies/defence-numbers/.

19 Satta, Marianna. "Industrial Attrition: Europe's Defence Procurement Paradox." Atlas Institute for International Affairs, February 21, 2026. https://atlasinstitute.org/industrial-attrition-europes-defence-procurement-paradox/.

- Secondly, the competition policy dimension, particularly in domains such as AI and electronic warfare, presents a distinct structural problem. The European defence technology market is currently populated by a large number of micro-companies attempting to fill a vast capability gap, producing a fragmented landscape in which no single actor achieves the economies of scale necessary for sustained R&D investment or competitive output.

    - A layered industrial architecture, in which EU-level prime contractors are nominated for strategic platform categories, while SMEs compete within supply chains below them, would preserve competition where it adds value while enabling the consolidation that this industry demands.

1.3.3 Networks

For this machinery to function, the EU cannot confront its strategic challenges alone. As the world's largest trading bloc[20], the EU has the weight to build and formalise a stronger alliance network. As of June 2026, it holds twelve: Moldova, Norway, South Korea, Japan, Albania, North Macedonia, the UK, Canada, India, Iceland, Australia and Ghana[21].

Yet the most strategically significant partner out of all still lacks a concrete Security and Defence Partnership - Ukraine. The EU and Ukraine signed Joint Security Commitments on June 2024, which offered the invaded country the chance to participate on equal terms in SAFE common procurement[22]; followed in December 2025 by an EDF association and a dedicated €300 million Ukraine Support Instrument under the European Defence Industry Programme[23]. However, the alliance is missing coherence that would naturally follow from a single legal architecture, instead of the current separate Council decisions. The EU should consolidate them into a Comprehensive EU-Ukraine Security and Defence Partnership, built on the existing Association Agreement, that locks in institutional durability ahead of accession.

This recommendation gains urgency from a recent shift in the EU's internal politics. Since the change of government in Hungary following the April 2026 election removed the single biggest veto risk to deeper EU-Ukraine integration, with Budapest lifting both its EPF reimbursement block and its veto on Ukraine's accession talks in June 2026[24], the EU should use this window to consolidate Ukraine's status while political consensus holds. Otherwise, it risks the same patchwork persisting until the next point of friction reopens it.

2 EU MILITARY INTEGRATION AND COOPERATION: FRAMEWORK OF DEFENCE COOPERATION WITHIN THE EUROPEAN UNION.

2.1 DEFENCE COOPERATION AMONG EU MEMBER STATES

2.1.1 Mechanisms for coordination and joint capability development

In the last decades, European defence cooperation has gradually evolved through a series of mechanisms designed to improve coordination among Member States and promote joint capability development. Rather than relying on a single defence-planning framework, the EU has developed instruments that seek to align national priorities, identify capability gaps, and encourage collaborative investment in military assets.

At the centre of this architecture is the Capability Development Plan (CDP), managed by the European Defence Agency (EDA)[25]. Since 2008, the CDP has provided a long-term assessment of Europe's security environment and identified priority capability areas across the five defence domains: land, air, maritime, space and cyber. By identifying common requirements and future challenges, it serves as a reference point for national defence

20 European Commission, Directorate-General for Trade, The EU's Position in World Trade: Economic Indicators and Global Relations (Brussels: European Commission, 2025), https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/eu-position-world-trade_en.

21 European External Action Service, "EU Security and Defence Partnerships," last modified March 24, 2026, https://www.eeas.europa.eu/eeas/eu-security-and-defence-partnerships_en.

22 Council of the European Union, "EU-Ukraine Security Commitments," June 27, 2024, https://www.consilium.europa.eu/media/oredhmis/eu-ukraine-security-commitments-en.pdf.

23 Council of the European Union, "European Defence Industry Programme (EDIP)," last modified December 8, 2025, https://www.consilium.europa.eu/en/policies/defence-industry-programme/.

24 Barigazzi, Jacopo. "Hungary Lifts Veto on Reimbursements for EU Military Aid to Ukraine." Politico Europe, June 1, 2026. https://www.politico.eu/article/hungary-lifts-veto-on-reimbursements-for-eu-military-aid-to-ukraine/.

25 The European Defence Agency (EDA) is an agency of the European Union (EU) that promotes and facilitates integration between member states within the EU's Common Security and Defence Policy (CSDP). It is one of the three Common Foreign and Security Policy (CFSP) agencies under the leadership of the Council, together with the EUISS (European Union Institute for Security Studies), and SatCen (European Union Satellite Centre).

planners and facilitates multinational cooperation. Complementing this process is the Coordinated Annual Review on Defence (CARD), launched in 2017. CARD evaluates Member States' defence plans, missing capabilities, and areas where collaborative projects could generate greater efficiency and reduce duplication. Its findings have repeatedly stressed that rising defence budgets create an opportunity to address long-standing capability gaps through joint action rather than fragmented national spending[26].

The most visible mechanism for capability development is Permanent Structured Cooperation (PESCO[27]), established in 2017. PESCO enables EU Member States to carry out collaborative projects with a set of legally binding obligations, including closer coordination of defence planning and efforts to improve interoperability. Since its creation, dozens of projects have been launched in areas such as cyber defence, maritime security, military mobility and space capabilities. Although PESCO has significantly expanded the institutional framework for cooperation, its practical impact has been mixed. Many projects remain limited in scope and continue to support primarily national forces rather than creating genuinely integrated European capabilities[28]. PESCO supports cooperation across domains including land, air, maritime, cyber and space. Several projects focus directly on pooling expertise and resources, ranging from a European Medical Command and Cyber Rapid Response Teams to military disaster relief capabilities, maritime surveillance networks and specialised helicopter training[29].

The challenge of translating coordination mechanisms into concrete military capabilities reflects a broader structural issue within European defence cooperation. Despite repeated initiatives since the late 1990s, defence planning remains largely centred on national decision-making, with Member States often reluctant to give up control over defence priorities. This has complicated efforts to achieve longstanding EU objectives, such as developing rapidly deployable multinational forces and reducing dependence on external support for strategic enablers, including airlift, satellite communications and advanced reconnaissance systems[30].

Recent EU initiatives have therefore placed increasing emphasis on joint capability development and procurement. The Strategic Compass, adopted in 2022, called for a more coherent approach to capability planning, greater coordination among defence ministers, and strategic enablers and next-generation military systems. In parallel, the European Defence Fund (EDF) has provided financial incentives for collaborative research, innovation and capability development projects involving multiple Member States. More recently, initiatives such as the European Defence Industry Reinforcement through Common Procurement Act (EDIRPA) and the proposed move towards more coordinated defence programming seek to encourage Member States to acquire capabilities collectively rather than through separate national procurement processes[31].

The concept of pooling resources is not new in European defence, but it has gained renewed importance as governments seek to preserve military capabilities despite financial constraints. Pooling and sharing arrangements allow countries to combine assets, infrastructure or services that would otherwise be maintained separately. Examples include multinational air transport arrangements, shared surveillance capabilities and joint procurement programmes. Such cooperation enables Member States to acquire capabilities collectively, achieve economies of scale and reduce the burden of maintaining expensive military assets independently. The logic is particularly relevant for high-cost capabilities such as strategic transport, air-to-air refuelling and logistical support, which many countries would struggle to sustain on their own[32].

Military mobility has also emerged as an important area of multinational cooperation. The EU's Military Mobility Package seeks to improve transport infrastructure, simplify cross-border procedures and facilitate the movement of troops and military equipment across Europe. Better coordination of roads, railways, ports and airports reduces logistical bottlenecks and enables Member States to deploy forces more rapidly when needed. By improving connectivity and interoperability, military mobility strengthens the practical foundations of multina-

26 Sebastian Clapp, European Capability Development Planning (Brussels: European Parliamentary Research Service, European Parliament, March 2024), accessed June 14, 2026, https://epthinktank.eu/2024/03/06/european-capability-development-planning

27 The abbreviated form PESCO will be used from now on.

28 Egmont Institute, "The Coordination Problem in European Defence Planning," September 27, 2021, accessed June 14, 2026, https://egmontinstitute.be/the-coordination-problem-in-european-defence-planning

29 European External Action Service, "Other EU Defence Initiatives and Programmes," European External Action Service, accessed June 14, 2026, https://www.eeas.europa.eu/eeas/other-eu-defence-initiatives-and-programmes_en

30 Clapp, European Capability Development Planning.

31 Clapp, European Capability Development Planning.

32 The European Defence Pooling & Sharing: From Words to Deeds," C4 – Sub-Theme 2, Rome Conference Report, 2013, accessed June 14, 2026, https://www.statewatch.org/media/documents/news/2015/jan/med-2013-c4-rome-conference-report-2-european-defence-pooling.pdf

tional defence cooperation while also enhancing coordination with NATO and other partners[33].

The growing focus on coordination and joint capability development has also been reinforced by the EU's broader defence agenda. The White Paper for European Defence – Readiness 2030 and the associated ReArm Europe/Readiness 2030 initiative emphasise the need for Member States to invest together, procure equipment jointly and strengthen Europe's ability to deploy forces rapidly across the continent. While these initiatives are strongly linked to defence industrial policy and financing, they also support the objective of improving collective capability development by encouraging more coordinated investment decisions and reducing fragmentation in European defence spending[34].

Overall, the EU has established an increasingly sophisticated framework for defence coordination through instruments such as the CDP, CARD, PESCO and the EDF. These mechanisms have improved transparency, identified common priorities and created new opportunities for cooperation. However, their effectiveness continues to depend on Member States' willingness to align national planning processes and translate political commitments into jointly developed and procured military capabilities[35].

Past experience has shown that while Member States are generally willing to cooperate at the tactical and technical levels, deeper forms of integration remain more difficult to achieve. Differences in national priorities, strategic cultures and defence planning traditions can slow progress and limit the scope of cooperation. Nevertheless, as security challenges become increasingly transnational, multinational initiatives and pooled resources are likely to remain central components of European defence cooperation.

2.1.2 European Missions and Operations

Under the framework of the Common Security and Defence Policy (CSDP), European missions and operations represent one of the most visible instruments of defence cooperation among EU Member States. Through these missions, the European Union contributes collectively to international peace, security, and crisis management by deploying both civilian and military personnel in regions affected by instability and conflict. Since the launch of the first CSDP missions in 2003, the EU has conducted more than forty overseas missions and operations across Africa, the Western Balkans, Eastern Europe, and the Middle East**. These actions are designed not only to support partner countries but also to strengthen the security of the European Union itself by addressing threats before they reach EU borders**[36].

EU missions and operations are an essential component of the EU's Common Foreign and Security Policy (CFSP) and reflect the Union's broader objective of promoting peace, stability, and development. In response to an increasingly volatile geopolitical environment, particularly along its eastern and southern neighbourhoods, the EU has expanded its operational engagement abroad. As of 2026, the EU conducts 22 ongoing CSDP missions and operations worldwide, including 13 civilian missions and 9 military missions and operations, reflecting the Union's integrated approach to crisis management and international security[37].

The operational tasks of EU military missions vary according to the needs of the host country and the nature of the crisis. Military missions are primarily focused on training and reforming armed forces, assisting in the creation of safe and secure environments, combating piracy, and disrupting trafficking networks. Examples include the EU Military Assistance Mission in Ukraine (EUMAM Ukraine), which strengthens the capabilities of the Ukrainian Armed Forces through training programmes, and Operation Atalanta, which combats piracy and protects maritime routes in the Horn of Africa. Executive military operations, such as EUFOR Althea in Bosnia and Herzegovina, may also contribute directly to maintaining security and stability under international mandates. Alongside military activities, civilian missions constitute a major pillar of EU external action. These missions focus on areas such as border management, conflict prevention, combating organised crime, judicial reform, and strengthening the rule of law[38].

The effectiveness of these missions depends on a complex command and coordination structure. Military training missions are directed through the Military Planning and Conduct Capability (MPCC), which serves as the EU's central military headquar-

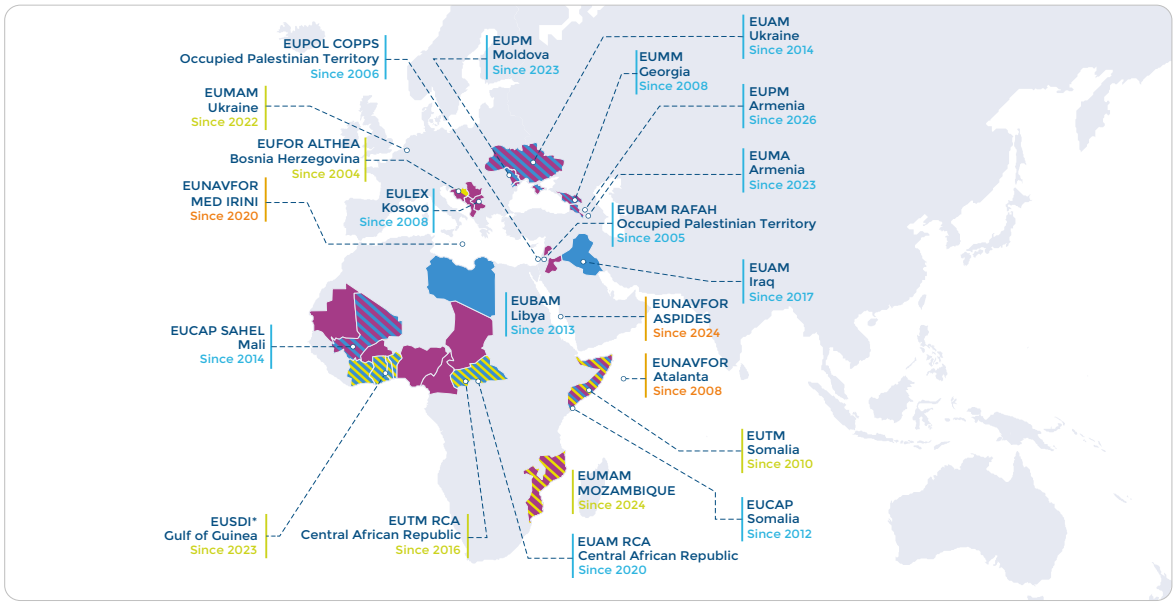
33 EEAS, "Other EU Defence Initiatives and Programmes."
34 European Commission, "Future of European Defence," European Commission, accessed June 14, 2026, https://commission.europa.eu/topics/defence/future-european-defence_en
35 Egmont Institute, "The Coordination Problem in European Defence Planning."
36 European External Action Service (EEAS). "Missions and Operations." Accessed February 2025. https://www.eeas.europa.eu/eeas/missions-and-operations_en
37 EEAS, "Missions and Operations."
38 EEAS, "Missions and Operations."

ters in Brussels. Financial support for military-related activities is facilitated through the European Peace Facility (EPF), which allows the EU to fund operations and assistance measures with defence implications despite treaty restrictions on using the EU budget for military expenditure. This institutional framework enables Member States to conduct joint operations while sharing costs, expertise, and responsibilities[39].

A key actor supporting the planning and execution of these missions is the European Union Military Staff (EUMS), which functions as the primary source of military expertise within the European External Action Service (EEAS). The EUMS provides early warning, intelligence assessments, strategic planning, logistics coordination, communications support, and operational monitoring. Through its specialised directorates, the EUMS contributes to crisis response planning, capability development, and cooperation with international partners. It also works closely with the EU Military Committee and civilian actors to ensure coordination between military and civilian dimensions of CSDP missions. In this way, the EUMS strengthens the EU's ability to conduct integrated crisis management operations and reinforces the military component of European external action[40].

Overall, European missions and operations demonstrate how defence cooperation among EU Member States has evolved beyond simple political coordination and joint capability development into practical and operational collaboration. By combining military and civilian instruments, common command structures, and shared funding mechanisms, the EU has developed a unique model of crisis management that supports both international stability and European security interests. These missions therefore represent a concrete expression of EU military integration and a key mechanism through which Member States act collectively in addressing contemporary security challenges. However, despite these advances, **EU missions and operations remain dependent on the political will and military contributions of individual Member States,** meaning that they fall short of constituting a fully integrated European army as envisioned by some advocates of deeper defence integration. *Figure 1*

EU SECURITY AND DEFENCE ENGAGEMENT AROUND THE WORLD



5 Ongoing military missions/operations

13 Ongoing civilian missions

3 Ongoing military naval operations/EUNAVFOR

1 Civilian & military initiative

Integrated Approach

EU security and defence actions are deployed and implemented in concert with other EU tools and instruments to achieve strategic impact.

Objectives

Peace-keeping, conflict prevention, strengthening international security, supporting the rule of law, prevention of human trafficking and piracy, contributing to maritime security, providing military equipment and security infrastructure to EU partners.

- Military missions/operations
- Civilian missions
- European Peace Facility assistance measures
- Military naval operations/EUNAVFOR

39 European Parliamentary Research Service, EU Missions and Operations Abroad.

40 European External Action Service (EEAS), "EU Military Staff," https://www.eeas.europa.eu/eums_en

2.1.3 Intelligence cooperation and information sharing

While joint capability development and CSDP missions represent the most visible dimensions of defence cooperation within the European Union, **effective military integration also depends on the ability of Member States to exchange information, assess threats collectively, and coordinate responses to emerging security challenges**. Intelligence cooperation and information sharing therefore constitute an important component of the EU's overall framework of defence cooperation.

The European intelligence landscape remains relatively underdeveloped at the supranational level. While each of the 27 European Union member states maintains its own national intelligence services, cooperation among them is generally limited and lacks comprehensive formalised mechanisms for intelligence sharing.

Over the course of European integration, several EU bodies have acquired functions related to intelligence production and analysis. Notable examples include:

- Europol,
- The European Border and Coast Guard Agency (Frontex),
- The European Union Satellite Centre (SatCen),
- The European Maritime Safety Agency (EMSA),
- Specialised units within the European External Action Service (EEAS), such as:
    - The Intelligence Directorate of the EU Military Staff (EUMS INT) and
    - The European Union Intelligence and Situation Centre (EU INTCEN)

Despite their analytical roles, **these organisations largely depend on open-source information and data provided by member states**. Unlike national intelligence services, they generally do not possess independent collection capabilities such as human intelligence networks, covert operations, or communications interception[41]. An important exception is SatCen, which is often regarded as the only EU-level body with a significant capacity to generate intelligence products from information obtained directly by the Centre. Its sources include imagery from European satellite systems such as Copernicus, as well as commercially acquired satellite data from European and U.S. providers.

A clearer understanding of the EU intelligence framework requires distinguishing the roles of its principal bodies. EUMS INT is responsible for producing early-warning intelligence and situational assessments in support of EU civilian missions and military operations. EU INTCEN, meanwhile, provides strategic situational awareness and early warning by monitoring global risks and security developments for the High Representative of the Union for Foreign Affairs and Security Policy. The analytical outputs of these entities, together with contributions from SatCen and other sources, are integrated through the Single Intelligence Analysis Capacity (SIAC), which serves as the EU's primary mechanism for coordinated intelligence assessment.

Although Europe possesses its own space infrastructure and geospatial intelligence (GEOINT) capabilities, significant reliance on external partners (particularly the United States) continues to shape the EU's approach to the space domain. As a result, European institutions have increasingly emphasised the need to strengthen strategic autonomy by expanding investment in the continent's space industrial base in order to avoid over-reliance on external capabilities. These dependencies create potential vulnerabilities, for instance, during international crises, as geopolitical tensions or military conflicts —such as the 2026 war in Iran— may lead to interruptions in the supply of satellite imagery and related data from American commercial providers to European agencies such as SatCen[42].

Continued reliance on U.S. based space service providers raises questions regarding the EU's long-term strategic autonomy. **Dependence on external actors may limit Europe's ability to guarantee secure and independent access to space**, particularly amid growing uncertainty surrounding the future trajectory of transatlantic security cooperation.

Current efforts focus on two main areas. First, the European Union seeks to coordinate funding across multiple initiatives. The EU Space Programme, supported by a budget of approximately €13 billion, is designed to complement defence-related instruments such as the European Defence Fund, as well as research programmes including Horizon Europe. This approach aims to create stronger links between scientific research, technological development, and operational deployment. Second, policymakers are prioritizing technological sovereignty. Measures are being implemented to reduce dependence on non-EU suppliers and to secure access to critical components, materials,

41 Gruszczak, Artur. Intelligence Security in the European Union: Building a Strategic Intelligence Community. Cham: Palgrave Macmillan, 2016.

42 New Economy Forum, "NEF Online with Mr. Louis Tillier, Director of the EU Satellite Centre (SatCen)," YouTube livestream, April 15, 2026, https://www.youtube.com/watch?v=j6F1VBuLMOg

and technologies required for the development and maintenance of European space systems[43].

Recent discussions on strengthening the EU's intelligence architecture illustrate both the growing importance of intelligence cooperation and its limitations. As part of the development of a new European Security Strategy, proposals have emerged to expand the role of the EU Intelligence and Situation Centre (INTCEN), the body responsible for

43 Council of the European Union, "Space, Security and Defence," accessed May 31, 2026

EU MEMBER STATES-MAIN INTELLIGENCE SERVICES

Civil / Domestic and foreign civil intelligence

Military intelligence

CZECHIA CZ
- Civil: Security Information Service (BIS)
  Office for Foreign Relations and Information (ÚZSI)
- Military: Military Intelligence (VZ)

DENMARK DK
- Civil: Security and Intelligence Service (PET)
- Military: Defence Intelligence Service (FE)

GERMANY DE
- Civil: Federal Office for the Protection of the Constitution (BfV)
  Federal Intelligence Service (BND)
- Military: Federal Office for the Military Counter-Intelligence Service (MAD)

NETHERLANDS NL
- Civil: General Intelligence and Security Service (AIVD)
- Military: Military Intelligence and Security Service (MIVD)

IRELAND IE
- Civil: Garda Crime and Security Branch (CSB)
- Military: Defence Forces Directorate of Intelligence (G2)

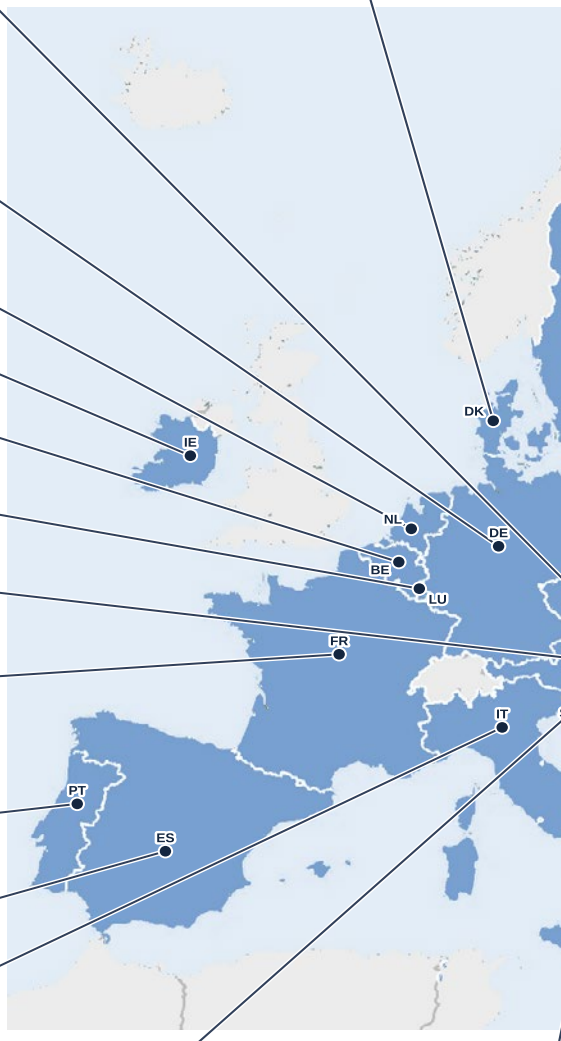
BELGIUM BE
- Civil: State Security Service (VSSE)
- Military: General Intelligence and Security Service of the Armed Forces (ADIV/SGRS)

LUXEMBOURG LU
- Civil: State Intelligence Service (SRE)
- Military: —

AUSTRIA AT
- Civil: Directorate for State Protection and Intelligence (DSN)
- Military: Military Intelligence Service (HNaA)
  Military Defence Agency (AbwA)

FRANCE FR
- Civil: General Directorate for Internal Security (DGSI)
  General Directorate for External Security (DGSE)
- Military: Directorate of Military Intelligence (DRM)
  Directorate of Defence Intelligence and Security (DRSD)

PORTUGAL PT
- Civil: Security Intelligence Service (SIS)
  Strategic Defence Intelligence Service (SIED)
- Military: Military Intelligence and Security Centre (CISMIL)



SPAIN ES
- Civil: National Intelligence Centre (CNI)
  Intelligence Centre against Terrorism and Organised Crime (CITCO)
- Military: Armed Forces Intelligence Centre (CIFAS)

ITALY IT
- Civil: Information and Internal Security Agency (AISI)
  Information and External Security Agency (AISE)
- Military: Information and Security Department (RIS)

SLOVENIA SI
- Civil: Slovene Intelligence and Security Agency (SOVA)
- Military: Intelligence and Security Service of the Ministry of Defence (OVS)

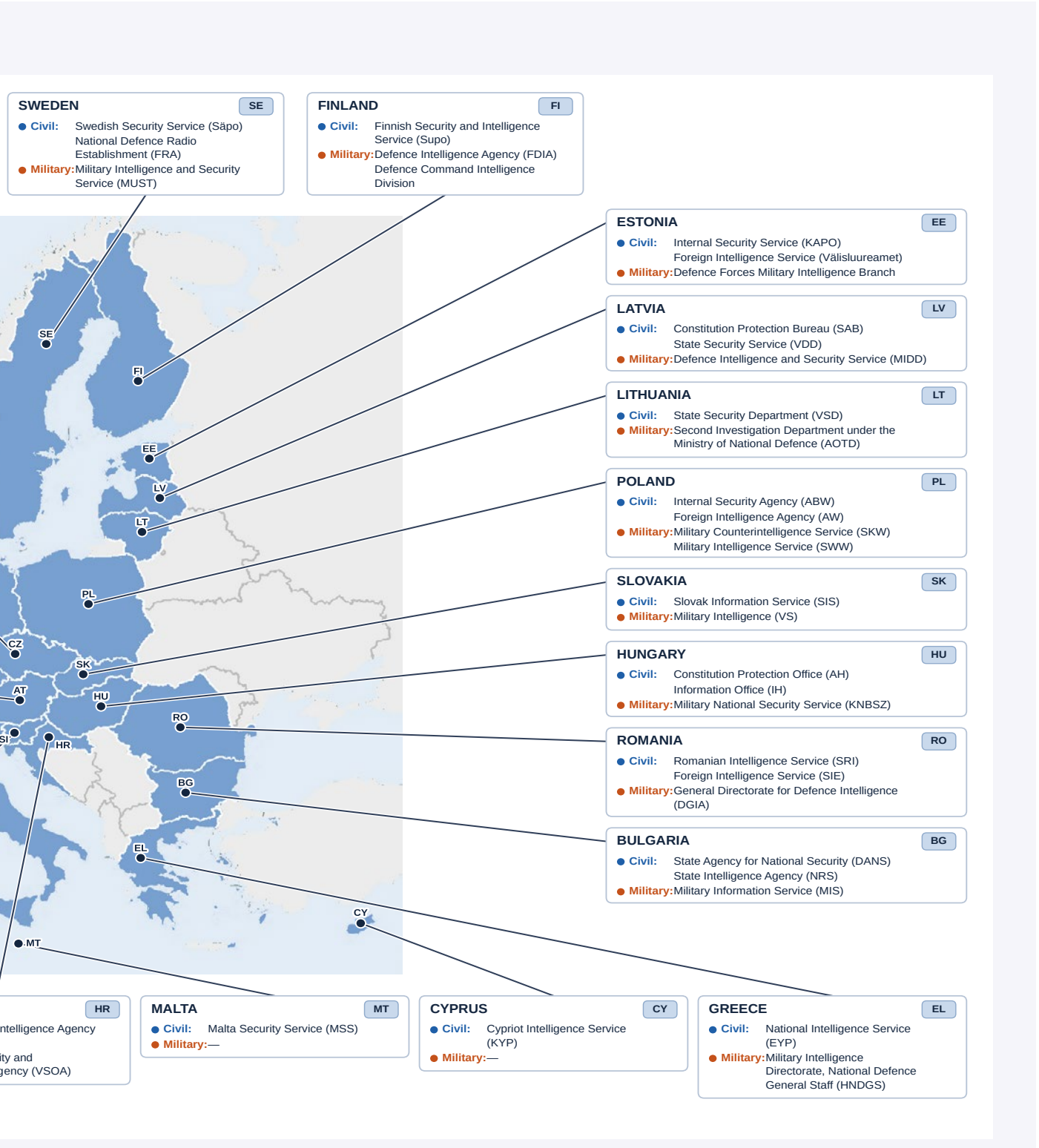
CROATIA
- Civil: Security and I (SOA)
- Military: Military Securi Intelligence Ag

Note: Main national intelligence organisations of each Member State. Abbreviations follow the official acronyms in the original language; service names are English translations. — = no separate service identified in the sources co

Source: Own elaboration based on FRA (2023), Surveillance by intelligence services, Annex 1, and the official sources of each service.

Note: Services listed reflect primary national intelligence organizations as of 2018. Abbreviations correspond to English translations of official names.
Source: Open sources and official government information.

analysing intelligence voluntarily shared by Member States and providing assessments to EU decision-makers. However, debates surrounding these proposals have once again highlighted the reluctance of national intelligence services to transfer sensitive information to supranational structures. Officials from several Member States have stressed that intelligence remains primarily a national responsibility, while concerns over trust and sovereignty continue to constrain deeper cooperation. In any case, the discussion reflects a broader recognition that **effective intelligence-sharing is becoming increasingly important in addressing**



onsulted.

Figure 2: Main Intelligence Services from EU Member States.
Source: Own elaboration. Map generated using Artificial Intelligence.

cross-border threats such as cyberattacks, foreign interference, sabotage and hybrid warfare[44].

2.2 EU-NATO COOPERATION

2.2.1 Institutional and Operational Relationship between the EU and NATO

The institutional and operational relationship between the European Union and the North Atlantic Treaty Organisation (NATO) has become a central element of the European security architecture. Although both organisations share many members and strategic interests, they were created with different institutional purposes. NATO remains the primary framework for collective defence and military deterrence in Europe, particularly through Article 5 of the Washington Treaty. The EU, by contrast, has developed its security and defence role mainly through the Common Security and Defence Policy (CSDP), focusing on crisis management, civilian missions, defence capability development, resilience, sanctions, and regulatory instruments. This difference has created **a relationship based not on institutional replacement, but on functional complementarity**[45].

The foundations of EU–NATO cooperation were established during the post-Cold War period, when European states sought to strengthen their own crisis-management capacity while preserving NATO's central role in transatlantic security. The most important early framework was the Berlin Plus arrangements, concluded in 2002–2003. These agreements allow the EU to access NATO planning capabilities, command structures and common assets for EU-led military operations in cases where NATO as a whole decides not to engage. Berlin Plus provided the institutional basis for operations such as Operation Concordia in North Macedonia and Operation Althea in Bosnia and Herzegovina, showing that EU military action could be supported by NATO structures without undermining the Alliance's primacy in collective defence[46].

However, the practical development of EU–NATO cooperation remained limited for many years. Political disagreements between member states, different strategic cultures, and unresolved institutional tensions restricted deeper coordination. One of the most persistent problems has been the fact that not all EU Member States are NATO Allies, and not all NATO Allies are part of the EU. This creates political and procedural difficulties, particularly when decisions require consensus or when sensitive information is involved. As a result, **cooperation has often advanced more easily in technical and operational areas than in politically sensitive domains.**

The security environment changed significantly after Russia's annexation of Crimea in 2014 and even more sharply after the full-scale invasion of Ukraine in 2022. These events reinforced **the perception that European security could no longer be treated as a low-priority or primarily civilian policy area.** In response, the EU and NATO intensified their cooperation through a more structured political framework. The 2016 Joint Declaration on EU–NATO cooperation, signed in Warsaw by the Presidents of the European Council and the European Commission together with the NATO Secretary General, identified key areas for closer cooperation, including hybrid threats, cyber defence, maritime security, military mobility, defence capabilities, defence industry, exercises and partner capacity-building[47].

This agenda was expanded through later Joint Declarations in 2018 and 2023. The third Joint Declaration, signed in January 2023, reflected a much more demanding geopolitical context marked by Russia's war against Ukraine, strategic competition, cyber threats, foreign interference, attacks on critical infrastructure and growing instability in Europe's neighbourhood. It reaffirmed that a stronger and more capable European defence should contribute positively to transatlantic and global security, while remaining complementary to NATO[48].

Institutionally, EU–NATO cooperation takes place through regular political dialogue, staff-to-staff contacts and coordination between specialised bodies. The European External Action Service (EEAS), the European Union Military Staff (EUMS), the European Commission, NATO's International Staff and NATO's military structures maintain channels of communication in areas such as resilience, cyber security, military mobility, hybrid threats and capability development.

Operationally, the relationship is based on **a practical division of labour.** NATO concentra-

44 Roussi, Antoaneta. "EU's Intelligence Hub Eyes Bigger Role in Security Overhaul." POLITICO Europe, May 27, 2026. https://www.politico.eu/article/eus-intelligence-hub-eyes-bigger-role-in-security-overhaul/

45 NATO, Relations with the European Union, NATO, accessed June 16, 2026.

46 European External Action Service (EEAS), EU-NATO Cooperation Factsheet, EEAS, accessed June 16, 2026.

47 NATO, Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of NATO, Warsaw, July 8, 2016.

48 NATO and European Union, Joint Declaration on EU-NATO Cooperation, January 10, 2023.

tes on collective defence, deterrence, military planning, interoperability and high-intensity military operations. The EU contributes through crisis-management missions, economic sanctions, financial instruments, defence industrial policy, regulatory coordination, infrastructure funding and civilian-security tools.

Military mobility is one of the clearest examples of operational complementarity. The EU can use its regulatory and financial instruments to improve transport infrastructure, simplify cross-border procedures and support the rapid movement of troops and military equipment across Europe. These efforts directly benefit NATO and illustrate how EU instruments can strengthen NATO's operational effectiveness without duplicating NATO's military role[49].

The war in Ukraine has further demonstrated the importance of EU–NATO coordination. NATO has remained the principal framework for deterrence and collective defence, while the EU has played a major role through sanctions, financial assistance, military support mechanisms, training missions and defence-industrial initiatives.

The EU Strategic Compass, adopted in 2022, also reflects this closer relationship. It recognises NATO as the foundation of collective defence for its members while arguing that the EU must become a more capable security actor. NATO's 2022 Strategic Concept similarly identifies the European Union as a unique and essential partner. Together, these documents show a growing convergence in threat perception and strategic priorities[50].

Overall, EU–NATO cooperation has evolved from limited institutional coordination into a structured strategic partnership and remains one of the key pillars of contemporary European security.

2.2.2 Complementarities, Overlaps and Areas of Strategic Dependence

The relationship between the EU and NATO is characterised by a combination of complementarity, institutional overlap and strategic dependence. While both organisations pursue the common objective of ensuring security and stability in Europe, they operate through different institutional frameworks and possess distinct sets of capabilities.

The concept of complementarity has become the dominant framework guiding EU–NATO relations. NATO remains responsible for collective defence, deterrence and military readiness, while the EU provides economic, regulatory, diplomatic and industrial instruments that NATO does not possess. This functional division allows each organisation to address different dimensions of modern security challenges while pursuing common strategic objectives.

The EU has progressively strengthened its contribution to defence through initiatives such as Permanent Structured Cooperation (PESCO), the European Defence Fund (EDF), the Coordinated Annual Review on Defence (CARD) and the Strategic Compass. These instruments seek to improve defence capability development, encourage joint procurement and strengthen Europe's defence industrial base. NATO has generally welcomed these efforts, provided that they remain compatible with Alliance planning and contribute to burden-sharing among European allies[51].

Despite these areas of cooperation, **discussions regarding institutional overlap** have become increasingly relevant. Programmes such as PESCO, the EU Rapid Deployment Capacity and various capability-development initiatives have occasionally been viewed as potential sources of redundancy. However, many scholars and European institutions reject the notion that current EU initiatives constitute harmful duplication, arguing that they seek to address capability gaps that NATO itself has repeatedly identified[52].

The issue of strategic dependence represents perhaps the most significant challenge within the EU–NATO relationship. Despite substantial increases in European defence spending following Russia's invasion of Ukraine, **Europe continues to rely heavily on the United States for several critical military capabilities.** These dependencies are particularly evident in intelligence, surveillance and reconnaissance (ISR), satellite-based systems, strategic airlift, aerial refuelling, missile defence, cyber capabilities and advanced command-and-control systems[53].

49 European Commission, Military Mobility, European Commission, accessed June 16, 2026.

50 Council of the European Union, A Strategic Compass for Security and Defence (Brussels: Council of the European Union, 2022); NATO, NATO 2022 Strategic Concept (Madrid: NATO, 2022).

51 Council of the European Union, A Strategic Compass for Security and Defence (Brussels: Council of the European Union, 2022).

52 European Defence Agency, Coordinated Annual Review on Defence (CARD) Report. Brussels: European Defence Agency, 2024. https://eda.europa.eu/docs/default-source/documents/card-report-2024.pdf.

53 NATO, NATO 2022 Strategic Concept (Madrid: NATO, 2022).

Strategic intelligence remains one of the most important areas of dependence. Although European countries possess sophisticated intelligence services and institutions such as EU INTCEN and SatCen, the United States continues to provide much of the strategic intelligence that supports NATO operations and European decision-making. American satellite networks, surveillance systems and intelligence-sharing mechanisms remain essential components of Europe's security architecture[54]. A similar situation exists in strategic transport, logistical support and missile defence, where American technological superiority continues to provide a substantial share of NATO's operational effectiveness[55].

Nuclear deterrence constitutes another area of dependence. Following the withdrawal of the United Kingdom from the European Union, France became the EU's only nuclear power. Nevertheless, NATO's nuclear deterrence posture remains overwhelmingly dependent on the strategic capabilities of the United States[56].

Russia's full-scale invasion of Ukraine has further highlighted these dependencies. While European states have increased defence expenditure and accelerated military cooperation, the conflict has demonstrated the continued importance of American military assistance, intelligence support and logistical capabilities. At the same time, **the war has strengthened arguments in favour of developing greater European defence capabilities** in order to reduce vulnerabilities and increase strategic resilience. This has revitalised debates surrounding European strategic autonomy.

The concept of strategic autonomy remains contested among EU Member States. For some governments, it refers to the ability of Europe to act independently when necessary while remaining firmly anchored within NATO. Others fear that excessive emphasis on autonomy could weaken the transatlantic relationship or create unnecessary duplication of existing structures. The 2023 Joint Declaration on EU–NATO Cooperation reflects an attempt to reconcile these perspectives. It emphasises that **a stronger and more capable European defence contributes positively to transatlantic security** while reinforcing the Alliance's overall effectiveness[57].

Overall, the relationship between the EU and NATO demonstrates that complementarity currently outweighs competition. Although institutional overlaps occasionally generate political debate, most European defence initiatives are designed to address capability shortfalls rather than replace NATO structures. Nevertheless, significant strategic dependencies on the United States, as NATO's hegemonic power, continue to shape the limits of European defence autonomy. The future evolution of European security will therefore depend on finding an effective balance between strengthening European capabilities, preserving transatlantic cohesion and ensuring that EU defence initiatives reinforce rather than undermine NATO's deterrence and defence posture.

3 TOWARDS THE DEVELOPMENT OF A EUROPEAN DEFENCE INDUSTRY

European defence has reached a critical juncture, characterized by high-intensity military confrontation on the continent and a drastic deterioration of the security environment since early 2025[58] [59]. This shift in the international order demands an urgent transition from temporary emergency measures towards the structural preparation of European defence readiness. **The ongoing Russian aggression against Ukraine has become an existential challenge for the European Union**[60]. Since 2024, the Russian Federation has mobilized its economy into a war model, dedicating 40% of its federal budget and up to 9% of its GDP to the defence industry. In response, the collective defence spending of the 27 EU Member States reached a record €343 billion in 2024 (1.9% of GDP), with projections reaching 2.1% of GDP for 2025.

However, even with this historic surge in spending, **external dependence remains a critical vulnerability for European sovereignty**, as 78% of defence acquisitions between February 2022 and June 2023 ori-

54 European Parliament Research Service (EPRS), EU-NATO Cooperation: State of Play and Future Prospects (Brussels, 2024).

55 RAND Europe, European Strategic Autonomy and Defence Cooperation (2024).

56 SIPRI, Military Expenditure and European Defence Capabilities Report, latest edition.

57 NATO and European Union, Joint Declaration on EU-NATO Cooperation, January 10, 2023.

58 European Commission. "White Paper for European Defence – Readiness 2030." European Commission, March 2025.

59 European Commission. "Proposal for a Council Regulation establishing the Security Action for Europe (SAFE) through the reinforcement of European defence industry Instrument." European Commission, March 19, 2025

60 European Commission. "Communication from the Commission: Accommodating increased defence expenditure within the Stability and Growth Pact." European Commission, March 19, 2025

ginated from outside the EU. Consequently, strategic autonomy is no longer a mere aspiration but a long-term necessity, especially as traditional allies rebalance their focus away from the continent[61]. To address these challenges, the EU has launched the "ReArm Europe" plan, a comprehensive framework designed to mobilize up to €800 billion to ensure that Member States invest "more, better, together, and European"[62]. This strategy aims to build a robust European defence posture by 2030, capable of countering not only conventional aggression but also a global technological arms race in areas like AI and quantum computing, alongside an increasing tide of hybrid threats.

3.1.1 FRAGMENTATION IN DEFENCE INDUSTRY

The European Defence Technological and Industrial Base (EDTIB) is currently characterized by a persistent fragmentation of demand along national lines[63]. **This structural weakness stems from an industrial landscape where dominant "national champions" focus their production almost exclusively on satisfying their respective domestic markets, which fundamentally hinders the creation of a truly integrated European defence market.** This lack of cooperation has a direct and negative impact on the Union's competitiveness and response capacity[64]. The absence of coordination has led to a multiplication of defence systems of the same kind within the EU, generating critical inefficiencies in public spending. Consequently, the industry often operates under sub-optimal performance, missing the so-called "collaborative dividend": the opportunity to leverage economies of scale that would otherwise reduce unit costs and improve overall industrial efficiency[65]. Furthermore, fragmented spending on research and technology (R&T) halts the development of emerging disruptive technologies, which are vital for maintaining a technological edge and ensuring long-term military sovereignty.

The statistical evidence of this problem is stark. Currently, only 18% of defence equipment is acquired cooperatively, a figure that falls significantly short of the 35% historical objective set by the European Defence Agency (EDA) and the new 40% target established for 2030 by the European Defence Industrial Strategy (EDIS)[66].

This **internal lack of cohesion translates into a dangerous external dependence**[67]. Between February 2022 and June 2023, 78% of the defence acquisitions made by EU Member States originated from outside the Union[68]. Moreover, the value of intra-EU defence trade currently represents only 15% of the total market value, whereas the strategic aim is to reach at least 35% by 2030 Without a major shift towards aggregated demand, the EU risks exacerbating these dependencies, further undermining the competitiveness and readiness of the EDTIB[69].

3.1.2 SOVEREIGNTY AND DIFFICULTIES IN COOPERATION

According to the **White Paper for European Defence**, Member States retain exclusive responsibility for their own troops deployment, and for defining the specific needs of their armed forces. Furthermore, any EU initiative must respect the right of Member States to protect their essential security interests in accordance with Article 346 of the TFEU[70].[71] Sovereignty-first approaches have historically translated into significant administrative and regulatory barriers that hinder cooperation[72]. These facts are able to benchmark the great challenge for the development of a unified European defence framework; the inherent tension between collective action and national sovereignty.

Bureaucracy also constitutes an obstacle for things such as military mobilization, which is limited by complex procedures of diplomatic authorization and lack of harmonization in procedures.These administrative hurdles cause severe delays in cross-border deployments, undermining the EU's capacity to respond. The European Defence Technological and Industrial Base (EDTIB) often faces obstacles in the granting of construction and environmental permits for industrial projects, as well as difficulties in the exchange of classified and sensitive information. On the other hand, strict fiscal

61 European Defence Agency. "Annual Report 2025." European Defence Agency, 2026

62 European Commission. "European Defence Industrial Strategy (EDIS)." European Commission, March 2024

63 European Commission. "White Paper for European Defence – Readiness 2030." European Commission, March 2025.

64 European Commission. "Proposal for a Council Regulation establishing the Security Action for Europe (SAFE) through the reinforcement of European defence industry Instrument." European Commission, March 19, 2025.

65 European Commission. "Proposal for a Council Regulation establishing the Security Action for Europe (SAFE) through the reinforcement of European defence industry Instrument." European Commission, March 19, 2025

66 European Parliament. "Legislative Train 06.2026: A New Era for European Defence and Security." European Parliament, June 20, 2026.

67 European Commission. "European Defence Industrial Strategy (EDIS)." European Commission, March 2024.

68 European Parliament. "Legislative Train 06.2026: A New Era for European Defence and Security." European Parliament, June 20, 2026

69 European Defence Agency. "Annual Report 2025." European Defence Agency, 2026.

70 European Commission. "White Paper for European Defence – Readiness 2030." European Commission, March 2025.

71 European Commission. "Proposal for a Council Regulation establishing the Security Action for Europe (SAFE) through the reinforcement of European defence industry Instrument." European Commission, March 19, 2025.

72 European Defence Agency. "Annual Report 2025." European Defence Agency, 2026.

rules have limited the capacity of Member States to ramp up defence spending without endangering their stability paths. To address this, the Commission has proposed the coordinated activation of the "**national escape clause**", allowing States to deviate from net expenditure paths to accommodate defence investments of up to 1.5% of GDP[73].

3.1.3 INDUSTRIAL COOPERATION AND STRATEGIC AUTONOMY

The European Union sees its strategic autonomy evolve from just a political aspiration to a structural need in response to the deterioration of the international order and geopolitical tensions. Furthermore, international competitiveness promotes a transition from temporal emergency measures to a permanent state of European Defence Readiness, based on the foundation of higher spending to reinforce competitiveness on the technological and industrial European foundation (EDTIB)[74,75]. This strategic framework is based on 3 fundamental principles:

- **1st.** Aggregation of demand through national acquisition coordination with the aim to surpass the European defence market fragmentation, as it's been discussed, allows member states to benefit from scale economies, major industrial predictability and reinforce interoperability from first design phases to capacity development[76].

- **2nd.** The union has introduced a number of juridical and economical incentives to defence investment, such as the Security Action for Europe (SAFE) instrument, which will mobilize up to 150 billion euros in loan support to conjoined defence related acquisitions, such as drones and aerial defence systems. This is conjoined with the creation proposal of the Structure for European Armament Programme (SEAP) and fiscal measures such as VAT exemptions for joint procurement initiatives[77].

- **3rd.** The European Defence Industrial Strategy (EDIS) establishes measurable targets for 2030, including conducting at least 40% of defence procurement collaboratively, increasing the value of intra-EU defence trade to 35% of the European defence market, and allocating at least 50% of defence procurement expenditure to the EDTIB by 2030, with this proportion rising to 60% by 2035[78].

These initiatives pretend to materialize the collaboration dividend allowing the Union to reach an industrial and technological capacity that no other State member could reach by themselves, while also reducing external import dependency. This would **consolidate the role of the European Union as the most autonomous defence provider inside the euroatlantic security architecture.**

3.2 PRIORITISATION OF MILITARY CAPABILITIES

For most of the post-Cold War period, EU Member States planned their defence investments in isolation, producing a patchwork of incompatible national systems and collective gaps that no single country could address alone. The publication of the White Paper for European Defence, Readiness 2030 in March 2025 marked a decisive break with this pattern. For the first time, the EU institutions produced a framework explicitly identifying which military capability domains were most urgently deficient and most in need of coordinated investment. The gaps identified were not invented by the Commission: they were derived directly from the EU Capability Development Plan (CDP), coordinated by the European Defence Agency (EDA), and aligned with NATO's own capability targets for its European members. This dual alignment is deliberately significant, as it establishes that collaborative EU programmes can serve as a vehicle through which Member States meet their NATO commitments more efficiently than by acting alone.

The White Paper identifies seven priority capability domains, integrated air and missile defence against the full spectrum of airborne threats, artillery systems and long-range precision strike, ammunition and missiles including strategic stockpiles, drones and counter-drone systems across all environments, military mobility enabling the rapid movement of forces across EU territory, artificial intelligence , quantum computing, cyber, and electronic warfare, and strategic enablers and critical infrastructure protection, covering capabilities

73 European Commission. "Communication from the Commission: Accommodating increased defence expenditure within the Stability and Growth Pact." European Commission, March 19, 2025.

74 European Commission. "White Paper for European Defence – Readiness 2030." European Commission, March 2025.

75 European Commission. "European Defence Industrial Strategy (EDIS)." European Commission, March 2024.

76 European Commission. "European Defence Industrial Strategy (EDIS)." European Commission, March 2024.

77 European Commission. "Proposal for a Council Regulation establishing the Security Action for Europe (SAFE) through the reinforcement of European defence industry Instrument." European Commission, March 19, 2025.

78 European Parliament. "Legislative Train 06.2026: A New Era for European Defence and Security." European Parliament, June 20, 2026.

such as air-to-air refuelling, encrypted communications, and space-based services.

The October 2025 Defence Readiness Roadmap expanded this structure further into nine Capability Coalitions, adding ground combat and maritime domains, and proposed that Member States form lead-nation groups around each area, with concrete implementation plans by Q1 2026, projects launched in H1 2026, and financing in place to close critical shortfalls by end-2028.

The strategic logic behind each priority domain becomes clear when examined against the current threat environment and the lessons drawn from the war in Ukraine. Air and missile defence stands as the most immediately urgent area: Russia's sustained use of ballistic missiles, cruise missiles, and drone swarms against Ukrainian infrastructure has demonstrated that without a layered, integrated continental air defence system, even advanced societies are vulnerable to strategic paralysis. Europe's current national air defence systems are technologically inconsistent, geographically patchy, and operationally unlinked. The proposed European Air Shield aims to address this, supported by the SAFE instrument, which provides up to 150 billion in EU-backed loans for collaborative procurement. Land and ground combat has re-emerged as a central priority after decades of neglect, as the war in Ukraine restored the reality of large-scale, high-intensity armoured warfare on the European continent. The EDA confirms that while Member States collectively possess substantial numbers of tanks and infantry fighting vehicles, these assets are severely fragmented.

The cyber AI, and electronic warfare domain is the most rapidly evolving of all the priority areas. The war in Ukraine has served as its most intensive real-world testing ground: Russian cyber operations preceded the kinetic invasion by months, and electronic warfare has been deployed at a scale not seen since the Second World War, with both sides jamming communications, disrupting drone navigation, and blinding enemy sensors. The White Paper acknowledges that the EU's strategic competitors are investing heavily in AI, quantum computing, autonomous systems, and directed-energy weapons, and warns that **the window of opportunity for Europe to remain competitive is closing.** Military mobility has also emerged as a critical enabler: practical obstacles such as differing rail gauges, bridge weight limits, and complex cross-border customs procedures can delay the movement of military convoys across EU territory by days or weeks. A 2025 European Court of Auditors Special Report concluded that the EU's Military Mobility Action Plan 2.0 lacked sufficiently solid foundations. Finally, space has consolidated itself as a contested and indispensable military domain. Modern forces depend on satellite systems for navigation, communications, intelligence, and precision targeting, all of which are increasingly vulnerable to jamming and direct attack. The proposed European Space Shield, building on Galileo, Copernicus, and IRIS², aims to protect these assets and ensure their resilience for defence purposes.

3.3 STRUCTURAL AND POLITICAL BARRIERS

The gap between the ambition of the White Paper and the EDIS and what European defence integration has historically delivered is enormous, and it is not primarily a gap of ideas, but of financial resources, institutional design, and political will. **The financial obstacle is rooted in the legacy of post-Cold War defence underfunding.** Combined EU defence spending fell from around 2.5% of GDP in the early 1990s to approximately 1.3% by the mid-2010s, leaving production lines shut down, stockpiles depleted, and the industrial base atrophied. Since Russia's full-scale invasion of Ukraine in 2022 Member States have significantly reversed this trend: combined EU defence expenditure rose from 218 Billion in 2021 to 343 billion in 2024, with defence investment exceeding 106 Billion for the first time, a 42% increase in real terms compared to 2023. However, this still falls well short of what is needed. The United States spent 845 billion on defence in 2024, nearly two and a half times the combined EU total, and achieves far greater capability per euro spent due to its integrated procurement market. The ReArm Europe plan aims to mobilise up to €800 billion in additional European defence spending through SAFE, national fiscal flexibility, EIB financing, and redirected cohesion funds, but the actual amount will depend entirely on Member States' willingness to commit.

The institutional obstacle is equally significant. EU defence policy operates through overlapping institutions, the EDA, the EU Military Staff, PESCO, DG DEFIS, and the High Representative's office, each with distinct mandates and relationships with national governments. The European Court of Auditors' October 2024 opinion on the EDIP criticised the regulation for lacking a firm policy design and clear accountability mechanisms, and warned that dispersing a limited €1.5 billion budget across too many projects would blunt its impact. **The political obstacle is the most fundamental.** Defence

ministers across all Member States face a structural incentive to channel procurement spending towards domestic suppliers: doing so protects jobs, maintains industrial capacity, and generates political credit at home. Supporting joint EU procurement, by contrast, transfers control to a supranational mechanism and yields little domestic reward. This logic has prevailed consistently for three decades despite repeated high-level commitments to deeper cooperation. A further dimension of the political barrier is legal: Article 346 TFEU grants Member States a broad derogation from EU law, including competition rules, whenever they judge that applying EU rules could compromise their essential security interests. Governments have routinely invoked this provision to exclude defence contracts from European competitive tendering entirely, and the 2009 Defence Procurement Directive (2009/81/EC), designed specifically to curb this practice, has had only limited success.

The fragmentation of European defence procurement is the most visible and quantifiable consequence of all the barriers described above Despite more than two decades of European-level initiatives designed to foster integration, from the EDA's 2007 collaborative procurement benchmark, to EDIRPA, EDIP, and SAFE, the structure of European defence procurement has changed remarkably little. The EDA's 2022 Coordinated Annual Review on Defence (CARD) found that only 18% of total investment in defence programmes involved cooperation between Member States, barely above the 11% recorded in 2020, and far below the 35% benchmark set in 2007. The October 2025 Defence Readiness Roadmap confirmed that collaborative procurement still stands at under 20%, despite a dramatically worsened security environment and record defence spending levels. The platform proliferation that results from this pattern is extraordinary: **EU Member States collectively operate more than 170 different major weapons systems, compared with around 30 in the United States**. European NATO members operate 12 different main battle tank platforms, the US Army operates one. Europe produces three operational combat aircraft types (Eurofighter Typhoon, Rafale, and Gripen), with a combined total of approximately 1,860 units ordered or delivered, against the US F-35 programme's planned output of around 3,556 units, a difference in scale that directly reduces European manufacturers' ability to lower unit costs.

The economic costs are substantial. A 2019 European Parliament study estimated that greater collaborative procurement could generate annual savings of approximately 22 billion, a more recent EPRS assessment raised this range to between 24.5 billion and 75.5 billion per year. Beyond the economic dimension, platform fragmentation imposes direct operational penalties: when allied forces from different Member States deploy together, their equipment frequently cannot share ammunition, spare parts, or communications frequencies, directly undermining collective military effectiveness. The structural driver of this fragmentation is industrial competition between national defence industries, each protected by its own government's procurement preferences and, where necessary, by national security exemptions under Article 346 TFEU. According to research by Bruegel economists, Germany and France each procure more than 80% of their defence equipment from domestic national suppliers. The EDIS seeks to counter this by setting ambitious targets, 40% of equipment procured jointly and 50% from EDTIB suppliers by 2030, and offering financial incentives through EDIP and SAFE. However, both the targets and the instruments remain non-binding and voluntary. The track record, 18% joint procurement in 2022 despite a 35% target set fifteen years earlier, gives grounds for a cautious assessment of whether the current frameworks will prove more effective than their predecessors.

4

TOWARDS A EUROPEAN ARMY: STRATEGIC NECESSITY OR POLITICAL UTOPIA?

The debate on the path towards a "European Army" has become a great topic of discussion in security and defence related discourse within Europe, especially in recent times. This idea is nothing new however, as it has been discussed since the early days of the European project[79].

For some, it represents **the logical culmination of European integration:** a standing military force under common political authority, able to defend the EU's territory and interests without excessive reliance on external actors. For others, it is little more than a political slogan, something that advocates for European sovereignty, but institutionally unrealistic in a Union still marked by divergent

79 Bergmann, Max. "Why It's Time to Reconsider a European Army." Center for Strategic and International Studies, February 28, 2025.

strategic values and priorities, as well as heavy dependence on NATO.

As such, it is important not to frame this topic as a binary choice between a fully supranational european army, against the current models of cooperation within security and defence. This approach risks diminishing the question of if the European Union is capable of progressively transforming its current national defence efforts into a coherent and united military framework.

In that sense, the "European Army" debate is better understood not just as a symbolic project, but as a matter about strategic autonomy, military integration, and a scenario where **European states have the ability to act together as a credible security and defence provider.**

As such, before evaluating its feasibility, it is necessary to understand what the concept actually refers to. It is also equally important to understand the drivers and obstacles that are linked with this idea of an "European Army", as well as possible scenarios that a greater step towards further security and defence integration can take.

4.1 CONCEPTUALISING AN 'EUROPEAN ARMY'

There are a couple of notes worth mentioning when trying to conceptualize the idea of an "european army". This is not necessarily a new concept, and has been approached by many high level figures, such as René Pleven, then Prime Minister of France, whose 1950 plan for a European Defence Community remains the earliest concrete attempt, or more recently Emmanuel Macron, current President of the French Republic, to name a few examples[80]. And truth is that it is a concept that is ambiguous, as it can take many different forms and approaches[81].

First and foremost, it is a model which highlights enhanced military integration, leading to the creation of a supranational standing force with a unified command structure, common rules of engagement, and shared operational authority.

On a second note, the idea behind this concept is also linked with a structured compatibility, where national armies remain sovereign but increasingly normalize equipment, doctrine, training, and logistical procedures within each other. T**his idea allows to bring harmony between the different national structures**, thus enabling stronger joint operations under a coordinated European command. As it stands, the "European Army" is still a hypothetical idea, one that would act as a replacement for the Common Security and Defence Policy and would go beyond the proposed European Defence Union.

4.2 DRIVERS TOWARDS GREATER EUROPEAN MILITARY INTEGRATION

As it was the case for the creation of the European Union as a whole, the drivers towards a greater European military integration are motivated by the current geopolitical landscape where Europe positions itself. There are different catalysts that we are able to pinpoint in order to better understand the current conjuncture.

One clear point traces back to February 2022, amidst Russia's full-scale invasion of Ukraine, which has now gone over more than four years. The threat presented by the Russian Federation and the existence of a large conflict in European soil has compelled member states to take action, particularly in terms of energy security and providing military support to Ukraine. The Russian invasion **has also made European leaders realize that war in the continent is not a distant reality**[82].

Still on the topic of the past years, the re-election of Donald Trump as president of the United States of America has forced Europeans to rethink their approach to security topics and take on higher responsibilities. Trump's open criticism of these countries' involvement in NATO, and explicit questioning of Article 5 commitments, has left Europeans on alert. Although the US remains a strategic ally for EU member states, it is not a guarantee that relations in the future will stay healthy, meaning that there may be the need to rethink the EU's strategic autonomy[83].

However, **one thing is for sure: Europeans are taking action**. More specifically, member states are investing more and more in their defence spending, in order to meet the target values established. At the European Union level, one example is ReArm Eu-

80 Pfeufer, Jonas. "The European Army – The Future of European Defence?" EuroDefense Network, June 19, 2024.

81 Franke, Ulrike. "The 'European Army', a Tale of Wilful Misunderstanding." European Council on Foreign Relations, December 3, 2018.

82 Genini, Davide. "Restructuring the EU's Defence Industrial Base amid Geopolitical Shifts." European View 32, no. 5-6 (2025).

83 Everts, Steven. "Europe Must Focus on Defending Itself, Not on Keeping Trump Happy." European Union Institute for Security Studies, June 15, 2026.

rope, which aims to mobilise €800 billion. So, it is clear that **there is a financial momentum in order to take further steps towards a greater European integration in terms of security and defence**[84].

Furthermore, the fragmented European defence industrial base is beginning to consolidate itself, showing a greater industrial consolidation. Several European companies are forming joint ventures to pool technologies and achieve greater results together[85].

Finally, over the last years many institutional mechanisms within the EU have paved the way to an increasing dependence when it comes to defence capabilities. A few examples are the Strategic Compass (2022), the EU Rapid Deployment Capacity (RDC), the European Defence Fund, European Defence Industry Programme (EDIP), and the Defence Readiness Roadmap 2030.

4.3 POLITICAL/INSTITUTIONAL OBSTACLES

Despite the drivers listed that illustrate a favourable scenario to establish an European Army, at the same time, the European Union faces both political and institutional obstacles that pose a threat to a greater security integration, which are also worth noting.

An important aspect to take into account is **the sovereignty aspect**. Defence is the most intimate expression of national sovereignty, and the European Union is no exception: as it is not a defence union, national defence and security is very much a national responsibility[86]. Furthermore, national defence is still associated with many factors that are closely linked with its national citizens, such as history, geography, culture, etc. This means that, by wanting to establish a supranational EU body that operates within security and defence, it is important that member states are aligned and, at the same time, that there is a **high level of political trust.**

In line with this, the different states that make up the European Union also have different divergent strategic cultures and threat perceptions across the Union. **EU member states do not approach defence from a common strategic baseline**[87]. For frontline states in Eastern Europe, deterrence against Russia and territorial defence remain the overriding priority. For Southern member states, instability in North Africa and the Sahel, maritime security, migration-related pressures, and the protection of Mediterranean routes often occupy a more prominent place.

When regarding institutional obstacles, and despite recent developments, the structural points within the EU such as Treaty on European Union (TEU) provide only limited support for territorial defence. Article 42(2) TEU refers to a possible "common defence," but the conditions for establishing it are strict and would likely require treaty and constitutional changes. Beyond this provision, the TEU offers no clear legal basis for EU-led territorial defence[88].

Although Article 42(7) TEU contains a mutual defence clause similar to NATO's Article 5, it is addressed to the Member States rather than the EU itself. In addition, the framework for military operations under Articles 42–46 TEU is mainly designed for crisis-management missions outside EU territory, not for territorial defence.

Still on the institutional side, we must also consider PESCO's underperformance. Member states' progress under the Permanent Structural Cooperation have been limited by their fundamental reluctance to cooperate meaningfully in defence[89]. The enforcement mechanisms are weak: after seven years of implementation, only half of the anticipated 26 PESCO projects reached full operational capability in 2025, with the other half projected ready between 2026 and 2029. Member states have also been unable to formally link PESCO with the European Defence Fund, limiting coherence between capability development and industrial investment, and as such, there is a need to rethink a more flexible approach to make use of PESCO's true capabilities[90].

Finally, despite the growing investment in defence and security by the different member states, **European states' industry capabilities are still heavily dependent on external actors**, with the leading

84 Mariette, Damien. "European Strategic Autonomy Also Encompasses Defense." CPRAM, September 4, 2023.

85 Sevi, Nurettin. "European Defence: Building Strategic Autonomy through Integration." Defense Domain, accessed June 24, 2026.

86 Loss, Rafael, Marta Prochwicz Jazowska, and Jana Puglierin. Making Defence European Again. Policy Brief. European Council on Foreign Relations, June 4, 2026.

87 Gilli, Andrea, Nicole Koenig, Margarita Šešelgytė, and Ricarda Nierhaus. "European Cohesion for Security and Defense." DGAP Policy Brief 1 (2026). German Council on Foreign Relations, February 2026.

88 Meijer, Karsten, and Arjen Klein. "A European Army and Three Difficult Choices." Verfassungsblog, March 6, 2025

89 Cordet, Maxime. "EU Defence Series: PESCO Must Step Up." International Centre for Defence and Security, March 7, 2025

90 Blockmans, Steven, and Karsten Meijer. "Pioneers Wanted: On the Differentiated Integration Pathways Towards a Genuine European Defence Union." Verfassungsblog, April 28, 2026.

partner being the United States of America[91]. Reducing this dependency would require increased budgets and a fundamental restructuring of buyers habits, a process that would take many years to adapt to.

4.4 POLICY OPTIONS AND FUTURE SCENARIOS

Having in mind the different drivers and obstacles that European states face, it is safe to note that greater cooperation in the realm of security and defence becomes a matter of handling the current situation and finding suitable alternatives for the current context.

It is notable that **member states require an enhanced strategic approach, one that is more cohesive and united**, in order to approach the security related challenges of our times. At the same time, it is also notable that, although the situation is looking positive, the status quo does not show the needed conditions for establishing a European Army, something that seems to still be far away. Hence, here are a couple alternative policy options and future scenarios.

The first scenario is an enhanced minimalist coordination, where Member states continue to spend more at the national level, and the EU-level mechanisms work as means to enhance coherence. This scenario proves to be less commitment oriented, since defence remains an intergovernmental area, and able to obtain short-term results. Despite this, the EU still faces structural vulnerability when talking about a coherent framework for the collective use of member states and their coordination.

The second scenario picks up on a core group of different member states that are capable and willing to deepen their integration in the realm of security and defence by improving already existing, such as PESCO as mentioned beforehand. This approach ensures that the members involved are willing to enhance their cooperation, and have their priorities aligned, setting ambition over universal participation from all member states. Positive results might even motivate states that weren't involved in a first phase.

A third scenario could be a functional supranationalist approach from within the European Union itself, where formal political unification is progressively introduced in key cooperation areas such as defence industrial standardisation, or cyber defence. This scenario avoids issues related to sovereignty, while, at the same time, it reinforces the capabilities of acting together.

91 Abulebada, Namat. "Prospects for a European Military." Fiker Institute, July 2025.

PROPOSALS

Proposal 1

From a policy perspective, the EU could consider **further expanding both Union-level and national capabilities in order to reduce external dependencies.** At the same time, maintaining close cooperation with the private sector remains important for fostering innovation, incorporating emerging technologies, and enhancing operational effectiveness. Such a balanced approach could contribute to the practical realisation of the EU's broader objective of strategic autonomy.

However, progress in this area faces significant political constraints. Initiatives involving defence integration, intelligence cooperation, or the transfer of additional competencies to supranational institutions require a degree of consensus among member states that remains difficult to achieve under current political conditions.

To improve defence cooperation, EU Member States should strengthen the implementation of existing coordination mechanisms rather than creating additional frameworks. Greater alignment between national defence planning, CARD recommendations, and PESCO projects would help ensure that increased defence spending translates into shared capabilities and reduces unnecessary duplication. Particular attention should be given to jointly developing and procuring strategic enablers, such as airlift, space-based assets, and cyber-defence capabilities, where collective action can generate significant economies of scale and reduce dependence on external actors.

At the political level, Member States should provide clearer guidance on the objectives of European defence cooperation and reinforce coordination with NATO. A more coherent division of competences between (and within) the EU and NATO, combined with stronger political commitment to collaborative capability development, would enhance interoperability, improve operational readiness, and strengthen Europe's capacity to respond to security challenges while preserving transatlantic cooperation.

This recommendation would improve interoperability and coordination across EU Member States by reducing duplication of capabilities and increasing the efficiency of defence investment. It would also reduce dependence on external partners, encourage greater willingness to share and integrate intelligence capabilities, and strengthen European strategic autonomy, ultimately contributing to a more coherent and resilient European defence architecture.

Proposal 1:
Strengthening EU defence coordination

Problem	Fragmented defence planning, duplicated capabilities, and unclear EU–NATO coordination weaken European defence effectiveness and increase dependence on external partners.
Intervention	Strengthen implementation of existing EU defence coordination by aligning national defence planning, CARD priorities, and PESCO projects, while reinforcing EU–NATO cooperation and joint capability development.
Actors	European Commission; European Defence Agency (EDA); EEAS; Member States; Council of the EU; NATO.
Immediate (0–18 months)	Improve coordination of defence planning and investment, strengthen EU–NATO political coordination, and expand joint capability development and procurement.
Structural (2–5 years)	Institutionalise coordinated defence planning, increase integration of intelligence-sharing systems and agencies, clearer EU–NATO responsibilities, and integrated capability development through stronger governance mechanisms.
Expected outcome	Greater interoperability, reduced duplication and external dependence, stronger European strategic autonomy, more willingness to integrate intelligence capabilities, and a more coherent and resilient European defence architecture.

Proposal 2

Additionally, the EU should consider **redesigning its defence funding architecture so that financial support is explicitly conditional on collaborative behaviour**, rather than treating joint procurement as a voluntary aspiration. At the same time, encouraging a more layered industrial structure would allow the European Defence Technological and Industrial Base to achieve the economies of scale it currently lacks without eliminating competition altogether (through SMEs competing within their supply chains while a limited number of EU-level main contractors would be responsible of major platform categories). Such an approach could contribute to closing the persistent gap between record defence expenditure and the EU's own 2030 targets for collaborative purchases and intra-EU defence trade.

However, progress in this area faces significant political constraints. Defence ministers face a structural incentive to direct procurement towards domestic suppliers, since doing so protects jobs and industrial capacity at home, while supporting EU-level investments returns comparatively lower domestic political reward. Article 346 TFEU further allows Member States to exempt defence contracts from EU competition rules whenever 'essential security interests' are invoked, a provision that has been used consistently to shield national markets from European-level tendering.

To improve industrial cooperation, the EU should tie access to instruments such as SAFE loans and EDIP grants to a minimum share of joint procurement, so that fiscal flexibility at the national level becomes an entry point into further integration rather than a substitute for it. Particular attention should be given to consolidating the fragmented base of micro-companies operating in emerging domains such as AI and electronic warfare, where no single actor in the EU currently reaches the scale needed for sustained R&S investment.

At the political level, Member States should treat the 40% joint-procurement and the 50% EDTIB-sourcing targets set out in the EDIS as binding conditions attached to EU co-financing, reversing the pattern by which similar targets set in 2007 were missed by a wide margin without any consequences.

This recommendation would reduce the equipment duplication that currently drives up costs and undermines interoperability across the Union. It would also make European defence manufacturers more competitive against non-EU suppliers, helping transform record levels of spending into capabilities that Member States genuinely share rather than duplicate.

Proposal 2:
Reforming EU Defence Industrial and Procurement Policy

Problem	Fragmentation of the European defence industry along national lines, combined with non-binding collaborative procurement targets, resulting in the multiplication of incompatible national weapon systems, weak economies of scale and continued dependence on non-EU suppliers.
Intervention	Tie access to EU co-financing instruments such as SAFE loans and EDIP grants to a minimum share of joint procurement, as well as encouraging a layered industrial structure where EU-level main companies are responsible for major platform categories, while SMEs compete within their supply chains.
Actors	European Commission; European Defence Agency (EDA); EEAS; Member States; European defence industry (eg. Airbus); European Investment Bank (EIB).
Immediate (0–18 months)	Attach joint procurement conditions to SAFE and EDIP disbursements, and identify priority domains, such as AI and electronic warfare, where industrial consolidation is most urgently needed.
Structural (2–5 years)	Change the EDIS's 2030 targets from a voluntary benchmarks into binding conditions for EU co-financing, and support the emergence of a smaller number of competitive EU-level prime contractors.
Expected outcome	Reduced multiplication of incompatible national weapons systems, lower unit and life-cycle costs, a more competitive European defence industrial base relative to non-EU suppliers and stronger conversion of record defence spending into shared (hence stronger) capabilities.

Conclusion

To prepare this policy brief, the analysts have approached the current European context by focusing on the transition from the emergency response triggered by recent geopolitical developments to the development of a long-term structural defence strategy. The shift from aspiration to strategic need of this defence and military cooperation between EU members does not only stem from the Russian aggression but also from the political changes done in the transatlantic relationship. Traditional allies, such as the United States, have increasingly rebalanced their strategic focus away from Europe, reducing their historical role as the continent's primary security guarantor. This shift has **transformed strategic autonomy from a political aspiration into a long-term structural necessity**.

To address this new reality, the Union is transitioning from reactive emergency measures toward a permanent state of "European Defence Readiness" by 2030. This evolution is guided by the core principle of investing "more, better, together, and European" to bolster the competitiveness of the European Defence Technological and Industrial Base (EDTIB) and mitigate critical external dependenciesWhen discussing investment, it is important to note that extreme fragmentation and external dependence reduce the impact of the record €343 billion spent on defence in 2024. Despite this unprecedented level of spending, these structural problems continue to limit the EU's operational capacity.

Beyond fragmented spending, the EU faces three interconnected challenges in regards to its defence industry:

Hardware
Closing critical capability gaps in air defence, drones, military mobility, and ammunition.
Software and institutional hurdles Simplifying bureaucracy through the Defence Omnibus to speed up information sharing and administrative procedures.
Industrial network Strengthening the European Defence Technological and Industrial Base (EDTIB) while prioritising Ukraine's integration as a strategic partner.

In order to overcome such challenges, **structural transformation of the European defence is supported in powerful funds designed to mobilize resources at a never before seen scale**. The central pillar of this strategy is the SAFE (Security action for Europe) instrument, and its 150 billion euros supported by the Union, destined for cooperative acquisition in priority areas such as aerial defence,drones and artillery. This financial support is complemented by the fiscal flexibility granted through the National Escape Clause, allowing Member States to deviate from their endorse next expenditure to accommodate massive defence investments of up to 1.5% of GDP. Nevertheless, it is argued that, in order to revert the 78% in external dependence in acquisitions, access to SAFE loans and NEC flexibility must be strictly conditioned to cooperative buying and reinforcement of EDTIB, transforming funding into an instrument to ensure structural industrial integration to realize the "collaborative dividend" .

These financial and industrial initiatives should not be understood in isolation but as part of a broader institutional framework that has gradually expanded European defence cooperation. Existing mechanisms such as the Capability Development Plan (CDP), the Coordinated Annual Review on Defence (CARD), Permanent Structured Cooperation (PESCO), the European Defence Fund (EDF), and Common Security and Defence Policy (CSDP) missions have strengthened coordination, improved transparency, and identified common capability priorities. However, as demonstrated throughout this brief, their effectiveness has been constrained by the predominance of national decision-making and the voluntary nature of cooperation. While these instruments provide the institutional foundations for collective capability development, achieving genuine European

Defence Readiness by 2030 will require moving beyond coordination towards binding integration, ensuring that defence planning, procurement, operational cooperation, and intelligence sharing become structural rather than optional features of the European security architecture.

The analysis concludes that achieving European Defence Readiness by 2030 requires **a fundamental shift from voluntary coordination to binding structural integration.** Funding tools such as SAFE and the National Escape Clause with strict conditionality will allow the Union to finally overcome the persistent fragmentation of its markets and realize the 'collaborative dividend'. Furthermore, the strategic integration of Ukraine and the simplification of the regulatory landscape through the Defence Omnibus is the only path for the EU to become a truly credible and autonomous security provider. The EU should spare no room for incrementalism and only cooperation will ensure peace on the continent through industrial unity and collective strength to tackle this historic challenge.

EUROPEAN SECURITY IN A CHANGING WORLD

DEFENCE & MILITARY CAPABILITIES *TOWARDS STRATEGIC AUTONOMY*

How can the EU transform its fragmented defence landscape into a coherent military capability framework?

€295B

Historic collective EU defence spending of €295 billion (EDA, 2024)

↑ SPENDING ≠ ↑ COOPERATION

Where does the money get lost?

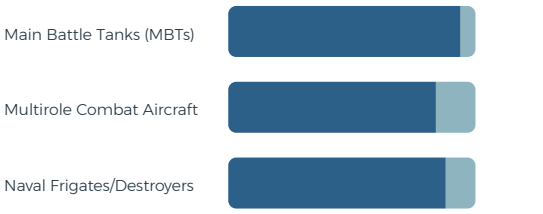
1. National protectionism in procurement
2. Duplication of weapon systems
3. Lack of standardisation across the 27 national inventories

THE SPENDING PARADOX

FRAGMENTATION VS. STANDARDISATION

Between €18 billion and €57 billion per year (estimated) lost due to platform fragmentation

EU V. US - NUMBER OF DIFFERENT PLATFORMS IN USE



78% Imported defence acquisitions between February 2022 and June 2023

FRAGMENTED DEFENCE INDUSTRY

18% Defence equipment acquired cooperatively by members as of March 2024

15% Value of intra-EU defence trade in total market value

The lack of cooperation undermines the EU's competitiveness by creating duplicated defence systems, inefficient public spending, and missed economies of scale that would improve industrial efficiency.



- Imported
- Not imported

Defence related acquisitions by EU-Members 2022-2023

EU

Defence funding
Defence industry
Sanctions
Military mobility
Crisis management
CSDP agencies (EDA, SatCen, etc.)

SHARED CAPABILITIES

- ✓ Cyber secaurity
- ✓ Hybrid threats
- ✓ Capability development
- ✓ Exercises
- ✓ Support to Ukraine
- ✓ Political dialogue

NATO

Collective defence
Deterrence
Military operations
Command structure
Article 5

SOVEREIGNTY AND THE EUROPEAN DEFENCE FRAMEWORK

The National Escape Clause → Defence investment flexibility (up to 1.5% of GDP) → Commission introduces

CHALLENGES	SOLUTION
National control over armed forces	Apart from these challenges, fiscal constraints limited the capacity of Member States to ramp up defence spending without endangering their stability paths.
Respect for Article 346 TFEU: Member States' essential security interests	
Significant administrative and regulatory barriers that hinder cooperation	**SOLUTION? €**

Glossary of abbreviations

AAR	Airborne Refueling
AAW	Anti-Air Warfare
AI	Artificial Intelligence
ASW	Anti-Submarine Warfare
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CARD	Coordinated Annual Review on Defence
CDP	Capability Development Plan
CFSP	Common Foreign and Security Policy
CSDP	Common Security and Defence Policy
c-UAV	Counter-Unmanned Aerial Vehicle
DG DEFIS	Directorate-General for Defence Industry and Space
EDA	European Defence Agency
EDF	European Defence Fund
EDIP	European Defence Industry Programme
EDIRPA	European Defence Industry Reinforcement through Common Procurement Act
EDIS	European Defence Industrial Strategy
EDTIB	European Defence Technological and Industrial Base
EEAS	European External Action Service
EIB	European Investment Bank
EMSA	European Maritime Safety Agency
EPF	European Peace Facility
EPRS	European Parliamentary Research Service
EU	European Union
EUFOR	European Union Force
EUMAM	European Union Military Assistance Mission
EUMS	European Union Military Staff
GDP	Gross Domestic Product
GEOINT	Geospatial Intelligence
HALE	High-Altitude Long-Endurance
H1	First Half (of the year)
INTCEN	European Union Intelligence and Situation Centre
ISR	Intelligence, Surveillance and Reconnaissance
MPCC	Military Planning and Conduct Capability
NATO	North Atlantic Treaty Organization
NEC	National Escape Clause
PESCO	Permanent Structured Cooperation
Q1	First Quarter (of the year)
R&D	Research and Development
RDC	Rapid Deployment Capacity
SAFE	Security Action for Europe
SatCen	European Union Satellite Centre
SEAP	Structure for European Armament Programme
SIAC	Single Intelligence Analysis Capacity
SLOCs	Sea Lines of Communication
SMEs	Small and Medium-sized Enterprises
TFEU	Treaty on the Functioning of the European Union
TEU	Treaty on European Union
UK	United Kingdom
US	United States
VAT	Value Added Tax

EQUIPO EUROPA





NUCLEUS CHAPTER 2

ECONOMIC SECURITY

SECURING EUROPE'S FUTURE SECURITY: ENERGY, ECONOMIC SECURITY AND COMPETITIVENESS IN AN ERA OF GEOECONOMIC FRAGMENTATION

Authors: Borja Álvarez Resa, Alejandra Sofía Carrera García, Luciana Belén Escalante Columbus, Sofía Martín Fernández, Diego Muñoz Carreño, Sheila Ozuo-Omén López, Pablo Prieto Medina.
Reviewers: María Villaverde Temes and Santiago Slullitel.

Forum on the Future of the EU

EUROPEAN SECURITY in a Changing World

EXECUTIVE SUMMARY

The European Union faces an increasingly volatile international order marked by geoeconomic fragmentation and systemic rivalry. Trapped between US dominance in digital infrastructure and capital markets, and China's near-monopoly on critical raw materials and clean-tech manufacturing, the EU risks economic marginalization. Nevertheless, this fragmentation presents an opportunity for the EU to leverage its single market power to become more geoeconomically assertive and resilient.

While the EU remains a global economic powerhouse with a GDP of €18 trillion and a 16.3% share of global trade, its structural power is constrained by external dependencies and internal market fragmentation. In digital infrastructure and artificial intelligence, US cloud hyperscalers control approximately 70% of the European market, while a single US firm controls around 85% of global AI hardware. In critical raw materials, China refines roughly 90% of the world's rare earth elements and controls 98% of permanent magnet production, creating an acute supply chokehold for Europe's green transition and energy security. Furthermore, capital market fragmentation triggers an estimated €470 billion in annual capital flight as scale-ups relocate to the US, compounding a persistent productivity gap exacerbated by over 13,000 regulatory acts passed between 2019 and 2024.

To secure long-term competitiveness while safeguarding sovereign interests, the European Union must bridge this implementation gap through streamlined coordination and targeted discretion. Addressing these vulnerabilities requires completing the Savings and Investments Union to retain domestic capital, deploying a synchronized European diversification strategy for energy and critical inputs, and harmonizing national investment screening alongside internal regulatory frameworks. By combining clear baseline standards with flexible, intelligence-driven governance, the EU can protect its strategic interests without insulating itself from global markets or compromising its underlying economic strength.

Keywords

Geoeconomics; Priority sectors; Competitiveness; Resilience; Strategic autonomy; Vulnerability; Interdependencies.

INTRODUCTION

Economic security has become a first-order priority within today's swiftly changing international relations. Despite being a domain to which EU Member States appeared initially reluctant to commit collectively, recent reports, and -most critically- the European Economic Security Strategy, have set objectives designed to minimise risks while simultaneously fostering economic growth and European competitiveness in **a policy area increasingly shaped by geopolitical tension.**

The EU accordingly seeks to secure a position within the global value chain and is starting to draft proposals designed to reduce vulnerabilities and differentiate its strategic position from the US-China rivalry, with the ambition of ceasing to be the passive arena in which that rivalry plays out[1].

This policy brief provides a structured and analytically rigorous overview of the sectors identified as most critical and priority within the EU's economic security framework. To this end, in order to ensure an evidence-based approach, the sources introduced are drawn mainly from EU institutional reports, meeting summaries and website official content. To adopt the critical and analytical approach a policy brief requires, these primary sources are complemented by external analysis, mainly reports and articles produced by leading think tanks.

Consequently, the ultimate objective of this document is to **analyse Europe's current position within today's geoeconomic context** -one characterised by intensifying rivalry and an accelerating competition towards technological and market dominance. In this context, and in alignment with the updated EU strategy[2] The analysis focuses not only on the areas where the bloc maintains critical dependencies, but also on those where other external actors still heavily rely on the EU.

Accordingly, the structure is as follows: It first provides an overview of the sectors identified as strategic priorities; it then offers a diagnostic of each sector's situation, distinguishing between areas of persistent interdependency and areas under relative European control. The document subsequently assesses the EU tools and mechanisms linked to the implementation and financing of the sectors. The policy brief concludes with an overall assessment, including analytical reflections, followed by two policy proposals.

1 CSIS. "Unveiling the European Union's Major Economic Security Update: Is a True Geopolitical Commission Emerging?". December 2025. https://www.csis.org/analysis/unveiling-european-unions-major-economic-security-update-true-geopolitical-commission

2 On December 2025 the European Commission announced a comprehensive update to the Economic Security Strategy.

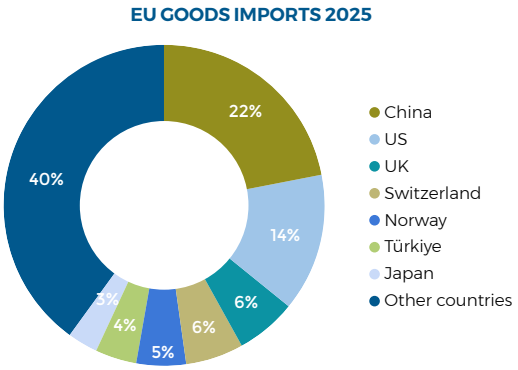
1 STRENGTH AND WEAKNESSES

The EU combines **significant structural strengths with persistent vulnerabilities** that shape its competitiveness, resilience and economic security. While the Single Market, the euro and a common trade policy provide a strong economic foundation, internal fragmentation and external dependencies continue to constrain the Union's strategic autonomy.

The Single Market is the cornerstone of European integration. Since 1993, it has guaranteed free movement of goods, services, capital and people across an economy of ~450 million consumers, 26 million businesses and €18 trillion in GDP[3] -boosting EU GDP by ~3-4% and creating some 3.6 million jobs[4]. Significant barriers persist nonetheless, particularly in services, where regulatory fragmentation limits the Market's full potential. Meanwhile, the euro has become the world's second international currency[5], eliminating exchange-rate risks across 21 Member States, easing trade and investment and strengthening Eurozone resilience through the ECB's price stability framework[6]. The EU's common trade policy reinforces these strengths: as the world's largest trading bloc, accounting for around 16% of global trade, with the most extensive network of trade agreements,the Union gains bargaining power, diversified export markets and improved access to strategic resources[7].

Despite these advantages, Europe's economic security is increasingly constrained by external dependencies. China dominates strategic clean-technology value chains -accounting around 90% of global manufacturing capacity for green-technology raw materials and finished products[8] -while the EU remains dependent on the US for key defence capabilities[9] and on East Asia for advanced semiconductors, exposing European industry to geopolitical tension and supply-chain disruptions.

Figure 0: EU Goods Imports (2025)



Source: Own Contribution based on Eurostat Data

A related challenge is **the relocation of innovative firms:** around 10% of European scale-ups relocated abroad, and nearly a third of EU unicorns moved headquarters outside the Union between 2008 and 2021[10], while no European company founded in the last half century has reached a €100 billion valuation[11]. Beyond the outflow itself, **the lack of a coordinated mechanism to monitor and retain high-growth firms weakens industrial policy,** particularly in AI digital technologies, where relocation also entails the loss of innovation capacity and technological know-how[12].

Internal constraints further compound vulnerabilities. Unanimity requirements constrain the Union's ability to respond rapidly to geopolitical developments[13] and regulatory fragmentation raises compliance costs and limits firms' ability to scale: between 2019 and 2024, the EU adopted approximately 13,000 legislative acts[14], with diverging national implementation adding complexity[15]. This is reflected in Europe's limited presence among the world's largest technology companies.

Fragmentation also affects long-term competitiveness[16]: limited electricity interconnections, incom-

3 European Commission. n.d. "Single Market". Brussels. https://commission.europa.eu/topics/single-market_en

4 *European Commission. n.d. "Single Market". Brussels. https://commission.europa.eu/topics/single-market_en*

5 *European Union. n.d. "The Euro - Benefits". Brussels. https://european-union.europa.eu/institutions-law-budget/euro/benefits_en*

6 *European Union. 2026. "Key European Union achievements and tangible benefits". Brussels. https://european-union.europa.eu/principles-countries-history/achievements_en*

7 *European Commission. n.d. "Trade". Brussels, https://commission.europa.eu/topics/trade_en*

8 *"A Potential Trade War With China: EU Strengths and Weaknesses." The Diplomat. October 01, 2024. https://thediplomat.com/2024/10/a-potential-trade-war-with-china-eu-strengths-and-weaknesses/*

9 *B. Wolff G. et al. The Governance and Funding of European Rearmament. Volume 60, Number 4 ·(2025)pp. 210–214. https://www.intereconomics.eu/contents/year/2025/number/4/article/the-governance-and-funding-of-european-rearmament.html*

10 *European Investment Bank. "Drivers of Relocation by Innovative EEU Start-ups and Scale-ups". 2026. Pg. 7.*

Garicano, Luis. "Strategic autonomy for Europe requires economic growth." CEPR. 2025. https://cepr.org/voxeu/columns/strategic-autonomy-europe-requires-economic-growth

12 *JRC. "Is Europe losing its startups?" European Commission. 2026. Pg.2.*

13 *Rothacher, Albrecht. "A global economic giant and political dwarf: strengths and weaknesses of EU foreign and security policy." MIWI, 2022. https://miwi-institut.de/archives/1950*

14 *Garicano, Luis. "Strategic autonomy for Europe requires economic growth." CEPR. 2025. https://cepr.org/voxeu/columns/strategic-autonomy-europe-requires-economic-growth*

15 *Draghi, Mario. "The future of European competitiveness Part A." European Union. 2025. https://commission.europa.eu/topics/competitiveness/draghi-report_en*

16 *OECD. "OECD Economic Surveys: European Union and Euro Area 2025".Pg. 88 .2025 https://doi.org/10.1787/5ec8dcc2-enc*

plete capital-market integration and productivity[17], demographic and digital-skills gaps continue to constrain growth[18]. According to the Draghi Report, lower productivity explains nearly three-quarters of the EU's per capita income gap with the US, showing that Europe's economic security depends as much on strengthening internal capacity as on reducing external dependencies.

THE EU'S COMPETITIVE POSITION IN THE GLOBAL ECONOMY

The European Union (EU) remains one of the world's leading economic powers, accounting for around 16% of global trade in goods and services and maintaining strengths in pharmaceuticals, aerospace, chemicals, advanced manufacturing and financial services[19]. Nevertheless, sustaining this position increasingly depends on productivity, innovation, investment and technological leadership, where Europe faces growing challenges from the United States (US) and China[20].

The global competitive landscape has further intensified these challenges. The US continues to outperform the EU across the main drivers of innovation-led growth. According to the European Commission's 2025 Annual Single Market and Competitiveness Report, EU labour productivity stands at only 78% of US levels, while research and development expenditure reaches 2.2% of GDP compared with 3.6% in the United States[21]. Backed by deeper capital markets and industrial policies such as the CHIPS and Science Act and the Inflation Reduction Act, the US has strengthened its leadership in artificial intelligence, cloud computing and advanced semiconductors[22]. Meanwhile, China has consolidated its position through long-term industrial planning, vertically integrated supply chains and global leadership in batteries, electric vehicles, solar technologies and critical raw material processing[23].

At the same time, Europe's competitive position is constrained by structural weaknesses within the Single Market. According to the Letta and Draghi Reports, regulatory fragmentation creates barriers equivalent to tariffs of approximately 44% for goods and 110% for services, limiting economies of scale and the growth of innovative firms across the Single Market[24]. High energy prices, with electricity costs remaining two to three times higher than in the United States and China, further reduce industrial competitiveness[25].

These challenges demonstrate that **assessing European competitiveness requires a sector-specific perspective rather than relying solely on aggregate economic indicators**. As technological leadership, resilient supply chains and strategic inputs increasingly shape economic security, identifying the sectors where the Union retains strengths or faces critical vulnerabilities becomes the next step of the analysis.

2 PRIORITY SECTORS

To provide a more visual explanation of Europe's economic dependencies, the following table has been prepared. Sectors classified as **Category A (Strength)** represent areas in which the European Union maintains a clear global competitive advantage that it can leverage as a source of strategic power. **Category B (Manageable Dependence)** includes sectors where external vulnerabilities exist, but the EU possesses sufficient capacity for diversification, risk mitigation, or niche leadership. Finally, **Category C (Critical Dependence)** identifies structural bottlenecks where the Union faces severe asymmetric risks and has limited room for manoeuvre.

Economic resilience comprises **five interrelated dimensions** that together address the main sources of strategic vulnerability: supply-chain robustness, understood as the capacity to absorb and recover from external shocks; resistance to economic coercion; resource security through reliable access to critical raw materials, energy and food systems; technological sovereignty over enabling technologies, standards and digital infrastructure; and geoeconomic projection through strategic part-

17 *Eurogroup. "Competitiveness of the European economy." 2024. https://www.consilium.europa.eu/en/press/press-releases/2024/11/04/competitiveness-of-the-european-economy-statement-of-the-eurogroup-in-inclusive-format/*

18 *Kammer,Alfred. "Europe's Integration Imperative." IMF. 2025. https://www.imf.org/en/publications/fandd/issues/2025/06/europes-integration-imperative-alfred-kammer*

19 *European Commission*, 2025 Annual Single Market and Competitiveness Report *(Brussels: European Commission, 2025).*

20 *Mario Draghi*, The Future of European Competitiveness *(Brussels: European Commission, 2024), Part A.*

21 *European Commission*, 2025 Annual Single Market and Competitiveness Report, *10-18.*

22 *Draghi*, The Future of European Competitiveness, *Part B, chap. 1.*

23 *Draghi*, The Future of European Competitiveness, *Part B, chap. 2.*

24 *Enrico Letta*, Much More Than a Market *(Brussels, 2024), 45-56; Draghi*, The Future of European Competitiveness, *Part A.*

25 *Enrico Letta*, Much More Than a Market *(Brussels, 2024), 45-56; Draghi*, The Future of European Competitiveness, *Part A.*

Sector	Classif.	Key dependency	Main suppliers
AI & digital infrastructure	C	~70% US cloud; ~85% Nvidia GPUs	US (+ China alt-stack)
Critical raw materials	C	~90% Chinese REE refining; ~98% of magnets; weaponized in 2025	China
Energy	B	Russian gas cut & locked; Rosatom fuel + Chinese clean-tech remain	Russia → US / China
Supply Chain	B	Maritime chokepoints; Chinese stakes in EU ports; Asian shipbuilding dependence	China
Semiconductors	B	ASML EUV chokepoint; Taiwan for leading-edge	US (policy) / Taiwan
Trade Policy	A	World's largest trading bloc in terms of exports and key trading partner for more than 80 countries	
Agriculture	A	Europe is a net exporter of finished food.	Russia-fertilizers US - Livestock Feed
Pharmaceutical	B (APIs)	China and India for the supply of numerous active pharmaceutical ingredients (APIs)	China (80%)
Financial Infrastructure	A	Euro = #2 currency; dollar-clearing chokepoint; fragmented markets	

Source: Own elaboration
European Economic Resilience: Evaluating external supply corridors and geoeconomic vulnerabilities

nerships and influence across global value chains. From this perspective, EU resilience extends beyond the shock-absorption capacity of the Single Market towards the active management of external dependencies. Recent initiatives, including the Critical Raw Materials Act (CRMA) and the Global Gateway, reflect this broader approach by promoting supplier diversification, resilient partnerships and greater strategic engagement with resource-rich countries. **Economic resilience emerges from the interaction of these five dimensions** rather than any single policy instrument. The EU's capacity to achieve it is best assessed in comparison with other major powers, particularly China, the United States, and Russia.

China's rapid, state-directed expansion through the Belt and Road Initiative (BRI) has focused on critical minerals, green energy, transport, and manufacturing[26]. Beijing has also strengthened its resilience against economic coercion through legal instruments, including the 2026 Regulations on Countering Improper Extraterritorial Jurisdiction and the Industrial and Supply Chain Security Regulations, which expand state protection over strategic sectors[27]. Lastly, it maintains dominance in AI, biotechnology, and 5G while exporting digital standards to create structural, long-term dependencies.

The United States prioritizes domestic industrial capacity, framing critical minerals, energy, and medical supplies as national security assets, driven by the National Energy Dominance Council and strategic reserves. Washington has secured technological leadership through the 2025 AI Action Plan, semiconductor investments, the GENIUS Act, and the "Pax Silica" partnership to set US-centric tech ecosystems. The US uses its domestic market scale, bilateral partnerships (EU, Japan, India), and tax/investment incentives (One Big Beautiful Bill Act) to attract capital and center industrial supply chains domestically.[28]

Lastly, Russia has adapted its supply chain by rerouting trade through third-party hubs (Türkiye, UAE), expanding links with China, and investing in the Northern Sea Route, though this increases costs and creates structural reliance on third countries.[29] It uses alternative payment mechanisms like A7, legal countermeasures, and redirects energy/mining partnerships to Africa (e.g., Rosatom). Nevertheless, it remains restricted by R&D limits, lost Western technology, and asymmetric dependence on Chinese markets.[30]

EU'S RESILIENCE

The resilience of the EU's supply chains is underpinned by the Single Market, where 61% of exports remain within the Union, reducing exposure to external disruptions[31]. **This resilience is reinforced by supplier diversification, strategic stockpiling,**

26 *Christoph Nedopil Wang,* China's Investment and Construction Engagement in the Belt and Road Initiative (BRI) 2026 H1 *(Green Finance & Development Center, July 26, 2026), https://greenfdc.org/chinas-investment-and-construction-engagement-in-the-belt-and-road-initiative-bri-2026-h1/?cookie-state-change=1785271048751*

27 *Jacob Gunter, Rebecca Arcesati, Helena Legarda, and Nis Grünberg,* China Is "Securitizing" Its Economy: Beijing Expands Security-First Economic Policy as Shocks from Global Crises Grow *(Mercator Institute for China Studies, April 23, 2026), https://merics.org/en/merics-briefs/china-securitizing-its-economy.*

28 *Council of Economic Advisers, "Strengthening America's Industrial Supply Chains," in* Economic Report of the President 2026 *(Washington, DC: Executive Office of the President, April 2026), https://www.whitehouse.gov/cea/2026-erp/.*

29 *Paché, Gilles. "Logistics under Fire: Russia's Supply Chain Response to Western Sanctions."* International Affairs and Global Strategy *103 (2026): 1–14. https://hal.science/hal-05511589v1/document*

30 *Council of the European Union. 2026. "21st Package of Sanctions: EU Hits Russian Energy, Financial Services and Crypto Hard.", July 23, 2026. https://www.consilium.europa.eu/en/press/press-releases/2026/07/23/21st-package-of-sanctions-eu-hits-russian-energy-financial-services-and-crypto-hard/*

31 *European Commission, Directorate-General for Economic and Financial Affairs,* European Economic Forecast: Spring 2026, *Institutional Paper 341 (Brussels: European Commission, 21 May 2026), 271, https://economy-finance.ec.europa.eu/publications/european-economic-forecast-spring-2026_en*

digitalisation, and lower energy dependence, although critical external vulnerabilities persist[32]. Furthermore, the EU has strengthened its structural resilience through a significant reduction in energy intensity and the diversification of its supply sources, factors that help mitigate vulnerability to external energy crises and geopolitical shocks, while reducing, rather than eliminating, exposure to critical external dependencies. The EU has also strengthened its defensive toolkit through the Anti-Coercion Instrument (ACI), which enables coordinated responses to economic coercion, as well as through broader efforts to reinforce domestic production in strategic sectors[33].

To enhance resource security, the EU launched the RESourceEU Action Plan, promoting joint procurement, strategic stockpiling, supply diversification, and greater access to critical raw materials[34]. In parallel, the Union has strengthened its technological sovereignty through measures targeting key technologies, digital infrastructure, and technological standards (see Chapter 3.5). Regarding the geoeconomic projection of the EU, it is particularly important to address one of the main European policies in terms of resilience, the **Global Gateway,** and compare it with its main rival, the **Chinese Belt and Road initiative.** *(Table 1)*

The evaluation of the EU's external infrastructure frameworks highlights that the trade-off between high standards and operational speed remains a defining feature of its strategic resilience. The Global Gateway's emphasis on transparency, environmental standards, and procurement rules ensures sustainable projects but also raises costs and delays implementation. This reduces its appeal in developing countries, where governments often prioritise rapid financing and delivery over regulatory alignment. This friction varies across regions. For middle-income Latin American economies seeking to upgrade value chains while avoiding dependency, the EU offers an attractive alternative[35]. Expanding Free Trade Agreements, including the EU–Mercosur agreement, and Sustainable Investment Facilitation Agreements **strengthens European supply chains and supports the EU's shift from market expansion to economic de-risking**. Regulatory integration thus becomes the EU's main tool for competing with the structural models of China and the US.

The blended finance model has struggled to mobilise private investment at the expected scale. Although the EU committed €300 billion for 2021–2027, by the end of 2025 only part had been disbursed, largely concentrated in a small number of flagship projects[36]. This execution gap is especially evident in Latin America and the Caribbean, where the Global Gateway has fallen short of its €45 billion investment target. By contrast, Africa has received the largest share of the initia-

Table 1

Dimension	Global Gateway (EU)	Belt & Road Initiative (China)
Objectives	Strategic autonomy, sustainable development, mutually beneficial partnerships, and value-adding cooperation..	Secure raw materials, expand export markets, internationalize RMB, build infrastructure dependencies.
Financing Model	Public-private blended model (€300B target, 2021–2027) via EIB/EBRD slowed by complex governance and deployment deficits.	State-backed public capital (>USD 1.5T since 2013) centrally deployed via state-owned banks, Minimal co-financing
Governance Standards and political influence	High EU procurement rules, environmental/social safeguards, strict transparency, and financial conditionality. Promotes democratic values.	State sovereignty and non-interference. State-centered bilateral governance without political/human rights conditionality. Leverage gained through strategic assets and economic dependence.
Infrastructure Delivery	Slower implementation and disbursement; higher standards increase upfront costs; strong reliance on private-sector mobilisation.	Over a decade of proven, rapid delivery across 150+ countries via state-directed financing and SOEs..
Resilience Impact	Creates multi-note, diversified networks to eliminate single points of failure.	Creates asymmetrical dependencies centered on Beijing.

32 *European Investment Bank*, Shock Waves from Turbulent Times: How EU Businesses Recalibrate Supply Chains *(Luxembourg: European Investment Bank, 26 June 2025), https://www.eib.org/en/publications/20250099-shock-waves-from-turbulent-times-how-eu-businesses-recalibrate-supply-chains*

33 *Gehrke, Tobias, and Nina Schmelzer.* Beijing Hold'em: European Cards against Chinese Coercion. *Policy Brief. London: European Council on Foreign Relations, 31 March 2026 https://ecfr.eu/publication/beijing-holdem-european-cards-against-chinese-coercion/*

34 *Comisión Europea, "Preguntas y respuestas sobre el Plan de Acción RESourceEU," QANDA/25/2886, Bruselas, 3 de diciembre de 2025, https://ec.europa.eu/commission/presscorner/detail/es/qanda_25_2886*

35 *Letta, Enrico. 2024.* Much More Than a Market (Letta Report). *Brussels: European Commission. https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf*

36 *Simone Tagliapietra, "Global Gateway: Europe's Answer to China's Belt and Road?" Bruegel Blog, January 2022. https://www.bruegel.org/blog-post/global-gateway. OECD, "Blended Finance in Fragile Contexts," DAC Working Paper (Paris: OECD, 2023). https://www.oecd.org/dac/blended-financefragile-contexts-2023.htm.*

tive's investment[37]. Overall, slow implementation reflects the EU's difficulty operating in complex middle-income markets, allowing strategic rivals to strengthen their infrastructure presence and secure long-term resource access before European alternatives emerge[38].

More broadly, the EU has yet to establish a coherent and viable alternative to China's vertically integrated model. Strategic Projects[39] and Partnerships[40] under the Critical Raw Materials Act with several countries, many of them in Africa, are a promising step, seeking to secure access to critical raw materials while promoting local processing and deeper economic cooperation. However, **slow implementation continues to expose a gap between the EU's strategic ambitions and its delivery capacity.**

3 INTERDEPENDENCIES

An analysis of capabilities related to the European Union's economic security requires a thorough examination of the structural vulnerabilities stemming from its global trade and industrial relationships. Having identified the priority sectors for the bloc (outlined in the preceding table), this section presents a **detailed diagnostic of those critical areas** in which the EU exhibits persistent and asymmetric interdependencies with external actors, particularly the United States and China. Across five key vectors—critical raw materials, semiconductors, energy security, supply chains, and digital infrastructure and artificial intelligence—it examines how external bottlenecks and geographic supplier concentration compromise European competitiveness and resilience. The objective of this section is **to map the scale of these strategic dependencies** in order to provide an evidence base for the risk-mitigation (de-risking) and diversification tools that the EU must deploy.

3.1 SEMICONDUCTORS

Semiconductors have evolved from being a neglected structural dependency to a EU's strategic priority. As the Draghi Report argues, they are a key enabler of Europe's industrial competitiveness and economic security[41], underpinning virtually every strategic sector. Indeed, COVID-19 shortages demonstrated how supply disruptions can rapidly cascade across industries, particularly automotive and electronics[42]. Yet the EU accounts for only ~10% of global semiconductor production[43], and the EU's manufacturing base falls critically short of consumption needs, remaining heavily dependent on imports of advanced logic and memory chips from Taiwan. In fact, nearly 80% of input suppliers and 63% of customers in European semiconductor value chains are located outside the Union[44], exposing the sector to growing geopolitical risks.

Geographic concentration further amplifies Europe's semiconductor vulnerability. East Asia, particularly Taiwan, dominates both legacy and leading-edge production, with only TSMC and Samsung possessing commercial capacity for the most advanced logic chips[45]. Within Europe, Infineon and STMicroelectronics remain global leaders in power semiconductors and automotive chips, yet no European company accounts for more than 8-10% of regional semiconductor revenue[46], illustrating the limited scale of the industrial base and its absence from the highest-value segments.

These structural constraints are reinforced by Europe's limited access to highly skilled labour, critical raw materials and competitively priced energy, all of which are essential for semiconductor fabrication[47].Financial support also remains comparatively modest: while the US CHIPS and Science Act provide $52.7 billion in direct funding, complemented by $24 billion in tax incentives, only €3.3 billion of the EU Chips Act comes directly from the European Commission[48]. As the EU represents

37 *European Commission, "Global Gateway," accessed August 1, 2026, https://commission.europa.eu/topics/international-partnerships/global-gateway_en.*

38 *GARCÍA-HERRERO Alicia. (2024).* David and Goliath: The EU's Global Gateway versus China' s Belt and Road Initiative. *Bruegel. https://www.bruegel.org/newsletter/david-and-goliath-eus-global-gateway-versus-chinas-belt-and-road-initiative*

39 *European Commission.* Selected Strategic Projects under CRMA. *https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials/strategic-projects-under-crma/selected-projects_en*

40 *Eszter Szedlacsek,* Critical Alliances: Mapping Africa's Mineral Partnerships with European Countries *(Berlin: Africa Policy Research Institute, June 22, 2026) , https://afripoli.org/critical-alliances-mapping-africas-mineral-partnerships-with-european-countries*

41 *Draghi, Mario. "The Future of European Competitiveness. Part B." European Union. 2024. Pg. 68.*

42 *Directorate-General for Internal Policies. "Impacts of the COVID-19 pandemic on EU industries." European Union. 2021.*

43 *"European Committee of the Regions Regions team up to speed up the expansion of the European semiconductor industry". 2023. https://www.cor.europa.eu/en/news/regions-team-speed-expansion-european-semiconductor-industry*

44 Ceruti, I. and Nardo M. "Semiconductors in the EU. State of Play, future trends and vulnerabilities of the semiconductor supply chain. *"JRC Technical Report. 2023. Pg. 32.*

45 Op cit. JRC Report. Pg. 17.

46 *IMARC Group."Europe Semiconductor Market Size, Share, Trends & Forecast (2026-2034)." Report Description. https://www.imarcgroup.com/europe-semiconductor-market*

47 *Mitchener, Brandon. "Chips Act spurs semiconductor investments in Europe." Science Business.19 Feb 2026 https://sciencebusiness.net/news/semiconductors/chips-act-spurs-semiconductor-investments-europe*

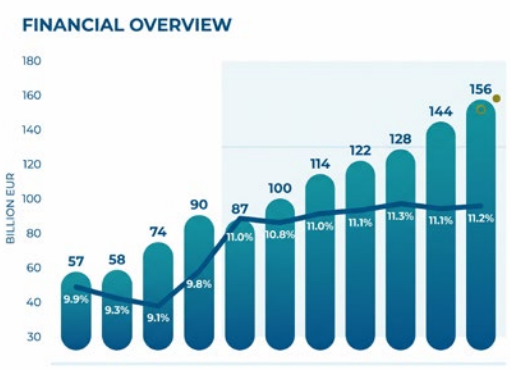
48 *Chips Act | U.S. Semiconductor Legislation and Policies https://www.european-chips-act.com/USA_Semiconductor_Legislation.html*

less than 10% of global semiconductor production but around 20% of global demand[49], these asymmetries have become an increasingly important source of strategic risk.

Export controls have become a central instrument of geoeconomic competition, as illustrated by the United States' October 2022 restrictions on advanced semiconductors and manufacturing equipment[50], which extended extraterritorial jurisdiction to products incorporating US technology[51]. These measures exposed the absence of a harmonised EU export-control framework[52], despite the Union's dual-use regime subsequent expansion to include semiconductor equipment, quantum technologies and advanced materials[53]. At the same time, Europe retains important sources of strategic leverage through frontier semiconductor research and manufacturing equipment -most notably ASML's global leadership in EUV lithography. The Dutch government's 2023 decision to restrict exports of advanced DUV systems to China demonstrated how these capabilities can be deployed as instruments of economic security[54]. Meanwhile, China's response has focused on expanding mature-node manufacturing, the segment supplying Europe's automotive, industrial and power electronics sectors, where its global market share is projected to reach 39% by 2027[55], reinforcing European exposure precisely where substitution options remain limited.

These developments have prompted a more active EU semiconductor strategy. The European Chips Act mobilises €43 billion to increase the EU's share of global semiconductor production to 20% by 2030[56], complemented by the Microelectronics IPCEI and the Alliance on Processors and Semiconductor Technologies. The Commission has approved thirteen state-aid decisions for first-of-a-kind facilities, representing more than €32 billion in investment[57], and granted Integrated Production Facility and Open EU Foundry status to four projects, providing streamlined permitting, priority administrative support and preferential access to pilot lines and crisis orders[58].

Figure 1: Semiconductors Value Chain Revenues in the EU



Source: Annex to the Communication on the State of the Digital Decade 2024. Pg. 14.

Moreover, in September 2025 all 27 Member States signed the Semicon Coalition Declaration committing to a reinforced semiconductor agenda[59], and the Commission followed in June 2026 with a proposed Chips Act 2.0 to further reduce dependencies and support advanced chip production[60].

However, the European Court of Auditors concluded that the 20% target for 2030 is unlikely to be met, due to insufficient demand analysis, the absence of a full impact assessment, and a funding architecture that mainly relies on Member States and private investors -with the European Commission committing only 10% of public funding[61]. Yet smaller Member States can act with greater agility, piloting innovation and niche capabilities like advanced packaging[62], with favourable wage and electricity costs[63] maximising the value of each euro.

Two structural gaps stand out. First, policy has prioritised manufacturing capacity over design

49 *In terms of the location of consumers or end users that buy electronic devices.* Op cit. *Pg. 16. JRC Technical Report.*

50 *Bureau of Industry & Security. "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)" October 7, 2022 https://www.bis.gov/press-release/commerce-implements-new-export-controls-advanced-computing-semiconductor-manufacturing-items-peoples*

51 *Eitel, Matthew. "Export Controls - The Keys to Forging a Transatlantic Tech Shield." Center for European Policy Analysis. 2023 https://cepa.org/comprehensive-reports/export-controls-the-keys-to-forging-a-transatlantic-tech-shield/*

52 *European Commission. "White Paper on Export Controls" 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024DC0025*

53 Op cit. *White Paper on Export Controls.Pg 9.*

54 *Trueman, Charlotte. "Dutch government revokes some ASML lithography export licenses, due to US pressure." DCD. January 2nd 2024 https://www.datacenterdynamics.com/en/news/dutch-government-revokes-some-asml-lithography-export-licenses-due-to-us-pressure/*

55 *Ezell, Stephen. "How Innovative Is China in Semiconductors?" ITIF. August 19, 2024 https://itif.org/publications/2024/08/19/how-innovative-is-china-in-semiconductors/*

56 *European Commission. "The EU Chips Industry". Last modified 14 April 2025 https://www.consilium.europa.eu/en/policies/eu-chips-industry/*

57 *II Pillar of the European Chips Act. European Commission. "European Chips Act". Last modified 23 June 2026 https://digital-strategy.ec.europa.eu/en/policies/european-chips-act*

58 *DigiByte. "Milestone in strengthening Europe's semiconductor manufacturing capacity under Chips Act reached" European Commission. Last modified 23 October 2025. https://digital-strategy.ec.europa.eu/en/news/milestone-strengthening-europes-semiconductor-manufacturing-capacity-under-chips-act-reached*

59 *DigiByte."Semicon Coalition calls for reinforced Chips Act." European Commission. Last modified 29 September 2025. https://digital-strategy.ec.europa.eu/en/news/semicon-coalition-calls-reinforced-chips-act*

60 *European Commission. "Proposal for the Chips Act 2.0."Last modified 3 June 2026. https://digital-strategy.ec.europa.eu/en/library/proposal-chips-act-20*

61 *European Court of Auditors. "The EU's strategy for microchips" Special Report. 2025 pg.7-8.*

62 *Mitchener, Brandon. "Chips Act spurs semiconductor investments in Europe."Science Business. 19 february 2026. https://sciencebusiness.net/news/semiconductors/chips-act-spurs-semiconductor-investments-europe*

63 *Electricity prices are around 18% less, with wages also 41% lower than the eurozone's average. Science Business.* Op. cit.

capabilities and system-level integration - where the highest value is captured[64]. The Draghi Report flags the EU's absence from these highest-value segments amid low-cost Chinese manufacturing competition, calling for a strategy focused on de-risking dependencies and building capability where the EU "has or can develop a competitive advantage"[65]. **Second**, the semiconductor industry faces a severe shortage of skilled labour that capital investment alone cannot solve[66].

3.2 ENERGY SECURITY

3.2.1. A Changing Energy Security Landscape

Article 194 TFEU establishes energy security as a fundamental objective of European Union energy policy alongside market integration, energy efficiency, renewable energy and interconnections[67]. **While energy remains a shared competence, Member States retain sovereignty over their national energy mix within a framework of solidarity.** Initially centred on ensuring secure and affordable energy supplies, this framework has evolved as the transition to climate neutrality has become closely linked to industrial competitiveness, technological leadership and economic resilience[68].

Russia's full-scale invasion of Ukraine in 2022 marked a turning point by exposing the costs of excessive dependence on external suppliers. In response, the European Union strengthened market integration through REPowerEU, coordinated gas storage and enhanced cross-border energy exchanges, significantly reducing reliance on Russian fossil fuels while reinforcing the resilience of the Internal Energy Market. These measures demonstrated the value of coordinated European action in mitigating geopolitical shocks and safeguarding energy supply[69].

Today, **energy security extends well beyond resource availability.** Hybrid attacks on critical infrastructure, disruptions to strategic maritime routes examined later in the supply chain section, intensifying geoeconomic competition through industrial subsidies, export controls and tariffs, together with growing cyber and climate risks, have expanded Europe's vulnerability landscape[70]. Consequently, long-term energy security increasingly depends on resilient infrastructure, secure technologies and competitive industrial capabilities. Ensuring these capabilities requires addressing both immediate supply risks and structural dependencies emerging from the transformation of the energy system. As shown in the previous table these capabilities can be grouped into three mutually reinforcing pillars: secure energy supplies, a resilient electricity system and industrial and technological sovereignty.

3.2.2 Strategic Technologies Supporting Energy Security

Europe's energy transition depends on a technological ecosystem capable of sustaining an increasingly electrified economy. As the Draghi and Letta Reports argue, strategic autonomy requires coordinated investment in technologies that underpin industrial competitiveness, supply-chain resilience and technological leadership[71]. This broader understanding of energy security extends beyond energy availability to encompass resilient infrastructure, strategic technologies and secure value chains[72]. As summarised in the previous table, These technologies perform complementary functions across the energy system but face distinct supply-chain, manufacturing and technology risks.

The first pillar comprises technologies that strengthen secure energy supplies by reducing dependence on imported fossil fuels. Renewable electricity, nuclear energy, renewable hydrogen and biomethane diversify the energy mix, enhance security of supply and support the decarbonisation of hard-to-abate sectors. Yet clean energy technologies remain dependent on global supply chains for critical raw materials, components and manufacturing capacity[73]. Reducing these vulnerabilities

64 *Ceruti, I. and Nardo M. "Semiconductors in the EU. State of Play, future trends and vulnerabilities of the semiconductor supply chain. "JRC Technical Report. 2023. Pg. 8.*

65 *Draghi, Mario. "The Future of European Competitiveness. Part B." European Union. 2024.Pg. 89.*

66 *European Court of Auditors. "The EU's strategy for microchips" Special Report. 2025. Pg. 45.*

67 *Consolidated Version of the Treaty on the Functioning of the European Union (TFEU), Article 194.*

68 *European Commission,* The European Green Deal *(COM(2019) 640); Regulation (EU) 2021/1119 (European Climate Law); Draghi (2024).*

69 *European Commission,* REPowerEU Plan *(COM(2022) 230); IEA,* Energy Security *(2024); European Commission (2022); Eurostat,* EU imports of energy products from Russia.

70 *NATO (Nord Stream sabotage); UNCTAD, Navigating Troubled Waters (Red Sea); IEA, Energy Security (Hormuz); European Commission, European Economic Security Strategy (JOIN(2023) 20); Draghi (2024); European Commission, Annual Single Market and Competitiveness Report 2025; European Commission communications on US tariff measures (2025).; ENISA, Threat Landscape (2024); IEA, Electricity 2024; IPCC AR6 (2023).*

71 *Mario Draghi,* The Future of European Competitiveness: Part A – A Competitiveness Strategy for Europe *(European Commission, 2024); Enrico Letta,* Much More Than a Market: Speed, Security, Solidarity *(European Council, 2024).*

72 *Benjamin K. Sovacool and Michael A. Brown, "Competing Dimensions of Energy Security: An International Perspective,"* Annual Review of Environment and Resources *35 (2010): 77–108.*

73 *Frank W. Geels, "The Multi-Level Perspective on Sustainability Transitions: Responses to Seven Criticisms,"* Environmental Innovation and Societal Transitions *1, no. 1 (2011): 24–40.*

requires expanding European industrial capacity and diversifying access to strategic inputs[74].

The second pillar reinforces the resilience of the electricity system. As electrification expands across transport, industry and heating, modern electricity grids, interconnectors, energy storage and digital

3.2.3 Critical Technologies for a Resilient European Energy System

Security Pillar	Technology	Strategic Contribution	Main Vulnerability
Technology to Strength Energy Supplies	Renewables (wind & solar)	Domestic clean electricity	Weather variability; import dependence
	Nuclear	Dispatchable low-carbon power	Costly; long deployment
	Renewable hydrogen	Decarbonisation of hard-to-abate sectors	High costs; infrastructure needs
	Biomethane	Renewable gas diversification	Limited feedstock
Electricity System	Grids & interconnectors	System integration and cross-border balancing	Permitting; investment gap
	Energy storage	System flexibility and balancing	Battery supply chains
	Digital energy systems	Grid optimisation and cybersecurity	Cyber risks; digital dependence
Sovereignty	Batteries	Electrification and storage	External manufacturing
	Electrolysers	Renewable hydrogen production	Limited manufacturing capacity
	Transformers & power electronics	Grid expansion	Manufacturing bottlenecks
	Wind & solar manufacturing	Clean-tech industrial base	Global competition; concentrated production

Source: Author's own elaboration based on European Commission documents, IEA analyses and academic literature.

energy technologies provide the flexibility and co-ordination needed to integrate growing shares of renewable generation while preserving system reliability and supporting the Internal Energy Market. Yet grid bottlenecks, lengthy permitting procedures and insufficient flexibility remain major constraints. Overcoming these challenges demands coordinated infrastructure investment, improved cross-border planning and deeper market integration[75].

The third pillar strengthens industrial and technological development by expanding Europe's capacity to develop and manufacture strategic technologies. Batteries, electrolysers, semiconductors, grid equipment and renewable manufacturing capabilities reinforce industrial competitiveness and strengthen strategic value chains, consistent with the objectives of the Net-Zero Industry Act, the Critical Raw Materials Act and the European Economic Security Strategy[76]. Technological leadership ultimately depends mostly on the ability to scale production, retain manufacturing capacity and coordinate public and private investment[77].

3.3 MARITIME CONNECTIVITY AS A PILLAR OF EUROPEAN ECONOMIC SECURITY

3.4.1 Why Maritime Supply Chains Matter for Europe

Maritime transport plays a central role in the European economy, carrying more than 70% of the EU's external trade[78] by volume and supporting industrial production, energy imports and access to critical raw materials. As the Union seeks to reduce strategic dependencies through initiatives such as the Critical Raw Materials Act (CRMA) and the RESourceEU Action Plan, **increasing attention has also turned to the resilience of the maritime networks that underpin these supply chains.** In this context, ports are emerging as strategic infrastructure whose security, efficiency and competi-

74 *International Energy Agency,* Energy Technology Perspectives 2023 *(Paris: IEA, 2023).*

75 *European Commission,* Action Plan for Grids, *COM(2023) 757 final; ACER,* Monitoring Report on the Performance of European Energy Markets *(2023).*

76 *European Commission,* Net-Zero Industry Act, *Regulation (EU) 2024/1735; European Commission,* Critical Raw Materials Act, *Regulation (EU) 2024/1252.*

77 *Dani Rodrik, "Green Industrial Policy,"* Oxford Review of Economic Policy *30, no. 3 (2014): 469–491; Mariana Mazzucato,* Mission Economy: A Moonshot Guide to Changing Capitalism *(London: Allen Lane, 2021).*

78 *Eurostat, "Maritime Transport Dominates International Trade," News Articles, September 25, 2025, https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20250925-1*

tiveness have become increasingly relevant to Europe's broader economic security.

Recent disruptions across Europe's principal maritime corridors illustrate how global chokepoints have become a growing source of economic vulnerability. The 2024-2025 Red Sea crisis, triggered by Houthi attacks, caused container traffic through the Suez Canal to collapse, forcing major shipping companies to reroute vessels around the Cape of Good Hope[79], adding 10-14 days to Asia-Europe voyages and contributing to higher freight costs and goods inflation across the Union[80]. Similarly, the 2026 Middle East crisis highlighted the strategic importance of the Strait of Hormuz, where disruptions affected energy supplies and a wider manufacturing value chains by increasing transit times, freight rates and insurance costs. At the same time, Russia's development of the Northern Sea Route, supported by China's Polar Silk Road initiative, is gradually creating **an alternative Eurasian shipping corridor** aligned with their strategic interests[81]. Sanctions, regulatory uncertainty and reputational risks have largely limited European participation, allowing Chinese operators to strengthen their presence in Arctic shipping. Demonstrating that maritime chokepoints increasingly constitute a systemic challenge for European economic security, reinforcing the importance of diversified transport corridors and more resilient supply chains.

3.4.2 Ports as Strategic Assets

Ports have become strategic assets at the intersection of economic security, supply chain resilience, and critical infrastructure protection. As the main gateways for the EU's external trade, safeguarding their competitiveness, security, and operational resilience is essential to strengthening the Union's strategic autonomy.

3.4.3 Chinese Stakes in European Terminals

Chinese logistics entities currently hold stakes in approximately 33 container terminals across the EU, including positions in 20 of the EU's largest ports[82]. **The Port of Piraeus** is the most acute case: the Chinese company COSCO holds a 67% stake in the Piraeus Port Authority[83], making it the only **European port where a Chinese state-owned enterprise exercises control over both the container terminals and the port authority.** Chinese companies maintain stakes in ports across Greece, Malta, France, Italy, Spain, Sweden, and Poland, as well as inland intermodal hubs in Germany, Belgium, and the Netherlands[84], creating structural exposure through access to critical infrastructure and operational data that EU FDI screening frameworks have only recently begun to address.

4 EU MEASURES TO STRENGTHEN MARITIME SUPPLY CHAINS

Regarding supply-chain performance, the EU has strengthened the resilience of critical logistics nodes, particularly ports. The 2026 EU Port Strategy seeks to enhance competitiveness, digitalisation, security and energy resilience through investment in advanced technologies, stricter screening of foreign investment in critical infrastructure and measures to reduce strategic vulnerabilities, contributing to more secure and resilient supply chains[85]. Its effectiveness, however, will depend on consistent implementation. Ensuring that smaller and regional ports are not left behind will be essential to avoid widening disparities across the European port network, while preserving competitiveness as European ports face stricter environmental requirements and increasing competition from North Africa, Turkey and Asia. In this context, the interaction between the EU Emissions Trading System (EU ETS) and the IMO's forthcoming Net-Zero Framework should be carefully assessed to minimise regulatory duplication, traffic diversion and carbon leakage, concerns also raised by

79 *International Transport Forum (ITF), "The Red Sea Crisis: Impacts on Global Shipping and the Case for International Co-operation," Background Paper (Paris: International Transport Forum, 2024)*

80 *Rodríguez, Álvaro, and Santiago Sainz. "Analysis of Maritime Geopolitics on Early 2026: The Red Sea Factor." Geneva: International Sustainable Development Observatory, February 2, 2026. https://isdo.ch/analysis-of-maritime-geopolitics-on-early-2026-the-red-sea-factor/.*

81 *Christian Koch and Amnah Mosly, "The Northern Sea Route: A Viable Alternative?" Gulf Research Center, March 14, 2026, https://www.grc.net/single-commentary/358.*

82 *Konrad Popławski, "Turning the Tide: The US Pushes Back against Chinese Influence in European Ports," OSW Commentary, Centre for Eastern Studies (OSW), March 17, 2025, https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-03-17/turning-tide-us-pushes-back-against-chinese-influence-european*

83 *UNCTAD, "Greece – Greece Privatizes the Port of Piraeus," Investment Policy Monitor, UN Trade and Development, April 8, 2016, https://investmentpolicy.unctad.org/investment-policy-monitor/measures/2882/greece-greece-privatizes-the-port-of-pireus.*

84 *Karin Smit Jacobs, "Chinese Strategic Interests in European Ports," European Parliamentary Research Service (EPRS), At a Glance, PE 739.367 (Brussels: European Parliament, February 27, 2023), https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2023)739367.*

85 *European Commission,* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: EU Port Strategy, *COM(2026) 112 final (Brussels, March 4, 2026).*

the European Sea Ports Organisation (ESPO) and the World Shipping Council (WSC)[86]. Striking the right balance between resilience, sustainability and competitiveness will therefore be central to the strategy's success.

Beyond logistics infrastructure, the **European Maritime Industrial Strategy strengthens Europe's shipbuilding, repair and maritime technology sectors** while recognising that maritime resilience depends on a competitive industrial base as well as secure infrastructure[87]. The strategy promotes the use of EU flags, seeks to address growing shortages of skilled maritime professionals and supports specialised shipbuilding, where Europe retains technological leadership despite the dominance of Asian producers in commercial vessel construction[88]. These measures contribute to reducing strategic dependencies and preserving critical industrial capabilities. Although both initiatives represent a significant step towards a more resilient maritime sector, their success will ultimately depend on sustained investment, effective implementation and the ability to maintain Europe's competitiveness while strengthening its economic security.

4.1 TECHNOLOGY AND ARTIFICIAL INTELLIGENCE

AI has become a strategic enabling technology underpinning Europe's energy systems, semiconductor industry and supply chains[89]. Although AI adoption among European firms has driven roughly 12% of the total recorded productivity increase since 2019"[90], this digital transition remains structurally dependent on foreign-controlled technology layers. By mid-2026, the EU relied on non-European providers, particularly the US, for more than 80% of its key digital products, services, infrastructure and intellectual property. Yet, **the EU's AI framework can be evaluated across three operational exposure vectors.**

Firstly, compute and infrastructure vulnerabilities expose the EU to both the checkpoint effect (sudden denial of computing power) and the panopticon effect (unauthorised data surveillance.) Because massive amounts of European corporate, state, and behavioral data are processed on US-owned hyperscaler servers such as Microsoft Azure and Google cloud, which together monopolise roughly 70% of the European cloud infrastructure market, critical data assets remain exposed to foreign intelligence laws. For example, the extraterritorial reach of the US CLOUD Act allows foreign jurisdictions to compel the disclosure of data managed by these providers, bypassing domestic legal channels because requests can be served to the U.S. corporate entity directly.

Second, material and supply chain vulnerabilities: European algorithmic frameworks rely on physical infrastructure the EU does not control, with a structural dependency on Asian manufacturing ecosystems -most critically Taiwan's fabrication facilities- for training frontier AI models. This is compounded by Nvidia's 85% share of global AI accelerator revenues. The lack of geographic diversification introduces single points of failure, where any regional instability or operational disruption could negatively impact the EU's digital transformation and technological autonomy.

Third, the EU faces a structural deficit in commercial scaling and talent retention. European tech companies face fragmented capital markets and regulatory obstacles that drive an innovation drain, as startups and talent migrate to foreign ecosystems to achieve scale. The Commission identifies a 'valley of death' for European scaleups: between 2008 and 2021, nearly 30% of European unicorns relocated outside the EU[91], undermining its ability to meet the Union's digital decade targets.

To mitigate these vulnerabilities, the EU response strategy has materialised around a regulatory and industrial framework. Proposed by the Commission, the Technological Sovereignty Package deploys three interconnected instruments to rebuild strategic autonomy across the technology stack, defining tech sovereignty as " Europe's ability to act independently in the digital world by developing and controlling key technologies,

86 *World Shipping Council, "WSC Recommends Alignment of EU ETS with IMO Net Zero Framework,"* Regulatory Filings, *July 11, 2025, https://www.worldshipping.org/regulatory-filings/wsc-recommends-alignment-of-eu-ets-with-imo-net-zero-framework ; European Sea Ports Organisation, "ESPO Welcomes the Council Conclusions on the European Ports Strategy: A Solid Basis for Further Discussions," press release, June 9, 2026, https://www.espo.be/news/espo-welcomes-the-council-conclusions-on-the-european-ports-strategy-a-solid-basis-for-further-discussions*

87 *European Commission, "Questions and Answers: EU Ports Strategy,"* European Commission Press Corner, *March 4, 2026, https://ec.europa.eu/commission/presscorner/detail/en/qanda_26_485*

88 *OECD,* Peer Review of the Korean Shipbuilding Industry 2026, *Reviews of Shipbuilding Economies (Paris: OECD Publishing, 2026), https://doi.org/10.1787/c19e0105-en.*

89 *Directorate-General for Energy. 2026. "Commission presents measures to digitalise Europe's energy system while ensuring sustainable digitalisation." Energy - European Commission. https://energy.ec.europa.eu/news/commission-presents-measures-digitalise-europes-energy-system-while-ensuring-sustainable-2026-06-03_en.*

90 *European Investment Bank. 2026. "Investment Report 2025/26: Capitalising on Europe's strengths." https://library.oapen.org/bitstream/handle/20.500.12657/113772/9789286161988.pdf?sequence=1&isAllowed=y.*

91 *European Commission. 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0270.*

data, and infrastructure, while reducing reliance on non-EU providers"[92].

Firstly, the Cloud and AI development act (CADA) targets the infrastructure deficit, establishing a unified regulatory framework to safeguard public order, data processing and sovereign infrastructure development. It mandates that critical administrative data, public infrastructure control systems, and high-security dual-use algorithms must be hosted exclusively within verified European sovereign cloud architectures through a four-tier sovereignty framework. Shielding European public functions from the extraterritorial reach of foreign legislation like the US CLOUD Act.

Second, as CADA's semiconductor complement, the Chips Act 2.0 addresses the hardware fabrication layer. With Europe's manufacturing share still around 10% and leading-edge logic entirely dependent on foreign boundaries, this upgraded framework builds on the original €43 billion initiative framework initiative by shifting the objective from absolute self-sufficiency to structural indispensability, prioritising targeted funding and fast-tracked state aid for European-based advanced packaging and specialised AI accelerator manufacturing facilities among others, ensuring Europe's control over a non-subsitutable node in the global semiconductor value chain[93].

Lastly, at the software and licensing level, the EU Open Source Strategy addresses vulnerabilities down the technology stack by treating open-source architecture as a geoeconomic lever to break foreign technology lock-in. According to the Commission's framework, the strategy secures digital autonomy specifically by "promoting European open alternatives to non-EU proprietary solutions in critical domains"[94]. However, software can't run without a solid physical infrastructure foundation. To protect the open digital frameworks from supply shocks, so that European AI is insulated from foreign resource manipulation, the Strategy (alongside the rest of the Techonolocal Sovereignty Package) operates in tandem with initiatives like the RESourceEU Action Plan.

5

UNDER CONTROL AREAS

The European Union's financial infrastructure constitutes a strategic pillar of its economic security by supporting investment, preserving monetary stability and strengthening the resilience of the Single Market. The euro, the free movement of capital and an integrated regulatory framework have created one of the world's largest financial markets, facilitating cross-border investment while enhancing the Union's capacity to absorb external shocks and finance industrial transformation. **This financial depth provides Europe with a significant comparative advantage in an international environment** where access to capital increasingly shapes competitiveness, technological leadership and strategic autonomy. However, these strengths coexist with structural dependencies that constrain Europe's financial sovereignty.

The Union has developed an integrated financial architecture underpinned by the European Central Bank, which safeguards price and monetary stability and supervises major banks. The Banking Union, with its Single Supervisory Mechanism (SSM) and Single Resolution Mechanism (SRM) enhances financial stability while limiting the risk of cross-border banking crises and reducing costs for taxpayers[95]. The Single Euro Payments Area (SEPA) enables transfers in euros across 41 European countries with the same conditions[96]; and TARGET Services, operated by the ECB, enable money and financial assets to move safely across the euro area. They allow euro area banks and financial institutions to transfer money, settle financial transactions and process instant payments in a safe and efficient way[97].

At the operational level, **the EU remains dependent on non-European financial infrastructures.** Around 61% of retail card payments are processed through US networks such as Visa and Mastercard[98], while cross-border financial messaging relies on SWIFT, whose operations remain closely linked to the dollar-based financial system and the extraterritorial reach of US sanctions. As a result,

92 *European Commission. 2026. "Strengthening Europe's Tech Sovereignty | Shaping Europe's digital future." Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty.*

93 *European Commission. 2025. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52025DC0047*

94 *European Commission. 2026. "The EU Open Source Strategy | Shaping Europe's digital future." Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy.*

95 *CONSILIUM. n.d. "Banking union". Brussels: CONSILIUM – European Council / Council of the European Union. https://www.consilium.europa.eu/en/policies/banking-union/*

96 *European Central Bank. n.d. "Single Euro Payments Area (SEPA)". Frankfurt: European Central Bank. https://www.ecb.europa.eu/paym/retail/sepa/html/index.en.html*

97 *European Central Bank. n.d. "TARGET Services". Frankfurt: European Central Bank. https://www.ecb.europa.eu/paym/target/html/index.en.html*

98 *European Central Bank. 2025.* "Report on card schemes and processors". *Frankfurt: European Central Bank.*

important parts of Europe's payment and financial infrastructure continue to be governed or influenced by actors outside the Union.

Recognising these vulnerabilities, recent reforms increasingly integrate financial infrastructure into the Union's economic security agenda. The Savings and Investments Union seeks to mobilise Europe's abundant private savings towards strategic investment[99], while the European Payments Initiative (EPI) and the proposed digital euro aim to strengthen European payment sovereignty and reduce reliance on external providers selecting 36 payment service providers[100]. In this context, Bizum illustrates Europe's capacity to innovate beyond national markets[101]. Its integration into the EPI creates the potential for a European bank-to-bank payment system capable of competing with Visa and Mastercard, expanding European control over payment infrastructure while reducing strategic dependencies. The strategic relevance of these initiatives extends beyond financial efficiency. The suspension of payment services for International Criminal Court Judge Nicolas Guillou following US sanctions, for issuing arrest warrants against senior Israeli politicians over alleged war crimes in Gaza[102], demonstrated how dependence on foreign-controlled financial infrastructures can amplify the extraterritorial effects of third-country decisions and constrain European institutional autonomy. Strengthening Europe's financial infrastructure therefore reinforces both the Union's economic resilience and its capacity to finance strategic priorities from within the Single Market.

Financial resilience also underpins Europe's broader industrial competitiveness. Despite its leading position in advanced manufacturing, capital goods, clean technologies and chemicals[103], the EU continues to face structural constraints that weaken its industrial performance. High energy costs, fragmented capital markets and an annual investment gap estimated at €750-800 billion limit productivity[104], reduce firms' capacity to scale and hinder investment in strategic technologies such as artificial intelligence and semiconductors[105]. **Recent industrial strategies therefore seek to overcome these bottlenecks** through investment mobilisation, regulatory simplification and reindustrialisation, reinforcing both competitiveness and economic security.

Similarly, **trade policy has evolved from market liberalisation towards strategic risk management.** As the world's largest trading bloc, accounting for approximately 15% of global trade in goods and services and is a key trading partner for more than 80 countries[106], the EU has complemented its extensive network of trade agreements with instruments designed to reduce strategic dependencies and strengthen resilience, including the Foreign Subsidies Regulation, the Carbon Border Adjustment Mechanism, the Anti-Coercion Instrument, and new mechanisms governing technology exports, research security and outbound investment[107]. Together, these measures reflect a gradual shift towards a more assertive geoeconomic policy while preserving the openness of the Single Market.

The Union also retains important strengths in agriculture and pharmaceuticals, although both sectors continue to illustrate the persistence of strategic dependencies. European agriculture remains highly productive and a leading exporter of high-value agri-food products, yet depends heavily on energy, imported protein crops and fertilisers while facing mounting pressures from climate change and rising production costs[108]. Likewise, European Unions' pharmaceutical industry achieved a record trade surplus -exporting pharmaceutical products worth €366.2 billion and importing €145.7 billion, resulting in a surplus of €220.5 billion[109]- confirming Europe's global competitiveness in innovative medicines. Yet its continued dependence on China and India for many active pharmaceutical ingredients (APIS) exposes the sector to persistent supply-chain risks.

99 *European Commission. 2026. "Savings and Investments Union". Brussels: European Commission. https://finance.ec.europa.eu/regulation-and-supervision/savings-and-investments-union_en*

100 *European Central Bank. 2026.* "ECB selects 36 payment service providers to join digital euro pilot". *Frankfurt: European Central Bank.* https://www.ecb.europa.eu/press/pr/date/2026/html/ecb.pr260714~8cd07d9d45.en.html

101 *The EPI is a collaborative effort by 16 major European banks to create a unified digital payment solution aimed at enhancing payment systems across Europe.*

102 *Corlin, Peggy (2026). "US sanctions turn International Criminal Court judge's daily life into a nightmare". Euronews. https://www.euronews.com/my-europe/2026/02/18/us-sanctions-turn-international-criminal-court-judges-daily-life-into-a-nightmare*

103 *Draghi, Mario. 2024.* The Future of European Competitiveness: Report by Mario Draghi. *https://commission.europa.eu/topics/competitiveness/draghi-report_en ; Letta, Enrico. 2024.* Much More Than a Market: Speed, Security, Solidarity. Empowering the Single Market to Deliver a Sustainable Future and Prosperity for All EU Citizens. *https://www.bruegel.org/news/eu-strategic-autonomy-and-industrial-policy.*

104 *Draghi, Mario. 2024.* The Future of European Competitiveness: Report by Mario Draghi. *https://commission.europa.eu/topics/competitiveness/draghi-report_en*

105 *Draghi, Mario. 2024.* The Future of European Competitiveness: Report by Mario Draghi .*https://commission.europa.eu/topics/competitiveness/draghi-report_en*

106 *Eurostat, "International Trade in Goods," Statistics Explained. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=International_trade_in_goods*

107 *European Commission and High Representative of the Union for Foreign Affairs and Security Policy. 2023.* Joint Communication to the European Parliament, the European Council and the Council on a European Economic Security Strategy. *JOIN(2023) 20 final.https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52023JC0020*

108 *European Commission,* EU Agricultural Outlook 2025. *https://agriculture.ec.europa.eu/media/news/eu-agricultural-outlook-2025-35-eu-agriculture-navigates-challenges-while-embracing-opportunities-2025-12-16_en*

109 *Eurostat, "EU Trade in Goods Surplus Reached €147 Billion in 2025," Eurostat News, April 13, 2026, https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260413-1.*

PROPOSALS

Proposal 1

EUROPEAN STRATEGIC ANCHORING AND COHESION MECHANISM (ESAC)

Rationale

The analysis conducted reveals a structural paradox in EU economic security: Europe has the architecture to reduce its strategic dependencies, yet fails to mobilise them coherently, as fragmented instruments and governance structures have themselves become a vulnerability. The proposal argues that addressing this requires not new resources but a new logic for deploying existing ones, treating them as a single coordinate architecture that recognises the complementarity between industrial and regional policy. Consolidating and expanding Europe's own industrial ecosystem, keeping European companies, capital and capabilities within EU strategic boundaries - aligning with the FDI screening framework as a priority within the EU's economic security agenda.

Objectives

The mechanism aims to address four structural problems simultaneously: the difficulty of reaching target market shares in critical sectors, worsened by the lack of a coordinative logic aligning financial flows with strategic priorities; persistent regional disparities, an underused asset and a source of internal fragmentation; the endogenous productivity and digital capability gap - an internal weakness overshadowed by the external dimension of the dependency debate; and the limited direct EU funding committed to priority sectors - illustrated by semiconductors, where only €3.3 billion of the €43 billion Chips Act envelope comes directly from the European Commission.

Governance Architecture

Inspired by the tiered financing logic of EU Cohesion Policy and the ERDF's threshold structure, the mechanism classifies projects and investment flows across three levels, combining a regional classification with a sectoral priority classification.

Under **Threshold 1, less developed and HGP (Highest Growth Potential)** regions receive the most critical sectors and the highest proportional financing, benefiting from competitive labour and energy costs, regulatory agility and untapped growth potential, thereby offering a higher investment return per euro spent, consistent with the principle of sound financial management. The Malta Enterprise model illustrates this approach, with electricity prices approximately 18% below the eurozone average and manufacturing wages 41% lower.

Under **Threshold 2, transitional and intermediate regions** associate with Threshold 1 projects, creating a vertically integrated EU supply chain; and absorb overflow capacity from Threshold 3 companies, acting as a bridge between levels.

Under **Threshold 3 leading European companies** participate through a positive conditionality framework, committing to transfer part of their growth capacity to Threshold 1 facilities in exchange for exclusive access to classified strategic projects reserved for mechanism participants; and a territorial subsidy covering a defined share of capex in Threshold 1 locations, with an equivalent effect to a fiscal advantage. If insufficient, two further layers apply: a dual-level performance incentive, transitional (years 1–3) for reducing EU dependencies, permanent only where matched by internal industrial growth -anchoring the strategy to endogenous growth rather than mere diversification; and free ETS credits linked to secondary installations in Threshold 1 regions, reducing operational costs. This conditionality framework has direct precedent in the EU Chips Act' IPF/OEF designations and operates on a dual classification axis linked to the priority sectors classification (A, B and C), creating favourable conditions for transitioning toward managed interdependence within a defined horizon.

Financing and Implementation

The mechanism relies exclusively on existing European instruments. Horizon Europe supports Threshold 1 anchor facilities and research; the EIB Group

finances Threshold 2 projects and SME participation through its regional investment capacity; while the Savings and Investments Union mobilises private capital for Threshold 3 participants. Together, these instruments provide a coordinated financing architecture without requiring additional EU funding.

Implementation combines European coordination with national delivery. DG GROW and DG REGIO jointly oversee the mechanism, supported by the EIB Group and governance structures modelled on the European Semiconductor Board. Member States remain responsible for implementation, while the Commission coordinates investment flows and monitors compliance through arrangements comparable to the IPF/OEF process. Threshold classifications are reviewed every five years, with interim assessments every three to reflect evolving market conditions and dependency profiles.

By linking industrial investment with territorial development, the mechanism creates a self-reinforcing cycle in which business growth supports regional convergence and strengthens European value chains. Anchoring production in less developed regions improves capital retention, reduces geographic concentration risks and reinforces industrial resilience. Even where full production sovereignty remains unattainable, expanding European manufacturing capacity in critical value chains strengthens the Union's bargaining position and economic security. *Table 3*

Proposal I Theory of Change. ESAC Mechanism at a Glance.

Security Pillar	Technology
Problem	Fragmentation of EU industrial, cohesion, and economic security policy instruments as well as a severe reliance on external homogeneous actors
Intervention	ESAC three-threshold mechanism anchoring critical sectors in less developed regions along with a conditionality enforcement architecture
Actors	European Commission (DG GROW / DG REGIO), EIB Group, Member States, leading European firms (SIU)
Immediate Outcomes (0–18 months)	Commission feasibility assessment; semiconductor sector designated as pilot domain
Structural Outcomes (2–5 years)	Full deployment across critical sectors; threshold classification review cycle established
Expected outcome	Reduced strategic dependencies; territorial convergence; capital retention within EU as well as a boosted bargaining position

Source: Author's own elaboration.

Proposal 2

Europe's economic security increasingly depends on its capacity to manage strategic dependencies across technologies, critical raw materials and global value chains. While existing initiatives, including REPowerEU, the Critical Raw Materials Act, the Chips Act and the European Economic Security Strategy, have strengthened Europe's response to individual vulnerabilities, they remain organised around separate policy frameworks. As strategic dependencies increasingly interact across sectors, fragmented governance limits the Union's ability to identify systemic risks and coordinate coherent policy responses.

Building on the recommendations of the Draghi and Letta Reports, this proposal establishes a **European Strategic Dependency Management Framework (ESDMF)**. Under the Framework of common governance methodology for identifying, assessing and managing strategic dependencies while strengthening coordination across existing industrial, trade and investment policies.

Objectives

The European Strategic Dependency Management Framework (ESDMF) aims to strengthen the European Union's capacity to anticipate, assess and manage strategic dependencies through a common governance methodology that supports more coherent industrial, trade and investment

policymaking. To achieve this objective, the Framework pursues four complementary goals:

- **Develop** a common methodology for identifying and assessing strategic dependencies across technologies, critical raw materials and strategic supply chains.
- **Support** evidence-based decision-making through a shared analytical framework for monitoring systemic vulnerabilities and prioritising strategic action.
- **Embed** diversification within European economic security policy by establishing common benchmarks and investment criteria that reduce excessive concentrations of risk while preserving the openness of the Single Market.
- **Strengthen** policy coherence by aligning existing industrial, trade and investment initiatives within a common strategic approach to dependency management.

Governance Architecture

The ESDMF is organised around three complementary assessments covering **strategic technologies, critical raw materials and strategic supply chains.** Together, they provide a common evidence base for identifying systemic vulnerabilities across the European economy.

Table 5.2.1, : Assessments and purposes

Assessment	Purpose
Strategic Technologies	Prioritise technologies according to strategic relevance, industrial capacity and external dependencies.
Critical Raw Materials	Assess supplier concentration, processing capacity, geopolitical exposure and substitution potential.
Strategic Supply Chains	Identify manufacturing bottlenecks, logistics vulnerabilities and external technological dependencies.

Source: Own elaboration.

Their findings feed into a **European Strategic Dependency Observatory,** which publishes an annual **Strategic Dependency Scoreboard** and continuously monitors Europe's strategic exposure.

Building on the Observatory's assessments, the Commission would establish **Diversification Benchmark**s to identify where policy intervention is needed to reduce excessive concentrations of strategic risk. Although non-binding, these benchmarks would guide industrial, trade and investment policies and support strategic partnerships with trusted partners.

To strengthen investment decisions, the Framework introduces a **Strategic Dependency Risk Score (SDRS)**, combining multiple indicators to identify critical dependencies and provide a common measure of strategic resilience. The SDRS would complement the assessment of existing EU funding instruments and support private investment through a transparent evaluation of strategic risk.The ESDMF would rely on existing European financial instruments, applying a common dependency assessment across mechanisms such as InvestEU, Horizon Europe, the Innovation Fund, IPCEIs and European Investment Bank financing. This common assessment would strengthen investment coordination and progressively integrate the Framework into the European Economic Security Strategy and the European Semester.

Together, these governance and financing arrangements would establish a coherent framework for anticipating and managing strategic dependencies across technologies, critical raw materials and supply chains. By aligning strategic assessment, policy coordination and investment prioritisation, the ESDMF would reinforce industrial competitiveness, strengthen the resilience of the Single Market and support a more secure and strategically autonomous European economy.

Proposal II. Recommendation / Theory of Change.

Assessment	Purpose
Problem	Excessive strategic dependencies combined with fragmented policy coordination increase Europe's exposure to external shocks.
Intervention	Establish a European Strategic Dependency Management Framework to identify, monitor and manage strategic dependencies through a common governance methodology.
Actors	European Commission, Member States, European Investment Bank, EU agencies and the private sector.
Immediate (0–18 months)	Establish the European Strategic Dependency Observatory; publish the first Strategic Dependency Scoreboard; develop Diversification Benchmarks.
Structural (2–5 years)	Integrate diversification into industrial, trade and investment policies; incorporate the SDRS into EU funding mechanisms; strengthen Strategic Partnerships with trusted partners.
Expected outcome	A more resilient, diversified and competitive European economy supported by stronger strategic risk management and more coherent policymaking.

Conclusion

The European Union enters a period of growing geoeconomic competition with considerable economic strengths, yet also with structural vulnerabilities that increasingly shape its economic security. The analysis suggests that strategic dependencies in critical raw materials, digital technologies, semiconductors and clean energy value chains have become a defining feature of the Union's external environment. Geopolitical tensions, supply-chain disruptions and risks affecting critical infrastructure further demonstrate that economic security increasingly depends on resilient industrial capabilities, technological leadership and secure value chains.

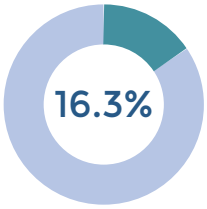
These external challenges are reinforced by persistent internal constraints. Productivity gaps, regulatory fragmentation and the incomplete integration of European capital markets continue to limit Europe's capacity to scale innovation and mobilise investment, despite the strengths of the Single Market and Europe's industrial base. Although recent initiatives have considerably expanded the Union's economic security toolbox, their long-term effectiveness will depend on stronger coordination across industrial, trade, energy, regional and investment policies.

The proposals developed in this policy brief address this governance challenge through complementary approaches. The European Strategic Dependency Management Framework (ESDMF) establishes a common methodology for identifying and monitoring strategic dependencies, strengthening policy coordination across existing EU instruments. Complementing this framework, the European Strategic Autonomy Clustering (ESAC) mechanism aligns industrial, regional and investment policies to reinforce European value chains, strengthen endogenous industrial capacity and support territorial convergence. Together, both proposals demonstrate how existing instruments can operate as a coherent framework for strengthening economic security.

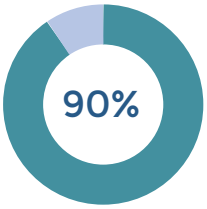
The analysis suggests that **Europe's long-term competitiveness will depend on improving the governance and coordination of existing instruments.** Greater policy coherence would strengthen the resilience of the Single Market, enhance industrial competitiveness and reinforce the European Union's capacity to manage strategic dependencies in an increasingly contested international environment.



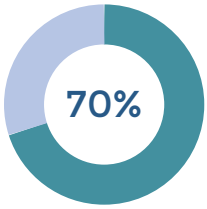
EU GDP — 2ND WORLD ECONOMY



GLOBAL TRADE SHARE



RARE EARTHS DEPENDENCY (CHINA)



CLOUD DEPENDENCY (US)

STRATEGIC DIAGNOSIS: STRENGTHS VS. VULNERABILITIES

✓ STRENGHTS

- **Single Market:** 450M citizens & 26M companies — drives +3–4% GDP and 3.6M jobs.
- **Euro & ECB:** 2nd global reserve currency; eliminates FX risk, buffers external shocks.
- **Trade Powerhouse:** Widest agreement network worldwide; #1 exporter of goods & services.
- **Brussels Effect:** Unmatched capacity to set global industrial & digital standards.

✕ VULNERABILITIES

- **Capital Flight:** 30% of European tech unicorns relocated outside the EU (2008–2021).
- **Regulatory Burden:** ~13,000 regulations (2019–2024) vs. ~3,500 in the US.
- **Productivity Gap:** Labor productivity at only 78% of the US level.
- **Energy Costs:** Electricity prices 2×–3× higher than in the US and China.

PRIORITY SECTORS – EXTERNAL DEPENDENCY BOTTLENECKS

Critical Raw Materials	90%	Rare earths refining & magnets concentrated in China
AI & Cloud Infra	70%	US hyperscalers; 85% GPU share Nvidia; exposed to US CLOUD Act
Energy	2–3×	Electricity prices 2×–3× higher than in the US and China
Supply Chains	67%	Chinese ownership across ~33 EU port terminals — Piraeus at 67%
Semiconductor Fabs	10%	EU global manufacturing share — ASML leads only in EUV equipment

GLOBAL GATEWAY (EU) VS. BELT & ROAD (CHINA)

EU GLOBAL GATEWAY

- €300bn (2021–27), blended public-private finance (EIB/EBRD), conditioned disbursement.
- High standards: environmental, social, transparency & gender safeguards
- Slower rollout due to compliance & co-financing requirements

VS.

CN BELT & ROAD INITIATIVE

- Direct state loans (China Dev. Bank); SOE-led execution
- Non-interference principle; opaque contractual terms
- Ultra-fast, vertically integrated – extraction to transport

Glossary of abbreviations

AI	Artificial Intelligence
CMU	Capital Markets Union
CRM	Critical Raw Material
CRMA	Critical Raw Materials Act
DSA	Digital Services Act
ECB	European Central Bank
EIB	European Investment Bank
EPI	European Payments Initiative
EU	European Union
FDI	Foreign Direct Investment
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
ICC	International Criminal Court
IMF	International Monetary Fund
IPCEI	Important Project of Common European Interest
PM	Prime Minister
SEPA	Single Euro Payments Area
SIU	Savings and Investments Union
SME	Small and Medium Enterprise
SRM	Single Resolution Mechanism
SSM	Singe Supervisory Mechanism
SWIFT	Society for Worldwide Interbank Financial Telecommunication
USA	United States of America
WTO	World Trade Organization

EQUIPO EUROPA



FOCAL CHAPTER 1

HYBRID THREATS AND INTERNAL SECURITY

BLURRED BORDERS, BLURRED ACTOR: HYBRID THREATS AND THE EROSION OF THE RULE OF LAW

Authors: Àlex Atanes Llera, Carolina Cárdenas Torres, Guilherme Ferreira Resende, Álvaro Higuera de Riaño and Andrés Torres Amaro
Reviewers: María Vallejo Fernández and María Villaverde Temes.

Forum on the Future of the EU
EUROPEAN SECURITY in a Changing World

EXECUTIVE SUMMARY

This policy brief examines how hybrid threats are reshaping European security and assesses whether the European Union is equipped to respond without undermining its own democratic foundations. Hybrid campaigns combine cyberattacks, foreign information manipulation and interference (FIMI), economic pressure, legal tools and the instrumentalisation of crises to erode institutional trust, polarise societies and disrupt critical infrastructure, while remaining below the threshold of armed conflict.

The topic is central to European security because these operations strike simultaneously at the political, digital and material underpinnings of the Union. Election interference, disinformation ecosystems such as Doppelgänger and Portal Kombat, repeated GNSS jamming in Eastern Europe and sabotage of Baltic Sea cables illustrate how hostile actors can generate both a crisis of legitimacy and a crisis of functionality inside the EU. In response, the Union has adopted an ambitious regulatory and institutional architecture: the NIS2 and CER Directives, the Digital Services Act and AI Act, the European Democracy Shield, the Cyber Diplomacy Toolbox, Hybrid Rapid Response Teams and a dense web of agencies and networks anchored by ENISA, EU INTCEN, EU-CyCLONe and the Hybrid CoE.

Yet three sets of challenges persist. First, capability gaps: uneven NIS2 implementation, shortages of cyber professionals, dependence on external technology providers and limited operational response capacity constrain the EU's ability to act at speed and scale. Second, coordination and governance gaps: intelligence sharing remains fragmented between EU structures and informal clubs; attribution is slow and politicised; and democratic oversight has not kept pace with expanding hybrid powers. Third, societal vulnerabilities: polarisation, exposure to FIMI and the risk of "emergency governance" threaten democratic and social resilience if responses are opaque or disproportionate.

The brief concludes that the EU has built a strong normative and regulatory shield, but must now close its operational and governance gaps if it is to move from being a primarily regulatory actor to a genuinely integrated security actor capable of withstanding future hybrid shocks.

Keywords

Hybrid threats; European Union internal security; Foreign information manipulation and interference (FIMI); Democratic and societal resilience; Cybersecurity and critical infrastructure; EU–NATO cooperation and governance gaps.

INTRODUCTION

Hybrid threats have become a defining feature of Europe's security landscape. They deliberately exploit the grey zones between peace and war, internal and external security, and physical and digital space, combining cyber operations, disinformation, economic coercion, legal pressure and the instrumentalisation of migration to weaken democratic institutions and societal cohesion. For the European Union (EU), these campaigns are not an abstract risk but **a daily reality that tests the Union's capacity to protect its citizens while remaining faithful to the rule of law and fundamental rights.**

Since 2022, as the war in Ukraine has reshaped Europe's security environment, these campaigns have become larger and more visible. Election-related foreign information manipulation and interference (FIMI), GNSS jamming across Eastern Europe and the Baltic region, and damage to undersea cables in the Baltic Sea show that hostile actors can strike at the political and material foundations of the Union at the same time. In response, **the EU has built a dense regulatory and institutional architecture,** ranging from the NIS2 and CER Directives and the Digital Services Act to the European Democracy Shield and the Hybrid Rapid Response Teams. **Yet this response unfolds in a policy area where key competences remain national**, since Article 4(2) TEU reserves national security to Member States, and where every new protective measure risks stretching legal and constitutional limits.

This policy brief asks whether the EU is structurally prepared to anticipate, deter and respond to hybrid, cyber and sub-threshold threats without eroding the democratic values that constitute its strategic centre of gravity. It argues that the Union has moved decisively from ad hoc crisis management towards a more systematic resilience agenda, but that critical capability and governance gaps still prevent its existing instruments from operating as a coherent whole.

To ensure an evidence-based approach, the analysis draws mainly on EU institutional sources, such as EEAS reports on FIMI, ENISA threat assessments, Council documents and European Parliament research. These are complemented by academic literature and analyses from think tanks and specialised media, which provide the critical perspective a policy brief requires.

T**he brief is structured as follows**. Section 1 sets out an operational definition of hybrid threats, explains why the current moment is critical and examines their anatomy and their impact on the rule of law. Section 2 assesses the EU's preparedness, looking at its resilience to cyber and hybrid attacks, coordination among Member States and persistent capability gaps. Section 3 turns to democratic and social resilience, with a focus on electoral processes, public trust and foreign influence on societies. Section 4 analyses the EU's cognitive response through the FIMI framework and the European Democracy Shield, together with the governance challenges of intelligence-sharing and attribution. Section 5 puts forward two policy proposals, a European Hybrid Response Mechanism (EU-HYBRID) and a European Democratic Resilience Initiative (EDRI). The conclusion then offers an overall assessment.

1

A NEW SECURITY LANDSCAPE

European security is increasingly shaped by threats that do not fit the older distinction between peace and war, internal and external security, or coercion and persuasion. Hybrid threats operate in this space of overlap: they combine cyber operations, disinformation, economic pressure, legal tools, and the instrumentalisation of migration or other crises in order to weaken decision-making, damage institutional trust, and strain democratic governance. The challenge for the European Union is not only that these threats have become more frequent and more sophisticated, but that countering them often requires responses that themselves risk stretching legal and constitutional limits. The result is a security environment in which resilience and rights are no longer separate concerns but part of the same policy problem[1].

1.1 OPERATIONAL DEFINITION OF HYBRID THREATS

For the purposes of this brief, **hybrid threats** are understood as **coordinated campaigns that deliberately combine military and non-military instruments, conventional and irregular tactics, and lawful and unlawful methods to undermine a target's political cohesion, social resilience, or decision-making processes while remaining below the threshold of armed conflict.** This definition is useful because it captures four features that matter for policy: multiplicity, integration, ambiguity, and political utility. Multiplicity refers to the use of several domains at once; integration refers to the sequencing of those measures; ambiguity concerns attribution and legality; and political utility refers to the fact that the goal is not necessarily military victory, but advantage gained through destabilisation[2].

This operational definition is important for two reasons. First, it avoids reducing hybrid threats to any single tool, such as cyberattacks or disinformation, which would obscure their cross-domain nature. Second, it helps distinguish hybrid campaigns from ordinary political competition or isolated incidents of crime and sabotage. The policy implication is clear: if the phenomenon is cross-domain and coordinated, then the response must also be coordinated, legally grounded, and institutionally disciplined[3].

1.2 WHY NOW

The present moment is significant because several trends have converged since 2024. First, foreign information manipulation and interference have become more visible and more systematic, including during electoral periods. The (European External Action Service) EEAS has described FIMI as a persistent feature of the current environment and has mapped its digital infrastructure, showing how foreign actors use multiple platforms, hidden networks, and coordinated channels to spread disinformation and polarisation[4]. **Second**, cyber pressure on critical infrastructure remains high, with EU threat reporting continuing to identify public administration, transport, finance, digital infrastructure, and manufacturing as exposed sectors[5]. **Third**, the EU itself has moved from treating hybrid threats as an episodic issue to framing them as a standing security problem requiring coordination across institutions, sectors, and levels of government[6].

These developments place the Union at a pivot point. **On one side** lies a more capable and more coherent resilience agenda, built around preparedness, early warning, and coordinated response. **On the other** lies a securitised reflex that can expand executive power without necessarily improving democratic protection. The issue is therefore not simply whether the EU can react, but whether it can do so in a way that preserves the rule of law while addressing threats that deliberately exploit its openness[7].

1.3 A SHORT ANCHOR CASE

A useful way to anchor the discussion is to look at the convergence of two recent patterns in the

1 European Parliament, EU Response to Hybrid Threats (Brussels: European Parliamentary Research Service, 2026).

2 European External Action Service, Countering Hybrid Threats (Brussels, 2024); Council of the European Union, "Hybrid Threats," 2025, https://www.consilium.europa.eu/en/policies/hybrid-threats/.

3 Luigi Lonardo, "EU Law Against Hybrid Threats: A First Assessment," European Papers 6, no. 2 (2021): 513–532.

4 European External Action Service, 2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI) (Brussels, 2025); European External Action Service, "Information Integrity and Countering Foreign Information Manipulation and Interference," 2026, https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en.

5 European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2025 (Heraklion: ENISA, 2025).

6 European Parliament, EU Response to Hybrid Threats.

7 European Parliament, EU Response to Hybrid Threats; Council of the European Union, "Hybrid Threats."

EU security environment: election interference through disinformation and cyber pressure on critical infrastructure. In the electoral domain, the EEAS has documented foreign information manipulation and interference as a recurrent feature of the current threat landscape, while the European Parliament has similarly described disinformation and cyberattacks as central tools used by external actors to shape public opinion and political outcomes[8]. In parallel, EU-level cyber and security reporting continues to show that critical sectors such as public administration, transport, digital infrastructure, finance, and manufacturing remain highly exposed to ransomware, phishing, DDoS activity, and espionage[9].

Taken together, **these developments show that hybrid threats operate across the political and material foundations of the Union.** They do not only distort information; they also target the systems that make democratic life possible in practice. When disinformation coincides with pressure on infrastructure, institutions face not one crisis but two: a crisis of legitimacy and a crisis of functionality. That combination is precisely what makes hybrid threats so difficult to contain through ordinary sectoral responses[10].

1.4 THREAT ANATOMY

1.4.1 Conceptual framing of hybrid threats

Hybrid threats should be understood as political strategies rather than isolated incidents. They belong to a broader field of state competition, but they are distinct from conventional military aggression because **they are designed to remain below the threshold of open conflict.** Their central objective is to produce strategic effects through ambiguity, disruption, and delay. For that reason, a useful way to analyse them is to examine intent, means, and effects together. Intent reveals the political purpose behind the campaign; means identify the instruments used; and effects show how institutions, publics, and decision-making systems are being stressed[11].

This conceptual framing matters because weak definitions create weak policy. If every disruptive event is treated as a hybrid threat, the concept becomes too broad to be useful. If, by contrast, coordinated interference is treated as a series of unrelated incidents, states will consistently underestimate the scale of the challenge. The purpose of the concept is therefore to distinguish a patterned campaign from a random disturbance, and to make visible the links between domains that security institutions often still treat separately[12].

1.4.2 Blurred borders: internal vs external, physical vs digital

One of the most important features of hybrid threats is that they blur the boundaries that once structured European security. Information operations and cyber intrusions now target domestic political processes directly, while migration crises and economic coercion can be used to generate instability inside the Union. As a result, **the traditional separation between internal security and foreign policy is becoming harder to sustain.** Measures that once belonged mainly to police, courts, and electoral authorities now intersect with diplomacy, sanctions, resilience planning, and cyber defence[13].

The same blurring is visible in the relation between physical and digital space. Social media, cloud infrastructure, and platform ecosystems allow hostile narratives or disruptive content to spread at high speed across borders, often before authorities can verify attribution or scope. This creates a policy problem that is both operational and legal: who should lead, what legal basis should be used, and how can rights be protected while the state responds to a suspected foreign interference campaign? The answer cannot be purely national, because the threat itself is transnational; but neither can it be purely supranational, because many of the relevant powers still remain with member states[14].

1.4.3 Blurred actors: state, non-state, public, private

Hybrid threats also blur the identity of the actors involved. They are often carried out by combinations of state intelligence services, private contractors, criminal networks, sympathetic media outlets,

8 European External Action Service, 2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI); European Parliament, EU Response to Hybrid Threats.

9 ENISA, ENISA Threat Landscape 2025.

10 European Parliament, EU Response to Hybrid Threats; European External Action Service, 2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI).

11 Lonardo, "EU Law Against Hybrid Threats," 515–518.

12 European Parliament, EU Response to Hybrid Threats.

13 Council of the European Union, "Hybrid Threats"; European Parliament, EU Response to Hybrid Threats.

14 Lonardo, "EU Law Against Hybrid Threats," 518–523.

and domestic intermediaries. This fragmentation serves several strategic purposes: it increases deniability, makes attribution more difficult, and allows hostile influence to move through jurisdictions and sectors that are not designed to work together. The result is a networked form of coercion in which formal responsibility is dispersed even when political direction remains clear[15].

Private actors are particularly important here. Technology platforms, data brokers, and analytics firms now shape information flows, visibility, and amplification at a scale that was once associated with public authorities. When those systems are manipulated, or when they are used to amplify divisive content, the line between commercial behaviour and political interference becomes harder to draw. This is one reason why hybrid threats are not only a matter of defence or intelligence; they are also a matter of regulation, oversight, and democratic accountability[16].

1.5 RULE-OF-LAW EROSION IN THE EU

The rule-of-law dimension is central, not secondary. Hybrid threats exploit weak institutions, but they can also encourage political responses that weaken those institutions further. Where judicial independence is fragile, media ecosystems are concentrated, or oversight bodies are under-resourced, societies become more vulnerable to external manipulation and internal distortion. At the same time, the language of hybrid threat can be used domestically to justify exceptional measures: broader surveillance, restrictions on independent media, accelerated procedures that reduce judicial scrutiny, or vague references to foreign influence that chill legitimate civic activity[17].

This creates a feedback loop. Weak rule-of-law systems are more vulnerable to hybrid pressure, and securitised reactions to hybrid pressure can further weaken rule-of-law safeguards. The danger is not only immediate political manipulation but the gradual normalisation of exceptional governance. For that reason, **the question for the EU is not simply how to defend against hybrid threats, but how to do so without allowing the response to become part of the erosion it seeks to prevent**[18].

2 TO WHAT EXTENT IS THE EU PREPARED

2.1 HOW RESILIENT IS THE EU TO CYBER AND HYBRID ATTACKS?

The European Union has become significantly more resilient to cyber and hybrid threats, particularly since Russia's full-scale invasion of Ukraine in 2022, which highlighted the need to protect critical infrastructure, democratic institutions, and digital networks. In response, the EU has strengthened its regulatory framework through measures such as the Digital Services Act (DSA), the NIS2 Directive, the Foreign Information Manipulation and Interference (FIMI) Toolbox, and the Rapid Alert System, improving its ability to detect, monitor, and respond to increasingly sophisticated threats.

These measures have been reinforced by a stronger institutional cybersecurity architecture. Agencies such as ENISA support Member States through technical expertise, coordinated response mechanisms, and cybersecurity exercises, while new resilience requirements have been introduced for critical sectors including energy, transport, telecommunications, healthcare, and finance[19]. European policy has also shifted from prevention towards resilience, recognising that cyber and hybrid attacks cannot always be avoided and that essential services must recover rapidly. This approach relies on close cooperation between public authorities and private operators, which own much of Europe's critical digital infrastructure[20].

The EU has also improved its ability to identify and expose hostile activities through enhanced intelligence sharing and coordinated monitoring. Incidents such as the GPS jamming and spoofing

15 European External Action Service, 2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI); European External Action Service, "Information Integrity and Countering Foreign Information Manipulation and Interference."

16 European Parliament, EU Response to Hybrid Threats; Lonardo, "EU Law Against Hybrid Threats," 523–526.

17 European Parliament, EU Response to Hybrid Threats; European External Action Service, 2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI).

18 European External Action Service. 2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI). Brussels: European External Action Service, 2025. https://www.eeas.europa.eu/eeas/2024-report-eeas-activities-counter-foreign-information-manipulation-and-interference-fimi_en

19 European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. Heraklion: ENISA, 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

20 European Commission. The NIS2 Directive. Accessed August 1, 2026. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

affecting Eastern Europe and the Baltic region in 2025 demonstrated both the growing sophistication of hybrid threats and the value of existing monitoring systems[21].

Despite this progress, **important challenges remain.** Cybersecurity capabilities and resources continue to vary across Member States, limiting the EU's capacity for rapid operational response. At the same time, hybrid threats have become increasingly sophisticated, combining cyberattacks with disinformation, sabotage, and political interference. Russian campaigns such as Doppelgänger and Portal Kombat illustrate how foreign actors exploit Europe's information environment to undermine public trust and democratic processes. Overall, although the EU is considerably better prepared than in previous years, its resilience remains dependent on stronger coordination and more uniform capabilities across Member States[22].

2.2 ARE MEMBER STATES EFFECTIVELY COORDINATED?

Although the European Union has significantly strengthened its resilience against cyber and hybrid threats, this resilience ultimately depends on effective coordination among Member States. Common legislation, specialised agencies, and shared cybersecurity policies can only be effective if national authorities exchange information rapidly, coordinate operational responses, and act collectively during cross-border crises. Consequently, **assessing EU resilience also requires evaluating the effectiveness of its coordination mechanisms.**

Coordination has improved considerably over the last decade as cyberattacks, foreign interference, and hybrid threats have become increasingly frequent and sophisticated. Recognising that no Member State can respond effectively in isolation, the EU has developed a broad network of cooperation involving national governments, EU institutions, specialised agencies, intelligence services, and international partners[23].

Key developments include the adoption of the NIS2 Directive, which harmonises cybersecurity standards and promotes cooperation in risk management and incident reporting, together with the growing role of ENISA and the EEAS in providing technical expertise, threat analysis, and operational support. Information sharing has become faster and more systematic, while large-scale exercises such as Cyber Europe have strengthened preparedness by testing communication channels, crisis-management procedures, and cross-border cooperation[24].

These coordination mechanisms have been tested during major crises. Russian disinformation campaigns such as Doppelgänger and Portal Kombat triggered coordinated responses through the EU Rapid Alert System, while suspected sabotage of telecommunications cables and energy infrastructure in the Baltic Sea reinforced cooperation in intelligence sharing, critical infrastructure protection, and the EU–NATO partnership.

Despite these advances, important limitations remain. Significant disparities in cybersecurity capabilities, technical expertise, financial resources, and institutional maturity continue to affect the effectiveness of collective responses. Differences in national legal frameworks, administrative procedures, and political decision-making often delay operational coordination during rapidly evolving crises [25].

Recent events, including interference in Romania's 2024 presidential elections and repeated GPS jamming incidents affecting civil aviation in the Baltic region, demonstrated that although information sharing has improved considerably, transforming shared intelligence into rapid and coordinated operational action remains difficult. Interoperability also continues to be a weakness, as effective cooperation depends on compatible communication systems, common technical standards, and harmonised crisis-management procedures across Member States[26].

Overall, **coordination among Member States is considerably stronger than before Russia's invasion of Ukraine.** The EU has strengthened information sharing, cybersecurity cooperation, crisis preparedness, and the protection of critical infrastructure, while cooperation with NATO has

21 European Union Aviation Safety Agency (EASA), Safety Information Bulletin No. 2022-02R4: Global Navigation Satellite System (GNSS) Outage and Alterations Leading to Communication / Navigation / Surveillance Degradation (Cologne: EASA, 2026). https://ad.easa.europa.eu/ad/2022-02R4

22 European Parliament. EU Response to Hybrid Threats. Brussels: European Parliamentary Research Service, 2026. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2026)789374

23 European Parliamentary Research Service (EPRS), EU Preparedness Union Strategy: Strengthening Europe's Civilian and Military Readiness (Brussels: European Parliament, 2026), https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/789374/EPRS_BRI%282026%29789374_EN.pdf

24 European Parliamentary Research Service (EPRS). EU Preparedness Union Strategy: Strengthening Europe's Civilian and Military Readiness. Brussels: European Parliament, 2026. https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/789374/EPRS_BRI%282026%29789374_EN.pdf

25 UAV Defence. "Europe's GPS Jamming Crisis: What 430,000 Incidents Mean for Critical Infrastructure Operators." UAV Defence, 2025. https://uav-defence.com/europes-gps-jamming-crisis-what-430000-incidents-mean-for-critical-infrastructure-operators

26 European External Action Service (EEAS). 2025 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI). Brussels: EEAS, 2026. https://www.eeas.europa.eu/eeas/2025-report-eeas-activities-counter-foreign-information-manipulation-interference-fimi_en

reinforced collective resilience[27]. Nevertheless, disparities in national capabilities and persistent operational challenges continue to limit the speed and coherence of collective responses, highlighting the need for further harmonisation, investment, and institutional integration effectively to respond effectively to increasingly sophisticated crises, particularly in operational response, technological sovereignty, and strategic autonomy. **One of the EU's main weaknesses is its limited operational response capacity.** Although measures such as the NIS2 Directive have improved prevention and preparedness, crisis management still relies largely on national authorities, often resulting in fragmented responses to large-scale cyber or hybrid attacks.

2.3 WHAT ARE THE CAPABILITY GAPS?

The previous sections have shown that the European Union has significantly strengthened its resilience against cyber and hybrid threats. However, important capability gaps continue to limit its ability to prevent, deter, and respond effectively[28]. **The EU also faces difficulties in attribution and deterrence, as hybrid threats operate below the threshold of conventional conflict, allowing hostile actors to exploit the so-called "grey zone"** with limited consequences[29].

Significant disparities in cybersecurity capabilities among Member States further reduce the effectiveness of collective responses. Differences in technical expertise, financial resources, and institutional capacity, combined with a shortage of qualified cybersecurity professionals, continue to hinder the development of a consistent level of preparedness across the Union[30].

Another major challenge is Europe's technological dependence. The EU relies heavily on private companies (many based outside Europe) for cloud computing, digital communications, software, and online platforms that play a key role in countering disinformation and protecting digital infrastructure[31]. This dependence limits European technological sovereignty and creates vulnerabilities if geopolitical tensions or supply chain disruptions affect access to essential technologies.

The protection of critical infrastructure remains a priority, as sectors such as energy, transport, telecommunications, healthcare, and financial services have become key targets of hybrid attacks. At the same time, emerging technologies, particularly artificial intelligence, are transforming the threat landscape faster than security and regulatory frameworks can adapt. This reflects **a broader challenge: European democracies continue to rely on rules designed for the analogue era** while confronting digital manipulation, foreign interference, and rapidly evolving online threats[32].

Although the EU has strengthened its resilience and coordination mechanisms, it still depends on NATO, particularly the United States, for cyber defence, intelligence, and military deterrence. Greater strategic autonomy will be essential to respond effectively to future cyber and hybrid threats.

3 DEMOCRATIC AND SOCIAL RESILIENCE IN THE EU AND ITS MEMBER STATES

As it has been seen in the sections above, hybrid threats are of the utmost importance to the Union and its Member States. For that reason, attention must also be paid to the democratic and social resilience against them, as both are cornerstones of the EU itself[33]. **Democratic resilience can be defined as "the ability of a political system to react to challenges so as to maintain democratic features"**[34], and while there is no global common definition for societal resilience, it refers to the ability of individuals, communities and institutions to withstand, adapt to, and recover from shocks and long-term pressures while maintaining essential functions[35]. Both types are interconnected and even overlap on different aspects. To understand to

27 North Atlantic Treaty Organization (NATO). NATO–EU Cooperation on Cyber Defence. Brussels: NATO. https://www.nato.int/cps/en/natohq/topics_78170.htm

28 European Parliament. EU Response to Hybrid Threats. Brussels: European Parliamentary Research Service, 2026. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2026)789374

29 European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. Heraklion: ENISA, 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

30 European Commission, Impact Assessment Report Accompanying the Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148 (SWD(2020) 345 Final) (Brussels: European Commission, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020SC0345

31 European External Action Service (EEAS), Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI) (Brussels: EEAS, 2026), https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

32 ABC. "Rumanía: ¿cómo se defiende la democracia analógica frente a la desinformación digital?." ABC, July 20, 2026. https://www.abc.es/internacional/rumania-defiende-democracia-analogica-desinformacion-digital-20260717005811-nt.html

33 European Union. 2025. "Aims and Values." European Union. 2025. https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en .

34 Richard Youngs & Elene Panchulidze (2026) Democratic resilience in Europe – and its limits, Democratization, 33:3, 589-608, DOI: 10.1080/13510347.2025.2581838

35 Redecker, C., Galariotis, I., Cataldo, F., Montanari, E. and Cappannini, A., Understanding societal resilience in Europe Evidence from statistical analysis in a polycrisis context, Publications Office of the European Union, Luxembourg, 2026, https://data.europa.eu/doi /10.2760/9452918, JRC145222 .

what extent the EU is resilient enough and where we can find capability gaps to be developed, we will assess what has been done in three main areas: the protection of the electoral processes, the protection and promotion of public trust and social cohesion, and the protection of both these aspects of foreign influence from third actors.

3.1 PROTECTION OF ELECTORAL PROCESSES

The main competences on the protection of the different electoral processes lay on the national authorities, who are in charge of ensuring that elections are fair and free from interference and manipulation[36], always in accordance with European and national law. To do so, different layers of capabilities and regulations are needed.

The first one is to have strong cybersecurity capabilities, which are key to protect the integrity of the voting process, to defend democratic institutions from foreign interference and safeguarding public trust. In this domain, the EU has approved two main pieces of regulation: the CER and NIS-2 Directives. Both of them aim at "reducing vulnerabilities and strengthen resilience of critical and digital infrastructure against online and offline threats"[37], as defined by the European Commission. The first one, the Directive on the Resilience of Critical Entities (CER Directive), aimed to strengthen the resilience of critical infrastructure before threats such as terrorist attacks, insider threats or sabotage. To do so, it makes Member States adopt a national strategy and carry out risk assessment every four years to identify the critical entities that provide essential services, with those entities having to identify, at the same time, risks that could significantly disrupt the provision of their services. Member States must also take appropriate measures and notify of incidents. Moreover, these Directives establish rules for identification of critical entities of European significance, meaning those that provide essential services to six or more Member States. Then, the NIS-2 Directive expands the sectors and types of critical entities, such as public electronic communications networks and services or data centre services[38].

The second one is to monitor and prevent, in a coordinated way, foreign interference in elections. To achieve so, the European Commission presented in 2025 the European Democracy Shield[39] (EDS). In one of the three pillars that the EDS is built upon, the one on safeguarding the integrity of the information space, the focus is put on countering foreign information manipulation and interference and disinformation campaigns. At the end of the day, what the Democracy Shield does is to build on existing legislation, like the Digital Services Act or the Artificial Intelligence Act. Furthermore, the EDS establishes the creation of a European Centre for Democratic Resilience. The Centre brings together expertise and capacities across participating Member States, EU Candidates, potential candidates and EU institutions, among many actors[40]. On top of that, there is also the European Cooperation Network on Elections, which brings together representatives of Member States' authorities with competence in electoral matters and creates a space for "concrete and practical exchanges on a range of topics relevant to ensuring free and fair elections, including data protection, cyber-security, transparency and awareness raising"[41]. From this framework, documents like the Election Integrity Checklist, a document aiming to be a reference to develop "national operational checklists [on the quality of elections] (...) in line with international standards"[42], have emerged. Lastly, it is also worth mentioning that efforts on combating disinformation and fake news campaigns have also been done, such as the already mentioned Artificial Intelligence Act, or the brand-new X (former Twitter) account French Response, run by the French Ministry of Foreign Affairs and used to counter disinformation.

The third layer is ensuring transparency throughout the process and protecting journalists, whistleblowers and civil society organisations (CSOs). In this case, we find important European regulation, such as the DSA, which imposes obligations on large online platforms to mitigate systemic risks like disinformation[43]; the Regulation on Transparency and Targeting of Political Advertising, which

36 "Free and Fair Elections." n.d. European Elections 2024: All You Need to Know. https://elections.europa.eu/en/free-fair-elections/.

37 "European Commission, "Critical Infrastructure Protection & Resilience – CER and NIS-2 Directives Enter into Force to Strengthen EU's Resilience," Europa, 2022, https://ec.europa.eu/newsroom/cipr/items/764849/en

38 European Commission, "Critical Infrastructure Protection & Resilience," 2022.

39 The abbreviated form 'EDS' will be used from now on.

40 European Commission, "Democracy and Electoral Rights," last modified 2026, https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights_en

41 European Commission, "European Cooperation Network on Elections," European Commission, accessed June 19, 2026, https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/european-cooperation-network-elections_en

42 Directorate-General for Justice and Consumers, European Commission, Checklist on the Integrity of Elections (Brussels: European Commission, June 6, 2025), https://commission.europa.eu/publications/checklist-integrity-elections-and-risk-management-matrix_en

43 European Commission, "Digital Services Act," Shaping Europe's Digital Future, accessed June 19, 2026, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

enhances accountability in how political ads are delivered and funded[44]; the European Media Freedom Act[45], which aims to protect media independence and pluralism; or the second pillar of the Democracy Shield, which is dedicated to strengthening democratic institutions, free and fair elections and free and independent media[46].

In conclusion, although the main competence falls on the Member States, the EU is using its regulatory power to create stronger capabilities and common guidelines that can help achieve a stronger resilience of the European electoral process, while at the same time it is also creating forums for national authorities to share their experience and practices in this domain.

3.2 PROTECTING PUBLIC TRUST AND SOCIAL COHESION

According to the spring Eurobarometer, 51% of Europeans trust the EU, three percentage points higher than in autumn 2025. The highest-trusting country is Portugal, at 66%. This is the highest overall level of trust in the Union since 2007. The age group that trusts the most in the EU is the young one: 59% of Europeans aged between 15 and 24 say they trust the European Union. Moreover, trust in the Commission is also at its highest point since 17 years ago, also standing at 51%. Thus, it is fair to argue that trust in the European project is in a positive level, although it is not short of challenges[47].

The EU is currently living in what some authors have described as polycrisis: a complex and interconnected set of crisis occurring simultaneously, often amplifying and influencing one another[48]. This state can lead to political paralysis, underperformance and loss of legitimacy in view of the European public. In this situation, societal resilience is essential to address the polycrisis, and the Joint Research Centre (JRC) of the European Commission has found that engagement and participation of civil society are key in strengthening it. For that, the JRC proposes to engage communities, address perceptions of insecurity and respond to citizens' expectations[49]. Moreover, in a research report of Eurofound on social cohesion and inclusive participation in a polarised Europe, they concluded that political engagement reduces polarisation on political institutions as "active interest in and attachment to one's country have been shown to have a considerable impact in depolarising citizens, at least with regard to trust in institutions"[50]. Therefore, doing the same at European level can have the same effects on EU institutions, and the EU is well aware of it.

That is why there are initiatives like the Citizens' Panels, where 150 randomly-chosen representative groups of citizens from all Member States debate key EU proposals[51]; the European Youth Event, an event designed for young Europeans to listen to experts and policy-makers as well as to give their opinion on legislation and the state of current affairs[52]; or the European Citizens' Initiative, which is an instrument through which Europeans can call the Commission to propose new laws[53]. Nevertheless, there are also critics on the quality and impact of this engagement, as, for example, the Citizens Take Over Europe organisation denounced that the Citizens' Panel on the next EU budget only briefly touched on the implementation of the specific recommendations the Panel participants co-created, and stayed for the most part far from the practical level. Instead, the session allowed [EU officials] to present the [budget] on their own terms. Thus, it is important for more engagement opportunities to appear, for more budget to be allocated to them, but also to make sure that they have a real impact in EU policy and decision-making.

When it comes to what polarizes European citizens, as described by a publication of the European Commission's Directorate-General for Migration and Home Affairs, the media plays a key role. It consists not only of the traditional one (print, radio or TV), but also of the new media (social media or mobile apps). The publications point out that where someone gets their information can significantly impact their understanding of events and

44 European Commission, "Transparency and Targeting of Political Advertising," Democracy and Electoral Rights, accessed June 19, 2026, https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/transparency-and-targeting-political-advertising_en

45 European Commission, "European Media Freedom Act," Shaping Europe's Digital Future, accessed June 19, 2026, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/european-media-freedom-act_en

46 European Commission, "Democracy and Electoral Rights," last modified 2026,

47 European Commission, "New Eurobarometer Survey Shows Record High Trust in the European Union," press release IP/24/6126, November 29, 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6126

48 European Commission, Joint Research Centre, "Unraveling the Polycrisis with Foresight and Innovation," EU Policy Lab, March 26, 2025, https://policy-lab.ec.europa.eu/stories/unraveling-polycrisis-foresight-and-innovation-2025-03-26_en

49 Joint Research Centre, "Rethinking Societal Resilience in a Time of Polycrisis," European Commission, September 1, 2025, https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/rethinking-societal-resilience-time-polycrisis-2025-09-01_en

50 Eurofound (2025), Social cohesion and inclusive participation in a polarised Europe, Publications Office of the European Union, Luxembourg.

51 European Commission, "European Citizens' Panels," Citizens' Engagement Platform, accessed June 21, 2026, https://citizens.ec.europa.eu/european-citizens-panels_en

52 European Parliament, "About Us," European Youth Event, accessed June 21, 2026, https://european-youth-event.europarl.europa.eu/en/about-us. (european-youth-event.europarl.europa.eu

53 European Commission, "European Citizens' Initiative," European Citizens' Initiative, accessed June 21, 2026, https://citizens-initiative.europa.eu/index_en

their perception of society. Thus, it is a tool for polarization, especially in an increasingly fragmented media environment in which disinformation has become a persistent policy concern[54].

A way through which the EU is fighting against polarization is, again, through the European Democracy Shield. It dedicates its third pillar to boosting societal resilience and citizens' engagement, which puts the focus on supporting education and the development of skills, as well as promoting citizens' participation and engagement in democratic life. Consequently, the strategy of the EU to protect public trust and social cohesion is clear: fight against polarisation through promoting citizens' engagement with politics, combining it with education on the matter as well as with regulation on social media transparency, which will be commented on in the latest section.

In that way, **Europe must pay attention to the levels of polarization, which is nowadays the biggest threat to social cohesion and public trust.** Most of this polarization happens through social media content, and as Arancha González Laya puts it: "it is in the EU where the democratic erosion provoked by algorithms and social media has the gravest effect, more than in the Member States, due to the fragility of its institutional legitimacy"[55]. As seen, the best way to fight it is through engaging with civil society and making them part of the decision and policy-making processes as much as possible, if not, it risks losing its legitimacy and letting their citizens fall in the loop of tailor-made content by foreign algorithms.

3.3 PROTECTING FOREIGN INFLUENCE ON SOCIETIES

Foreign influence operations have become a growing threat to democratic societies across the European Union. Foreign actors can exploit digital platforms to spread disinformation, manipulate public opinion, increase political polarization, and weaken trust in democratic institutions and European values. In response, the European Union has developed several instruments to strengthen democratic resilience. Again, the European Democracy Shield seeks to protect democratic processes from foreign information manipulation and interference by improving the integrity of the information environment and strengthening societal resilience. At the same time, the Digital Services Act (DSA) requires very large online platforms and search engines to assess and mitigate systemic risks, including those linked to disinformation, and to increase transparency around content moderation and advertising. The Artificial Intelligence (AI) Act separately imposes transparency obligations on providers and deployers of certain AI systems, requiring that AI-generated or manipulated content, including deepfakes, be clearly labelled as such[56]. Member States have also introduced national initiatives, such as the already mentioned "French Response" X account, which actively counters disinformation campaigns through strategic communication and public engagement[57].

4 THE EU'S COGNITIVE RESPONSE: FIMI AND THE DEMOCRACY SHIELD

In March 2015, the EEAS set up the East StratCom Task Force to counter foreign disinformation campaigns targeting the EU, marking **the beginning of its strategic communication response to foreign interference.** The EEAS did not formalize this activity under the FIMI (Foreign Information Manipulation and Interference) framework until its 2021 Annual Report, and published its first dedicated FIMI Threat Report in February 2023. From this pivotal moment, what tended to be innocuously deemed as "fake news" by institutional structures and actors began to be recognised as a challenge arising at the nexus of "national security, information integrity, democratic governance, and hybrid warfare"[58]. With annual reports by the EEAS since 2023, there's a steady advancement of its methodological approach, with each edition introducing a new set of updated institutional perspectives and tools[59].

54 European Commission, Directorate-General for Migration and Home Affairs, "Media and Polarisation in Europe: Strategies for Local Practitioners to Address Problematic Reporting," May 31, 2023, https://home-affairs.ec.europa.eu/whats-new/publications/media-and-polarisation-europe-strategies-local-practitioners-address-problematic-reporting-may-2023_en

55 González Laya, Arancha. Solos en el mundo: Estados Unidos amenaza, Rusia hace la guerra, China reconstruye un imperio... ¿Y Europa? Barcelona: Arpa Editores, 2026.

56 European Commission. 2026. "Countering Information Manipulation." European Commission. https://commission.europa.eu/topics/countering-information-manipulation_en

57 Le Monde. 2026. "French Response, the Foreign Ministry's X Account for Trolling Disinformation." January 18, 2026.

58 Cyber Risk GmbH. n.d. EU Foreign Information Manipulation and Interference (FIMI). Disinformation.ch. https://www.disinformation.ch/EU_Foreign_Information_Manipulation_and_Interference_(FIMI).html.

59 Strategic Communications (2026). Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). EEAS. March 17, 2026.

4.1 CORE TOOLS AND ACTORS

At a time when channels of connection and information are increasingly disrupted and exploited, new frameworks are proposed for traversing these channels[60], through the lens of the DISARM framework. It outlines key practices to tackle such malicious activities and establish a common understanding of these issues through the joint sharing of findings and insights from the government, media, civil society, and academics[61], providing a foundation for the adoption of efficient countermeasures[62]. Communicatively, the EEAS employs its Strategic Communication Task Forces, a.k.a. stratcom, as counterresponses to disinformation and as promoters of Brussels' institutional communication, activities across a diverse array of themes. These StratCom Task Forces mainly operate across distinct geographical areas, with the East Stratcom Task Force (Eastern Partnership and Central Asia) being highlighted for its EUvsDisinfo project, aimed to further anticipate, tackle and counter ongoing disinformation operations against the EU and its Member States, launched by Moscow[63]. Also, the EDS proposes 50 action points, organized around three priority areas, with its first pillar—safeguarding the integrity of the information space—being emphatic regarding the regulatory involvement of the DSA and its crisis protocol in the face of transnational information operations on platforms with more than 45 million monthly users within the EU, i.e., VLOPs. These must comply with EU legal obligations and diagnose potential systemic risks associated with their platforms. Afterwards, they must also report to the Commission and proceed to implement actions or modifications to reinforce their platforms against these risks and potential others[64]. Inside this framework, the former Code of Practice on Disinformation became the Code of Conduct on Disinformation under the DSA on 1 July 2025. It remains based on voluntary commitments for signatories, but for participating VLOPs and VLOSEs, compliance with its commitments now serves as a relevant benchmark for assessing risk-mitigation obligations under Article 35 DSA, and those commitments are subject to independent auditing[65].

4.2 DEMOCRATIC PARADOX AND EXAMPLES

Returning to the initial notion presented in this section, the use of manipulative tactics characterises FIMI. Tackling them demands structures, policies, actions that may have repercussions on national institutions and systems within the EU, when and how it's employed in less than normalised circumstances in democratic governance. In 2024, Romanian intelligence reported a coordinated TikTok campaign involving around 25,000 accounts that promoted Călin Georgescu's candidacy amid concerns over foreign interference. The Constitutional Court subsequently annulled the presidential election, citing irregularities affecting the electoral process. In March 2025, Georgescu's candidacy in the rerun was separately rejected by the electoral authorities, a decision upheld by the Constitutional Court. While companies owning the social media platforms have acknowledged this concerning manipulation and asserted that they have effective security measures in place to prevent illicit usage of their services[66], these events still unfolded after EU officials have warned and held discussions with these VLOPs regarding potential abuses and to share their input on risk assessment and mitigation measures taken within the context of this election[67]. It has also become more reported in the past few years that subsea cable incidents in the Baltic Sea region have become far more frequent. Episodes such as the Balticonnector gas pipeline, two subsea cables that connect Finland and Estonia, and a subsea data cable that connects Sweden and Estonia were all damaged in October 2023. With inspections later showing that both a Chinese ship and a Russian cargo ship were present at impacted areas[68]. Two institutionally distinct approaches towards this regional issue take the main stage. In Brussels, the Commission allocated nearly €6 million to build two Regional Cable Hubs, including one in the Baltic Sea, and €40 million to expand European capabilities for repairing undersea communication cables. These actions are framed by the EU Action Plan on Cable Security, which aims to strengthen the security and resilience of the continent's submarine data

60 Community of Democracies (2025). Counter-FIMI Toolbox for Diplomats.

61 ResPublica. n.d. Anatomy of Information Warfare: DISARM Framework. ResPublica. https://respublica.edu.mk/resursi/anatomy-of-information-warfare-disarm/?lang=en.

62 European External Action Service (EEAS) (2024). Report on Foreign Information Manipulation and Interference (FIMI) Threats

63 About EUvsDisinfo. n.d. EUvsDisinfo. https://euvsdisinfo.eu/about/.

64 European Commission (2026c). DSA: Very Large Online Platforms and Search Engines. Directorate-General for Communications Networks, Content and Technology. 2026. https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops.

65 European Commission (2025). Commission Endorses the Integration of the Voluntary Code of Practice on Disinformation into the Digital Services Act. European Commission. February 13, 2025. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_505.

66 Quaritsch, Luise (2026). How Has the DSA Performed in Protecting Election Integrity? DSA Observatory. March 4, 2026. https://dsa-observatory.eu/2026/03/04/how-has-the-dsa-performed-in-protecting-election-integrity/.

67 European Commission (2024). Commission Convenes Very Large Online Platforms and Search Engines to Monitor Election Readiness for the Romanian Presidential and Parliamentary Elections. European Commission. 2024. https://digital-strategy.ec.europa.eu/en/news/commission-convenes-very-large-online-platforms-and-search-engines-monitor-election-readiness.

68 JSIS, University of Washington (2025). Baltic Sea Undersea Cable Security.

and power cables and enhance the shared capacity to track, detect, and respond to threats targeting critical undersea infrastructure. In addition, a Baltic Sea Regional Hub project, which was granted €2.5 million, is supported to bolster surveillance and response systems in the region, reinforce national and cross-border security operations facilities, optimise information exchange platforms, and enhance the means to mitigate threats against regional critical marine infrastructure[69]. In Helsinki, a new military operation to improve the defence of critical infrastructure in the Baltic Sea region was revealed by NATO. Named the "Baltic Sentry", it is an effort to increase NATO's military footprint in this maritime space and to strengthen the capacity of allies to react to attempts of disruption in this area. Additionally, it was emphasised that NATO would collaborate with its allies to incorporate national surveillance capabilities in order to enhance the capacity to defend this critical undersea infrastructure[70]. In 2025, Poland reported multiple instances of Russian drones invading its airspace. They claimed that this was the first time that the country's sovereignty had been infringed on this magnitude since Russia's invasion of Ukraine. Poland went on to claim that the invasion constituted a serious breach of EU and NATO airspace and that Moscow's conduct brought the entire region nearer to warfare than it had in the modern past. Warsaw invoked Article 4 of the North Atlantic Treaty, which permits NATO countries to communicate their security issues with the North Atlantic Council and could culminate in a NATO unified decision or action[71].

As broadly exemplified by these cases, as hybrid threats become more sophisticated, governments increasingly resort to emergency-style measures to protect electoral integrity, critical infrastructure, and national security. These developments lead to a public dilemma, in which, democracies are meant to safeguard open societies against risks and threats perpetrated by actors who deliberately exploit this openness; while acting with opaque, exceptional mechanisms risks eroding the public perception of the legitimacy of democratic institutions. There's a further concern that repeatedly employing these exceptional responses may lead to a normalisation of an "emergency governance" that fundamentally erodes democratic functioning.

3.3 GOVERNANCE: INTELLIGENCE, INFORMATION-SHARING AND LEGAL CHALLENGE

From Capability Gaps to Governance Gaps

Section 2 of this Brief catalogues what the European Union (EU) materially lacks in operational terms. Yet the EU's most persistent vulnerability is not a deficit of instruments — it is a deficit of use. The EU possesses intelligence structures, information-sharing networks, and legal frameworks that constitute a formidable architecture on paper. **What it lacks is the political will and institutional infrastructure to make those tools operate as a coherent system rather than as parallel, voluntary, and often incompatible national arrangements**[72]. Three interlocking failures explain this gap: a fragmented intelligence architecture that discourages genuine sharing; operational networks that are technically capable but unevenly implemented; and a legal framework that simultaneously chills cooperation and fails to provide meaningful democratic oversight.

4.3.1 Intelligence Architecture: Design vs. Reality

The EU's principal analysis hub is the Single Intelligence Assessment Capacity (SIAC) — combining EU INTCEN (civilian analysis) and the EU Military Staff Intelligence Directorate (EUMS INT)[73]. The Hybrid Fusion Cell, embedded within INTCEN since 2016, was designed as the EU's dedicated hybrid threat sharing platform.

The structural problem: INTCEN does not collect intelligence independently — it analyses only what Member States choose to submit[74]. In May 2025, INTCEN's own chief acknowledged publicly that EU intelligence "services were not visible enough"[75]: a candid admission of systematic under-supply. Meanwhile, the most operationally relevant intelligence sharing in Europe happens through informal intergovernmental clubs that sit entirely outside the EU's legal and accountability framework *Figure 1 (next page)*:

69 European Commission (2026a). "Commission Funds First Regional Cable Hubs and Launches €40 Million Call for Cable Repair Capacity." European Commission. 2026. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1429.

70 NATO (2025). NATO launches 'Baltic Sentry' to increase critical infrastructure security. North Atlantic Treaty Organization. https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security

71 Security Council Report (2025). Emergency Briefing on Drone Incursion into Poland.

72 Gruszczak, A. (2026, January 21). Prospects for stronger and more effective European intelligence cooperation. Centrum Balticum.

73 EEAS. (2024). EEAS replies to additional questions — 2024 discharge. European External Action Service.

74 Gruszczak, A. (2026, January 21).

75 Euronews. (2025, May 22). EU intelligence centre chief: We know what Russia is doing.

Forum	Members	Nature	Democratic Oversight
Club de Berne	All EU states + UK, Norway, Switzerland	Intelligence directors' forum	None — classified
Counter Terrorism Group (CTG)	Same 30 states as the Club de Berne	Real-time operational exchange	No EU parliamentary mandate
Paris Group	Number of participating governments not independently verifiable in public sources	Security coordinator network	No secretariat, no formal acts

Figure 1: Informal Intelligence Cooperation Forums in Europe (Own elaboration)

The Hybrid Fusion Cell — the official EU mechanism — runs in parallel to these clubs without formal integration, creating duplicative analytical tracks and information asymmetries that hostile actors are well positioned to exploit.

4.3.2 Structural Limits and Legal Tensions

Two constraints systematically prevent genuine information flow through official EU channels:

Article 4(2) TEU[76] declares national security the sole responsibility of each Member State — but the Court of Justice has made clear that measures adopted in the name of national security do not automatically fall outside the scope of EU law when they impose obligations on private actors, as illustrated by the Privacy International judgment (C-623/17)[77]. The EU's 2025 internal security strategy, ProtectEU, reflects this ceiling: it calls on Member States to "enhance" — not mandate — intelligence sharing with SIAC[78].

Capacity asymmetries concentrate the most sensitive sharing in exclusive small-group formats, implicitly excluding lower-capacity Member States and reinforcing a self-perpetuating trust gap[79].

On the legal side, the GDPR, the Law Enforcement Directive (LED) and the ePrivacy Directive 2002/58/EC – following the 2025 withdrawal of the proposed ePrivacy Regulation –[80] establish partly overlapping data-protection regimes for cross-border processing of personal data in the EU, which can complicate the design of information-sharing arrangements between authorities and private operators in areas that fall within the scope of EU law, while activities conducted purely for national security purposes remain largely governed by domestic regimes. Legal uncertainty about which framework governs a given exchange disincentivises proactive disclosure to EU bodies — a documented chilling effect on operational cooperation[81].

4.3.3 The Attribution Gap in Practice

The most consequential governance failure is the attribution–unanimity trap. Imposing restrictive measures under the EU's sanctions framework against Russia's destabilising activities requires unanimous agreement in the Council[82], through a Common Foreign and Security Policy decision based on Article 29 TEU. This transforms every attribution decision into a diplomatic negotiation where any state with ties to the attributed actor can delay or dilute the response[83].

The consequences are empirically documented. Russian hybrid operations in Europe nearly quadrupled between 2023 and 2024 — from 13 to 44 documented incidents according to Leiden University research; the IISS confirmed the same fourfold increase[84]. Since October 2023, at least 11 undersea cables in the Baltic Sea region have been damaged, with several incidents raising concerns about deliberate sabotage and links to vessels associated with Russia or its shadow-fleet ecosystem. The EU Hybrid Rapid Response Teams (HRRTs), established by the General Affairs Council in May 2024, are a genuine step forward — and their first deployment to Armenia ahead of the June 2026 elections demonstrates operational feasibility[85]. However, they have not been activated in any major infrastructure sabotage incident affecting EU Member States since their creation[86].

76 European Union, Consolidated Version of the Treaty on European Union, OJ C 202, 7 June 2016, art. 4(2).

77 Court of Justice of the European Union (2020). Privacy International, C-623/17, Judgment of 6 October 2020

78 European Commission. (2025). ProtectEU — European internal security strategy (IP/25/920).

79 Gruszczak, A. (2026, January 21).

80 European Parliament (2025). Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy). Legislative Train. https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform

81 Institut Jacques Delors. (2025). A new internal security strategy for the European Union.

82 The Council of the European Union is the institution in which member state ministers meet by policy field; it should not be confused with the European Council, the summit of Heads of State or Government, or with the Council of Europe, a separate non-EU organisation composed of 46 member states.

83 SWP. (2021). Attribution: A major challenge for EU cyber sanctions. Stiftung Wissenschaft und Politik.

84 The Parliament Magazine. (2025, January 20). How Russia's hybrid war is undermining Europe; Intellinews. (2025). Russian sabotage operations in Europe almost quadrupled in 2024, IISS says.

85 EEAS. (2026). EU action on countering hybrid threats.

86 Council of the EU. (2024). Operational guidance for EU Hybrid Rapid Response Teams (ST-15660-2024).

4.3.4 Five Governance Gaps

Gap	Core Problem	Evidence	Democratic Oversight
Attribution gap	No rapid, credible EU-level attribution mechanism	11+ Baltic Sea cables damaged; attribution of individual incidents remains contested	None — classified
Funding gap	Fragmented, project-based resilience financing	HRRTs exist but undeployed in major MS incidents	No EU parliamentary mandate
Civil–military gap	No EU equivalent to NATO Article 4 rapid consultation	Poland 2025 drone crisis handled exclusively via NATO	None — classified
Intelligence-sharing gap	SIAC under-supplied; sensitive sharing in unaccountable clubs	INTCEN chief: "services not visible enough"	No EU parliamentary mandate
Democratic gap	Oversight and judicial review lag behind expanding hybrid powers	No EP oversight of INTCEN; CTG outside EU legal framework	No secretariat, no formal acts

Table 2: Key gaps in the EU's hybrid resilience architecture (Own elaboration)

PROPOSALS

Proposal 1

EUROPEAN HYBRID RESPONSE MECHANISM (EU-HYBRID)

Problem Statement

The EU has built extensive regulatory tools against hybrid threats, yet it still operates as a fragmented set of parallel systems rather than a unified security actor. SIAC depends on voluntary Member State submissions rather than independent collection, and its own chief admitted in May 2025 that EU intelligence "services were not visible enough". The most significant intelligence exchange in Europe still happens through informal, non-EU forums — the Club de Berne, the Counter Terrorism Group, and the Paris Group — none of which carry any EU accountability structure, creating duplicative tracks that hostile actors can exploit.

Attribution is the clearest symptom of this fragmentation. Because sanctions require Council consensus, any state sympathetic to an accused actor can delay or dilute a response. Russian hybrid operations against Europe nearly quadrupled between 2023 and 2024, from 13 to 44 documented incidents. Since October 2023, at least 11 undersea cables in the Baltic Sea region have been damaged, with several incidents raising concerns about deliberate sabotage and links to vessels associated with Russia or its shadow-fleet ecosystem. The Hybrid Rapid Response Teams created in 2024 were successfully deployed to Armenia ahead of its 2026 elections but have never been activated for a major infrastructure sabotage incident inside a Member State.

Two structural constraints compound this. Article 4(2) TEU reserves national security to Member States, and the 2025 ProtectEU strategy only "encourages" rather than mandates intelligence sharing with SIAC. Different EU and national data-protection regimes may apply depending on the nature and purpose of the information exchange, adding legal complexity to cross-border cooperation. Uneven NIS2/CER implementation and a shortage of qualified cyber professionals further limit collective operational capacity.

The Proposal

EU-HYBRID would establish a permanent EU Hybrid Response Mechanism integrating SIAC, ENISA, EU-CyCLONe, the Hybrid Fusion Cell, and Member States under common attribution, crisis-response, and coordination protocols. It absorbs functions currently split between informal clubs and official channels into one accountable structure, and introduces a pre-agreed, evidence-based attribution procedure to reduce coordination delays under the Council's unanimity rule that have previously hindered collective responses to incidents such as the Baltic Sea sabotage.

In the immediate phase (0–18 months), a fast-track attribution protocol would let a defined group of Member States, supported by SIAC and ENISA, issue provisional EU-level attribution within days. Common hybrid crisis procedures would standardise how EU-CyCLONe, the Hybrid Fusion Cell, and national centres classify and escalate incidents. Annual EU-wide exercises, building on the Cyber Europe framework, would stress-test these procedures. A real-time information-sharing platform would formalise intelligence flows currently trapped in informal clubs, and an EU preparedness dashboard would give a shared picture of exposure across energy, transport, telecoms, finance, and digital infrastructure.

In the structural phase (2–5 years), a Permanent Operational Coordination Centre would sit above SIAC, ENISA, and EU-CyCLONe with authority to trigger cross-domain response once attribution thresholds are met. Standing Hybrid Response Teams — a professionalised evolution of the HRRTs — would be pre-authorised for deployment inside Member States, not only abroad. Harmonised crisis management would align national legal and administrative procedures, and integrated cyber, intelligence, and infrastructure coordination would link ENISA, SIAC, and CER functions into a single operational chain instead of three regulatory silos.

Expected Outcome

By integrating existing but disconnected structures under common protocols, EU-HYBRID would produce faster, more coordinated, and more credible EU responses, reducing the operational fragmentation documented across attribution, intelligence-sharing, and civil-military coordination, and strengthening deterrence against actors currently exploiting the EU's slow, consensus-bound response.

Theory of change: European Hybrid Response Mechanism (EU-HYBRID) (own elaboration)

Assessment	Purpose
Problem	Fragmented operational response, slow attribution, uneven implementation of EU cybersecurity frameworks, and limited coordination prevent the EU from acting as a coherent hybrid security actor.
Proposal	Establish a permanent EU Hybrid Response Mechanism integrating SIAC, ENISA, EU-CyCLONe, the Hybrid Fusion Cell and Member States under common attribution, crisis-response and coordination protocols.
Actors	European Commission · EEAS · SIAC · ENISA · EU-CyCLONe · Member States
Immediate (0–18 months)	Fast-track attribution protocol · Common hybrid crisis procedures · Annual EU-wide exercises · Real-time information sharing · EU preparedness dashboard
Structural (2–5 years)	Permanent Operational Coordination Centre · Standing Hybrid Response Teams · Harmonised crisis management · Integrated cyber, intelligence and infrastructure coordination
Expected outcome	Faster, coordinated and credible EU responses, reducing operational fragmentation and strengthening deterrence against hybrid threats.

Proposal 2

EUROPEAN DEMOCRATIC RESILIENCE INITIATIVE (EDRI)

Problem Statement

The EU's exposure to hybrid threats is not only operational but societal. Foreign Information Manipulation and Interference (FIMI) has evolved since the EEAS first documented it in 2015 into a systematic, cross-platform phenomenon, with annual EEAS reporting since 2023 tracking increasingly sophisticated coordinated behaviour. Romania's 2024 presidential election illustrates the risk. Declassified intelligence and subsequent investigations pointed to a large-scale, Moscow-linked influence campaign on TikTok and other platforms amplifying far-right candidate Călin Georgescu, reportedly involving tens of thousands of coordinated accounts. In December 2024, the Constitutional Court annulled the first round and ordered the electoral process to be rerun in order to safeguard the legality and integrity of the vote, and in March 2025 the electoral authority refused Georgescu's candidacy for the new election, a decision the Court later upheld. In parallel, the European Commission opened formal proceedings against TikTok for suspected breaches of the Digital Services Act related to election-integrity risk assessment in the Romanian vote, underlining that existing instruments such as the DSA obligations for Very Large Online Platforms and the (then) Code of Practice on Disinformation can trigger ex post compliance scrutiny but do not guarantee real-time prevention of foreign information manipulation.

Beneath FIMI lies technological dependence: the EU relies heavily on non-European providers for cloud computing, digital communications, and the platforms that carry both public discourse and disinformation countermeasures, limiting sovereignty and creating exposure to geopolitical or supply-chain disruption. This is compounded by a shortage of qualified cybersecurity professionals across Member States, constraining the EU's collective capacity to build and defend digital infrastructure.

Social cohesion adds a third dimension. While EU trust stands at its highest level since 2007 — 51%, rising to 59% among 15–24-year-olds — the Union is navigating what researchers describe as a "poly-

crisis," capable of producing political paralysis and legitimacy loss if unaddressed. The European Parliament identifies media fragmentation and algorithm-driven content as central drivers of polarisation, and civil society groups have criticised engagement mechanisms like the Citizens' Panels for stopping short of genuine influence over EU decision-making. Left unaddressed, this combination risks becoming self-reinforcing, as eroding public trust weakens the resilience needed to resist further interference.

The Proposal

EDRI brings together four workstreams pursued separately today — FIMI response, technological sovereignty, cyber skills development, and democratic resilience — under the European Democracy Shield (EDS), which the Commission presented in 2025 around three pillars: safeguarding the information space, strengthening democratic institutions, and boosting societal resilience. EDRI links these through shared governance, so election protection, platform regulation, workforce development, and technological investment reinforce one another instead of operating in isolation.

In the immediate phase (0–18 months), election FIMI monitoring extends the EEAS's DISARM-based tracking into a standing, election-cycle capability, learning from the gap exposed in Romania's 2024 vote. Stronger DSA cooperation tightens the crisis-protocol mechanism for Very Large Online Platforms, moving beyond voluntary compliance. An EU Cyber Skills Programme addresses the professional shortage with ENISA, while mapping critical technological dependencies builds the evidence base the EU currently lacks. Media literacy initiatives build on the EDS's societal resilience pillar.

In the structural phase (2–5 years), a European Cybersecurity Academy converts the Skills Programme into a durable talent pipeline. Sovereign cloud, AI, and semiconductor investment, channelled through the European Investment Bank and the private sector, reduces technological dependence and gives the EU room to act independently of external providers. The European Centre for Democratic Resilience, operational since February 2026, becomes the long-term institutional home for this work, and a long-term cyber workforce strategy keeps skills investment aligned with an evolving threat landscape.

Expected Outcome

EDRI is designed to build democratic resilience and technological autonomy simultaneously, so societal preparedness against FIMI is reinforced by, rather than dependent on, external technology providers, giving the EU long-term capacity to withstand hybrid threats without resorting to emergency-style governance.

Theory of change: European Democratic Resilience Initiative (EDRI) (own elaboration)

Assessment	Purpose
Problem	Foreign information manipulation, technological dependence, social polarisation and cybersecurity skills shortages continue to undermine democratic resilience and strategic autonomy.
Proposal	Launch an integrated European Democratic Resilience Initiative combining FIMI response, technological sovereignty, cyber skills development and democratic resilience under the European Democracy Shield.
Actors	European Commission · EEAS · ENISA · European Parliament · Member States · EIB · Private sector
Immediate (0–18 months)	Election FIMI monitoring · Stronger DSA cooperation · EU Cyber Skills Programme · Mapping critical technological dependencies · Media literacy initiatives
Structural (2–5 years)	European Cybersecurity Academy · Sovereign cloud, AI and semiconductor investment · European Centre for Democratic Resilience · Long-term cyber workforce strategy
Expected outcome	Greater democratic resilience, technological autonomy, societal preparedness and long-term capacity to withstand hybrid threats.

Conclusion

The European Union has stopped improvising against hybrid threats: in barely half a decade it has built a formidable normative shield — NIS2, CER, the DSA, the AI Act, the European Democracy Shield, ENISA, EU-CyCLONe and the Hybrid Rapid Response Teams — that positions it, on paper, among the world's best-equipped actors. **Yet the problem is no longer regulatory but operational:** the Union has the tools but not always the wiring to make them act as one system rather than twenty-seven uncoordinated national responses.

The evidence is telling. The rise in documented Russian hybrid operations from 13 to 44 incidents between 2023 and 2024, the sabotage of Baltic Sea cables without joint attribution, and the largely national handling of the 2025 drone incursion into Poland all point to the same structural brake: unanimity on sanctions, ORCON limits on shared intelligence, and Article 4(2) TEU shielding national security from Brussels' reach.

This exposes the Union's defining paradox. The more forcefully it responds to disinformation and interference, the greater the risk of drifting into "emergency governance" that erodes the very democratic values it seeks to defend. Citizen trust in the EU, now at its highest since 2007, is an asset the Union cannot afford to spend carelessly.

The EU is therefore no longer a purely regulatory actor on hybrid threats, but remains structurally constrained by Member States' primary responsibility for national security under Article 4(2) TEU and unanimity in sanctions. Within those limits, improving attribution, strengthening structured intelligence-sharing, and reducing technological dependence is **the real test of whether Brussels can turn its legal architecture into operational strength.**

IS THE EUROPEAN UNION STRUCTURALLY PREPARED FOR HYBRID THREATS?

Assessing resilience, identifying gaps, and strengthening Europe's collective response.

1 THE CHALLENGE: WHAT ARE HYBRID THREATS?

CYBER ATTACKS
Disrupting critical systems, stealing data, or damaging infrastructure.

DISINFORMATION & INFORMATION MANIPULATION
Spreading false narratives to divide societies and undermine trust.

PROXY ACTORS & NON-STATE ACTORS
Using third parties or extremist groups to achieve strategic objectives.



ECONOMIC COERCION
Applying economic pressure or weaponising interdependence to gain political leverage.

POLITICAL INTERFERENCE
Influencing elections, policies, or public opinion to serve external interests.

MILITARY & PARAMILITARY PRESSURE
Using intimidation, intimidation and threats below the threshold of armed conflict.

OBJECTIVE: Hybrid threats exploit vulnerabilities across multiple domains simultaneously to achieve strategic advantage while remaining below the threshold of traditional conflict.

2 THE EU RESPONSE: A MULTI-LAYERED ARCHITECTURE

PREVENT
Build resilience and deter threats

- Strengthen societal resilience
- Protect critical infrastructure
- Secure cyberspace and data
- Counter disinformation
- Promote strategic communication

DETECT & ANALYSE
Anticipate and understand hybrid activities

- EU Hybrid Fusion Cell
- Intelligence sharing (INTCEN, Europol)
- ·Early warning systems
- Situational awareness
- Horizon scanning and analysis

RESPOND & RECOVER
Act collectively and strengthen recovery

- Coordinate EU response (HYBRID Toolbox)
- Diplomatic and economic measures
- Support to affected Member States
- ·Strategic communications
- Lessons learned and adaptation

3 CAPABILITY AND GOVERNANCE GAPS

FRAGMENTED RESPONSIBILITIES
Overlap and gaps across EU institutions and between Member States.

INFORMATION SHARING DEFICITS
Uneven intelligence sharing and classification barriers limit collective awareness.

CAPABILITY INEQUALITIES
Wide disparities in national capacities and access to critical technologies.

LEGAL AND POLICY CONSTRAINTS
Complex rules and limited mandates slow down decision-making.

RESOURCE AND SUSTAINABILITY GAPS
Insufficient funding, personnel, and long-term strategic investment.

KEY GAP: EU intelligence analysis relies on information voluntarily shared by Member States.

HYBRID ACTIVITY
13 → 44
Documented Russian hybrid operations in Europe, 2023–2024.

BALTIC SEA
11
Cables severed or damaged since October 2023.

PUBLIC TRUST
51%
Europeans who trust the EU — highest level since 2007.

4 REAL-WORLD EXAMPLES

ROMANIA (2024)
Large-scale cyber campaign targeting government networks. Attribution to Russian state-linked actors.

✓ Evidence:
CERT-RO, 2024 public report.

BALTIC SEA (2023–2024)
Multiple incidents of submarine cable damage in the Baltic Sea impacting connectivity and critical infrastructure.

✓ Evidence:
ENISA Threat Landscape 2024.

POLAND (2025)
Disinformation campaign ahead of elections using AI-generated content to manipulate public opinion.

✓ Evidence:
NASK, 2025 report.

5 POLICY RECOMMENDATIONS

STRENGTHEN COLLECTIVE RESILIENCE
- Invest in critical infrastructure
- Enhance cyber resilience
- Build societal resilience and media literacy

IMPROVE COORDINATION AND INFORMATION SHARING
- Empower the EU Hybrid Fusion Cell
- Enhance intelligence sharing
- Clarify roles and streamline decision-making

INCREASE INVESTMENT ANDCAPABILITIES
- Close capability gaps
- Support innovation and R&D
- Ensure sustainable funding and skilled personnel

CONCLUSION: A STRONGER EUROPE, TOGETHER: Hybrid threats will persist and evolve. The EU's strength lies in unity, resilience, and decisive action. By closing structural gaps and investing in collective capabilities, Europe can safeguard its values, security, and democratic way of life.

Glossary of abbreviations

AI Act	Artificial Intelligence Act
CER Directive	Critical Entities Resilience Directive
CFSP	Common Foreign and Security Policy
CSIRTs	Computer Security Incident Response Teams
CTG	Counter Terrorism Group
DDoS	Distributed Denial of Service
DISARM	Disinformation Analysis & Risk Management framework
DSA	Digital Services Act
EASA	European Union Aviation Safety Agency
ECCC	European Cybersecurity Competence Centre
ECI	European Citizens' Initiative
ECN on Elections	European Cooperation Network on Elections
EDS	European Democracy Shield
EEAS	European External Action Service
EMFA	European Media Freedom Act
ENISA	European Union Agency for Cybersecurity
EP	European Parliament
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network
EU INTCEN	European Union Intelligence and Situation Centre
Eurojust	EU Agency for Criminal Justice Cooperation
Europol	EU Agency for Law Enforcement Cooperation
EUvsDisinfo	Flagship project of the EEAS East StratCom Task Force that collects, analyses and exposes disinformation campaigns targeting the EU and its Member States
FIMI	Foreign Information Manipulation and Interference
Frontex	European Border and Coast Guard Agency
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
HRRTs	Hybrid Rapid Response Teams
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
JRC	Joint Research Centre
LED	Law Enforcement Directive
NATO	North Atlantic Treaty Organization
NIS2	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union
ORCON	Originator Control
SIAC	Single Intelligence Assessment Capacity
TEU	Treaty on European Union
VLOPs	Very Large Online Platforms Platforms with more than 45 million monthly users in the EU


EQUIPO
EUROPA



FOCAL CHAPTER 2

TECHNOLOGY AND FUTURE SECURITY, THE FUTURE OF EUROPEAN SECURITY

EMERGING TECHNOLOGIES, CONNECTIVITY AND STRATEGIC DEPENDENCIES

Authors: Celia Camuñas, Yusara El Aitour Maslouhi, Wissame El Mouden and África Itziar Casas.
Reviewers: María Vallejo Fernández and María Villaverde Temes.

Forum on the Future of the EU
EUROPEAN SECURITY in a Changing World

EXECUTIVE SUMMARY

This paper examines how emerging technologies are reshaping European security, focusing on three connected issues: the growing role of artificial intelligence and other emerging technologies in security and defence; the increasing strategic importance of secure and resilient digital connectivity and the European Union's difficulty in reducing critical technological dependencies. The analysis covers how AI, quantum technologies, autonomous systems and advanced connectivity are transforming security and economic activity; why telecommunications networks and digital infrastructure have become critical assets for European resilience; and why the EU remains dependent on third countries for infrastructure, data, semiconductors, digital platforms and other critical technologies. These dependencies create vulnerabilities ranging from cyberattacks and network disruption to supply-chain risks and reliance on foreign suppliers.

This topic is highly relevant for European security because recent conflicts in Ukraine, Gaza, and Iran have shown that AI now plays a central role in modern warfare. At the same time, these conflicts have revealed how heavily Europe relies on American cloud providers, Asian semiconductor manufacturers, and foreign platforms to operate its own defence systems. This is not only an economic issue, but a political one: whoever controls the servers, chips, and data ultimately holds power over Europe's most critical systems, particularly in times of crisis.

Three main challenges emerge from this analysis. First, an industrial challenge: Europe has strong research talent and solid regulation, but struggles to turn innovation into globally competitive products, mainly due to fragmented funding and limited investment. Second, a legal and governance challenge: the AI Act excludes AI systems used exclusively for military, defence or national-security purposes from its scope. This leaves those uses outside the AI Act's regulatory framework and raises questions about accountability and the interaction between national rules, EU defence policy and international lawThird, a strategic challenge: rather than pursuing full self-sufficiency, the EU must balance security, economic competitiveness, and democratic values — a balance the EU has increasingly addressed since 2025 through its defence-readiness and technological-sovereignty initiatives.

Keywords

Digital sovereignty; Military use of AI; European strategic autonomy; Autonomous weapons; Technological dependency; Dual-use technology.

INTRODUCTION

The rapid evolution of emerging technologies, particularly artificial intelligence, has **fundamentally altered the landscape of global security and modern warfare.** What was once the domain of science fiction has become a tangible component of military doctrine, intelligence gathering and geopolitical competition. Advances in machine learning, big data analytics, robotics and advanced connectivity are compressing decision-making timelines, blurring the boundaries between civilian and military applications, and redefining what it means to project power and to defend against threats in the twenty-first century. In this context, **technological superiority is no longer simply an advantage on the battlefield; it has become a core determinant of strategic influence, economic resilience and political autonomy.**

Against this backdrop, the EU, while established as a global pioneer in digital regulation, setting standards that have shaped norms well beyond its borders, faces significant systemic challenges in **translating its robust research and talent capabilities into sovereign industrial power.** European universities, research centres and start-ups generate world-class scientific output, yet the Union continues to struggle with fragmented markets, limited access to scale-up capital, slow procurement processes and uneven investment across Member States. The result is **a persistent gap between innovation and deployment**, in which promising technologies are frequently developed in Europe but scaled, commercialised or acquired elsewhere.

Achieving a sustainable balance between technological competitiveness, democratic oversight and defence readiness is no longer merely an economic ambition, but **a paramount security imperative**. The Union must reconcile its commitment to fundamental rights, ethical safeguards and the rule of law with the urgent need to accelerate innovation, mobilise investment and strengthen its defence-industrial base. This tension is not insurmountable, but it demands **coherent governance frameworks, closer coordination between the EU and its Member States, and deeper cooperation with like-minded partners.**

This paper **explores the impact of disruptive technologies on defence domains, analyses the extent of the EU's global competitiveness, and proposes strategic avenues to bridge the gap between regulatory leadership and true strategic autonomy.** It first examines how artificial intelligence, autonomous systems, cognitive warfare and quantum technologies are transforming the conduct of security and defence. It then assesses the Union's technological and industrial position relative to other global actors, identifying structural strengths, weaknesses and critical dependencies. Finally, it puts forward a set of policy recommendations aimed at strengthening Europe's innovation ecosystem, reinforcing its defence-technological capacity and ensuring that technological progress remains aligned with European values and security interests.

1 TECHNOLOGY AND FUTURE SECURITY: KEY DOMAINS

1.1 AI AND DEFENCE APPLICATIONS

Artificial intelligence (AI) can be defined as the ability of a computer program to perform reasoning processes or tasks usually associated with human intelligence[1]. This disruptive technology has become a crucial weapon in the defence field and has completely transformed modern warfare. Wars accelerate innovations and technological developments. In current conflicts, the battlefield is also a testing ground to new technological applications.

However, alongside its tactical advantages, the militarisation of AI introduces profound ethical and legal dilemmas, particularly regarding autonomous lethal decision-making and human accountability, that must be carefully addressed.

Autonomous systems are defined as hardware or software machines capable of performing specific tasks or functions without direct human input once activated. Autonomous systems can adapt to unpredictable environments and understand a higher content to achieve assigned goals, unlike automated systems which follow fixed, and deterministic rules. They can be distinguished by the human involvement in the decision, from semiautonomous, with humans in the loop, to fully autonomous, with humans out of the loop. Autonomous systems are not truly self-governing entities but tools that exist within a framework of human policy[2].

The Russia and Ukraine war was the first international conflict in which both sides have actively used AI for military purposes[3]. This technology has been implemented in different security areas. For example, Ukraine has applied AI to combat disinformation, by fighting against fake media, detecting deepfake audio and video clips, and exposing bot networks, to identify potential narratives that could target Ukraine's reputation. AI is also a significant tool for consolidating data from various sources, such as robots, satellites and drones. In this regard, AI-equipped robots can clear mines and unexplored land, helping to develop safer strategies. It also has been used to simulate combat training scenarios and to monitor surveillance video, analyse facial recognition and conduct reconnaissance. These applications are done by First Person View (FPV) drones, facial recognition software and neural networks of acoustic sensors[4]. On the other side, Russia is also using this technology, which is a particular concern for the European Union (EU) given the constant threats that it has faced since the war began. Russian suspected drones have interfaced European airspace, such as Poland's[5] and there have been security incidents affecting Romania, Finland and the Baltic countries[6]. Romania has also suffered hybrid attacks, such as the suspected Russian creation of TikTok bots during the presidential elections campaign[7].

Furthermore, Israel uses AI for the military field. The use of it has significantly scaled up since 7 October 2023. During the first weeks within the Gaza war, Lavender and The Gospel, AI decision-support systems, were used to compile a list of 37,000 potential targets[8]. They additionally adopted Where's Daddy? a system that tracks individual's locations ahead of potential strikes[9].

Likewise, the US has applied AI systems to the Iran conflict[10]. Primarily is using AI with similar applications: intelligence, surveillance, reconnaissance (ISR), logistics and autonomous systems. The Pentagon's AI strategy includes AI-enabled weapons systems like the MQ-9 Reaper drone or the Sea Hunter autonomous naval vessel to prevent submarine warfare, it is ally with Palantir Technologies, and other important defence companies, as well as the application of the strategic Project

1 Francesca Rossi, "Artificial Intelligence: Potential Benefits and Ethical Considerations", Report PE 571.380. Policy Department C: Citizens' Rights and Constitutional Affairs (October 2016): 1-1 doi: 10.2861/31941

2 Paul Williams Andrew and Paul D. Scharre. "Autonomous Systems: Issues for Defence Policymakers", (2015) 8-56 https://apps.dtic.mil/sti/tr/pdf/AD1010077.pdf

3 Sebastian Clapp. "Defence and Artificial Intelligence." Report PE 569.580. EPRS European Parliamentary Research Service (2025)1-2 https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf

4 Vitaliy Goncharuk."Artificial Intelligence in Defence of Ukraine". International Centre for Defence and Security, No. 6 ISSN 2228-2076 (2024) 1-3 https://icds.ee/wp-content/uploads/dlm_uploads/2024/09/Layout-AI-in-Defence-of-Ukraine.pdf

5 Alan Charlish, Lidia Kelly and Barbara Erling. "Poland downs drones in its airspace, becoming first NATO member to fire during war in Ukraine" Reuters (September 10th, 2025) https://www.reuters.com/business/aerospace-defense/poland-downs-drones-its-airspace-becoming-first-nato-member-fire-during-war-2025-09-10/

6 European Parliament, "News and Brief" (15/06/2026) https://multimedia.europarl.europa.eu/en/audio/news-in-brief-15062026-english_EPNB1506202601

7 Paul Kirby & Nick Thorpe."Romania's cancelled presidential election and why it matters" BBC, (December 6th, 2024) https://www.bbc.com/news/articles/cx2yl2zxrq1o

8 Jara Monter. "Cómo Israel Explota La IA De Grandes Tecnológicas Para Masacrar Gaza." El Orden Mundial-EOM (September 16th, 2025) https://elordenmundial.com/israel-inteligencia-artificial-microsoft-open-ai-ocupacion-gaza/#

9 Noor Hammad."The proliferation of AI-enabled military technology in the Middle East", International Institute for Strategic Studies (April 2nd, 2026) https://www.iiss.org/online-analysis/charting-middle-east/2026/04/the-proliferation-of-ai-enabled-military-technology-in-the-middle-east/

10 Anna Nadibaidze. "US Use of AI in the Iran Conflict Highlights the Continuing Debate Around the Role of People in Warfare." LSE United States Politics and Policy (May 18th, 2026) https://blogs.lse.ac.uk/usappblog/2026/05/18/us-use-of-ai-in-the-iran-conflict-highlights-the-continuing-debate-around-the-role-of-people-in-warfare/.

Maven[11] which caused an internal debate in Google. The company's employees refused to be part of the Pentagon's plan because they didn't believe contributing with the project went with the ethical standards of Google, which were based on "not doing evil"[12]. In response, the company compromised to not use their AI for military or surveillance purposes. Nevertheless, these compromises were removed[13] when the new Trump administration came along and developed a new executive order in which imply big tech companies to contribute to an AI Action Plan to promote national security and economic competitiveness[14], leaving without effect the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy of Biden's Administration[15].

China is not belligerent in the conflicts discussed above, but it is a global leader in the development of AI. The People's Liberation Army (PLA) strategy is led in three areas: mechanisation, informatisation and intelligentization. Mechanisation aims to incorporate vehicles, machinery and equipment. The informatisation involves the introduction of information systems, networks and military data, which includes ISR, cyber operations and control. Since 2019, intelligentization is in the phase of the incorporation of AI, virtual and augmented reality, big data, autonomous systems, the internet of the things (IoT) and cloud computing. The PLA has described the achievement of this last phase as the "Metaverse War". From its point of view the metaverse becomes central for "winning the future" but also defines an essential area of future warfare[16].

Aware of the importance of the strategic integration of AI to modernize defence capabilities and internal security systems, **the EU is working on it with the aim of doing it with a trustworthy AI that can operate reliably in the high-risk adversarial scenarios typical of modern warfare**[17]. Through the European Defence Fund (EDF), the EU supports diverse projects, for instance, for cyber defence: PANDORA, for network threat detection: AInception, for augmented reality in soldier systems: LODESTAR, for military applications and simulation: KOIOS. It also works with Eu-Guardian: an AI-based automation of cyber incident management or FaRADAI: an AI framework that learns faster with less data[18]. Frontex is also examining how AI can support stronger EU border management, looking at technologies for biometric identification, such as facial recognition, fingerprint and iris scans[19], emotion analysis, risk assessment and migration monitoring that are already being tested or deployed[20]. Surveillance is enhanced by machine learning technologies like Automatic Target Recognition (ATR) which allows authorities to identify and track in real time. However, these uses of AI can be classified as high-risk in the AI ACT which raises debates and controversy on the use of it[21].

1.2 EMERGING TECHNOLOGIES AND FUTURE TECHNOLOGIES IN DEFENCE

Although AI is changing the current battlefield, other emerging technologies can have a crucial role and provoke a shift in power balances. That's why it is important to identify these technologies and their key domains.

We are recently more conscious about the manipulation that can be made by social media, which is an essential weapon to control the narrative of the enemy. Cognitive warfare is a tool of any political actor to influence how the target feels and modify their opinions and beliefs. Psychological Operations (PSYOPs) have been a traditional use in warfare[22] but with Artificial Intelligence these strategies become more powerful than ever: microtargeting, profiling, creation of bots and the deepfakes contribute to creating personalized

11 Sebastian Clapp. "Defence and Artificial Intelligence." Report PE 569.580. EPRS European Parliamentary Research Service (2025)2-3 https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf.

12 Irja Malmio. "Ethics as an enabler and a constraint – Narratives on technology development and artificial intelligence in military affairs through the case of Project Maven" Technology in Society 72 102193 (February 2023) https://www.sciencedirect.com/science/article/pii/S0160791X22003347/pdfft?md5=1619ade66c38d808781759c23485365f&pid=1-s2.0-S0160791X22003347-main.pdf

13 Ángel Jiménez de Luis. "Google cambia las directrices de su IA y elimina una cláusula que prohibía su uso en la fabricación de armas y sistemas de vigilancia" El mundo. (February 5th, 2025) https://www.elmundo.es/tecnologia/2025/02/05/67a2a073fdddff769d8b458e.html

14 Stopperich, Micah. "Removing Barriers to American Leadership in Artificial Intelligence." The White House (January 23rd, 2025) https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence

15 "Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy." United States Department of State (January 16th, 2025) https://www.state.gov/bureau-of-arms-control-deterrence-and-stability/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy

16 Joshua Baughman."The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield" (2024) https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/Baughman_CDRV9N3-Fall-2024.pdf

17 European Commission. "Artificial Intelligence (AI) in Defence" Defence Industry and Space (December 2025) ISBN: 978-92-68-35012-6 doi: 10.2889/1453267

18 ibid.

19 Research and Innovation Unit (INNOVATE). "Frontex Industry Days on AI Tools for Seamless Border Checks 20-21 February 2025" https://www.frontex.europa.eu/assets/Invitations/Outcomes/2025/AI_tools_Border_check/Report_-_Industry_Days_on_AI_Tools_for_Seamless_Border_Checks_20-21_February.pdf

20 Costica Dumbrava. "Artificial intelligence at EU borders Overview of applications and key issues". EPRS | European Parliamentary Research Service, PE 690.706 (July 2021) https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf#

21 Regulation(EU)2024/1689 of the European Parliament and of the Council. "Artificial Intelligence Act" (June 13th, 2024) https://eur-lex.ropa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

22 Curtis, Glenn (1989.) "An Overview of Psychological Operations (PSYOP)." Report 19951222 023. Library of Congress https://apps.dtic.mil/sti/tr/pdf/ADA302389.pdf

narratives that can affect the personal individual's decision-making. It's been already used against the European Union, with the big consequence of Brexit[23]. Perhaps, it can go further beyond the scope of social media. China has already developed the Intelligent Psychological Monitoring System, a smart sensor bracelet which records facial information, emotions changes and psychological states of soldiers to determine their combat psychological status[24]. In this regard, NATO had alarmed that we must defend and protect our minds[25].

Cognitive warfare can also be related with biotechnology by **neurotechnology**. Neurotechnology can be used as intercept-proof communication, remote device control, for instance brain controlled unmanned aerial vehicles; there have already been past cases where a fighter jet has been controlled by brain receptors. As well, it can have applications for war fighter enhancement and post-traumatic treatment of veterans[26]. It could be used to increase resilience to stress or other emotions that could impact soldiers' behaviour[27]. However, it can also be applied to manipulate the nervous system, memories or debilitate brain functions, such as espionage and interrogation tools[28]. Leaving aside the neuroscience applications, **biotechnology** brings opportunities such as using AI-enabled bio sensors for threat detention, synthetic biology, as well as human enhancement tools like exoskeletons for mobility and human-machine interfaces for improved decision-making[29].

Biotechnology can be applied not only in humans, but also in insects. In 2025, German company SWARM Biotactics developed surveillance systems using live cockroaches equipped with sensor technology. Indeed, **robotics and multi robots (swarm)** are playing, and will play, a crucial role in the future technology in the defence sector. These robotics simulates nature swarms, like ants and bees which facilitates mass moving with cohesion and coordination[30]. The effectively employment of swarm requires a high degree of information flow among different elements, it requires that individual elements can communicate with one another but also are able to process the information quickly[31]. There are different applications of swarms, it can be used for a coordinated attack and defence, like saturating enemy defences with waves of attacks from diverse directions simultaneously[32].

Other technologies which involve human-machine interaction and can have military applications are virtual and augmented reality.

Virtual reality (VR) first applications in the military was for flight simulators for training pilots. It's been used in military medicine, in the return of soldiers from deployment, in this regard, it is also applied for surgical and complex procedures by military doctors through transfer of training. It also has been used as military training through simulations. With multiple simulators and networked together, such as body area networks, it can be applied for training data collection when they are inserted into a VR military simulator, which provides a researcher's real time actions and postures response. Furthermore, it can also be useful to identify key elements in decision making, such as "to shoot or not" dilemmas or training stress resilience by exposing to difficult scenarios like tunnelling though rocks[33].

Augmented reality (AR) is the merging of virtual and the physical world. It normally it's applied in military field with the combination of multiple ISR streams, it can improve a soldier's space knowledge, create better training facilities, and to adapt quicklier and smarter to complex conditions[34].

Moreover, **quantum technology** is emerging as a future essential in defence. The military appli-

23 García-Orosa, Berta (2021). "Disinformation, social media, bots, and astroturfing: the fourth wave of digital democracy". Profesional de la información, v. 30, n. 6, e300603 https://doi.org/10.3145/epi.2021.nov.03

24 Nato Allied Combat transformation, "Cognitive Warfare: Beyond Military Information Support Operations" NATO (May 9th, 2023) https://www.act.nato.int/article/cognitive-warfare-beyond-military-information-support-operations/

25 Nato Allied Combat transformation, "Cognitive Warfare: Strengthening and Defending the Mind" NATO (April 5th, 2023) https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/

26 Rickli, JM., Ienca, M. (2021). "The Security and Military Implications of Neurotechnology and Artificial Intelligence". In: Friedrich, O., Wolkenstein, A., Bublitz, C., Jox, R.J., Racine, E. (eds) Clinical Neurotechnology meets Artificial Intelligence. Advances in Neuroethics. Springer, Cham. 209-210 https://doi.org/10.1007/978-3-030-64590-8_15

27 Rickli, Jean-Marc, "Neurotechnologies and Future Warfare" AI Governance & Military Affairs, Rsis Commentary (7th December 2020) CO20208.pdf

28 Rickli, JM., Ienca, M. (2021). "The Security and Military Implications of Neurotechnology and Artificial Intelligence" 208-2010

29 Nato Allied Combat Transformation, "Summary of NATO's Biotechnology and Human Enhancement Technologies Strategy" NATO (April 12th, 2024) https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/04/12/summary-of-natos-biotechnology-and-human-enhancement-technologies-strategy

30 Paul Scharre. "Unleash the Swarm: The Future of Warfare" (March 4th, 2015) https://warontherocks.com/unleash-the-swarm-the-future-of-warfare/

31 Ibid.

32 Ibid.

33 Akshat Upadhay. "Virtual Reality, Augmented Reality, and Warfare", Observer Research Foundation, Issue Brief No. 742 (October 2024) https://www.orfonline.org/public/uploads/posts/pdf/20241018100850.pdf

34 S.Gurusubramani., M.SureshAnand, J.JeganAmarnath, D.Sathishkumar, A.Sheela. "Augmented Reality in Military Applications" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1S 51-54, (October 2019) DOI:10.35940/ijeat.A1010.1091S19

cations could affect intelligence, security and defence capabilities[35].

Quantum sensing uses the principles of quantum physics within a sensor; it can provide alternative positioning, navigation, and timing (PNT) options, as well as detect gravitational and magnetic fields that could allow soldiers to continue to operate in GPS-degraded or denied environments[36]. It can also be used for ISR purposes, the quantum sensors could detect nuclear material, underground structures or electromagnetic emissions.

Quantum computing could achieve problem-solving faster than today's computers[37], enabling advances in AI models which could develop in more accurate lethal autonomous weapons systems.

Furthermore, Post-quantum cryptography could potentially decrypt classified information stored on encrypted media, allowing access to sensitive information[38] but also safeguarding it from cyber threats through high-speed processing.

Quantum simulation is the ability to simulate and model complex battlefield environments, enabling to run diverse potential scenarios, exploring the known strategies and new and unforeseen outcomes. These simulations offer insights into operational risks, adversary behaviours and tactical opportunities which leads to mitigating potential risks and strengthening defensive strategies[39].

Quantum communication can strengthen communications security, notably through quantum key distribution, which enables secure key exchange and can reveal interception attempts. It does not make communications inherently untraceable[40].

QUANTUM WARFARE

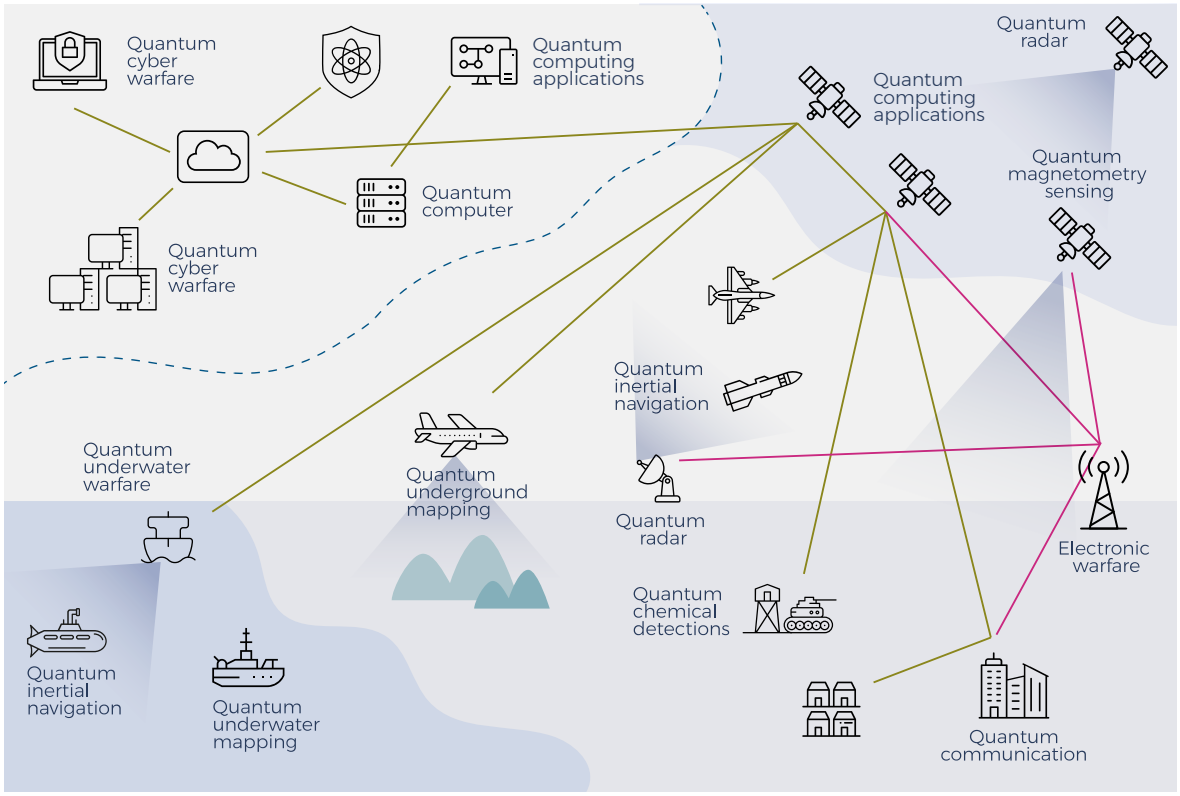


Figure 1: Quantum applications in warfare. Source: Krelina, Michal. (2021). "Quantum Warfare: Definitions, Overview and Challenges"10.48550/arXiv.2103.12548.

35 Michal Krelina, "Quantum Warfare: Definitions, Overview and Challenges", Faculty of Nuclear Sciences and Physical Engineering, Czech Technical University in Prague (March 24th, 2021) https://www.researchgate.net/publication/350341569_Quantum_Warfare_Definitions_Overview_and_Challenges

36 European Commission. "Quantum Technologies in Defence", Defence Industry and Space (December 2025) doi: 10.2889/1727389

37 Hank Hanna, "The Emerging Potential for Quantum Computing in Irregular Warfare", Irregular Warfare Center, Vol 3, No.1 (January 2025) https://irregularwarfarecenter.org/wp-content/uploads/13_1_Quantum-Computings-Emerging-Role-in-Irregular-Warfare.pdf

38 Congressional Research Service "Defense Primer: Quantum Technology " (May 12th, 2026) https://www.congress.gov/crs-product/IF11836

39 Hank Hanna. "The Emerging Potential for Quantum Computing in Irregular Warfare"(January 2025)

40 Ibid.

Technology	Uses and Applications
Cognitive Warfare	
AI-powered PSYOPs	Control the enemy's narrative; influence how the target feels and modify their opinions and beliefs (e.g. Brexit)
	Microtargeting, profiling, creation of bots and deepfakes to generate personalized narratives that affect individual decision-making
Smart sensor Bracelet	Intelligent Psychological Monitoring System: Record facial information, emotional changes, and psychological states of soldiers to determine their combat psychological status
Neurotechnology	
Neurotechnology	Intercept-proof communication
	Remote control of devices, e.g., brain-controlled unmanned aerial vehicles (UAVs); past cases of fighter jets controlled by brain receptors
	War fighter enhancement, post-traumatic treatment of veterans, increased resilience to stress and other emotions
	Manipulation of the nervous system and memories, debilitation of brain functions; espionage and interrogation tools
Biotechnology	
AI-enabled biosensors	Threat detection
Exoskeletons	Improved human mobility
Human-machine interfaces	Improved decision-making
Insect bio-robotics	ISR, e.g. Use of live roaches as cyborgs
	(SWARM Biotactics, German company)
Robotics	
Swarm robotics	Coordinated attack and defence; intelligence: improve target identification, geolocation accuracy, and provide increased resilience to spoofing
VR & AR	
Virtual Reality	Flight simulations, training pilots
	Military medicine
	Training data collection from soldiers
	Identify soldier's decision making dilemmas
	Build stress resilience / therapeutic purposes
Augmented Reality	ISR
	Improve soldier's space knowledge
	Help in training facilities
Quantum	
Quantum Sensing	Alternative Positioning, Navigation and Timing (PNT), detect gravitational and magnetic fields allow to operate in GPS-degraded or denied environments
	ISR, detect nuclear material, underground structures or electromagnetic emissions
Quantum Computing	Faster problem-solving
	More accurate lethal autonomous weapons systems
Post-quantum cryptography	Decrypt classified information
	Safeguard sensitive information from cyber threats
Quantum Simulation	Mitigating potential risks and strengthening defensive strategies
Quantum Communication	Untraceable communication networks, more secure military communication, without fear of detection

Figure 2: Summary of emerging technology in defence and their applications. Source: Own creation (Modified after a first AI elaboration)

Quantum technologies are also particularly relevant for the future security of telecommunications networks. Advances in quantum computing create long-term risks for existing encryption systems, increasing the importance of post-quantum cryptography and quantum-secure communications for the protection of sensitive and critical networks.

1.3 CONNECTIVITY AND TELECOMMUNICATIONS AS STRATEGIC INFRASTRUCTURE

The development of emerging technologies increasingly depends on the connectivity infrastructure that enables them to operate. Advanced telecommunications networks are becoming critical infrastructure for industrial production, transport, energy, public services and security. As

Europe becomes more digitalised, the resilience and security of these networks therefore become strategic concerns. 5G, and particularly the transition towards more advanced standalone networks, enables applications requiring greater reliability, lower latency and the connection of large numbers of devices. These capabilities are increasingly relevant for smart factories, autonomous systems, logistics, emergency services and other critical applications. Looking ahead, 6G is expected to further integrate connectivity, sensing, computing and AI.

This creates **a dual challenge for Europe**: ensuring sufficient investment in next-generation connectivity while protecting networks against cyber threats, disruption and supply-chain vulnerabilities. Telecommunications policy therefore increasingly intersects with industrial policy, cybersecurity and European strategic autonomy.

2 TO WHAT EXTENT IS THE EU COMPETITIVE AND SOVEREIGN

2.1 DOES THE EU HAVE THE TECHNOLOGICAL AND INDUSTRIAL CAPABILITIES TO COMPETE GLOBALLY?

The EU has become a global leader in tech regulation — think of the AI Act, the Cyber Resilience Act, the Digital Europe Programme and the European Chips Act. But regulating technology is not the same as producing it. This is the **core tension** behind Europe's competitiveness debate: **the EU sets the rules of the digital game, yet often doesn't own the technology being played with**[41].

On the strengths side, **Europe has real assets**: one of the world's largest internal markets, top-tier universities and research institutions, and a solid industrial base. European researchers contribute meaningfully to AI, cybersecurity and quantum computing, and the EU's data-protection model gives it a distinct identity compared to other powers. The weakness shows up in scale. The US has built global tech giants — Google, Microsoft, Amazon, Meta — that dominate by sheer size, while China has pursued a state-driven model combining public investment with industrial planning[42].. The EU has neither: no company of comparable global weight, and a more fragmented approach to funding innovation.

Artificial intelligence makes the gap especially visible. Europe does have strong research output and engineering talent, as well as companies developing their own foundation models. Mistral AI, valued at roughly €11.7 billion following its 2025 funding round, is often cited as Europe's leading example[43].What Europe lacks is the industrial platform: the coordinated, large-scale system that allows the US and China to turn research into globally deployed products[44]. Part of this disparity comes down to data and capital. Large US technology companies have access to vast pools of training data accumulated over years, while EU investment in AI development has remained considerably lower. According to the Stanford AI Index, private AI investment in 2024 reached approximately $109.1 billion in the United States, $19.4 billion in Europe and $9.3 billion in China[45].

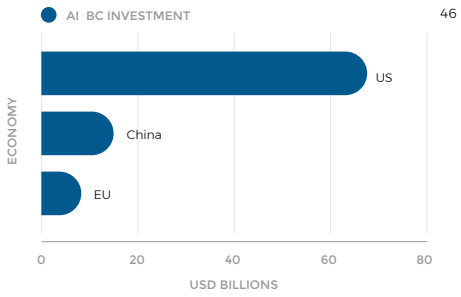


Figure 3: Investment in AI Development United States-China-EU. Source: Own creation

What this shows is that **Europe isn't short on ideas or talent.** The real bottleneck is the jump from research to a globally competitive product, slowed down by fragmented funding, limited venture capital, and differences between national markets.

41 Antonio Calcara."European Cloud Computing Policy: Failing in Europe to Succeed Nationally?" West European Politics 49, no. 4 (2025): 994–1028 https://doi.org/10.1080/01402382.2025.2491962

42 Antonio Calcara."European Cloud Computing Policy: Failing in Europe to Succeed Nationally?" West European Politics 49, no. 4 (2025): 994–1028 https://doi.org/10.1080/01402382.2025.2491962

43 Owen Carpenter-Zehe. "Why Is the EU Struggling to Scale Artificial Intelligence?" EUobserver (February 13th, 2026) https://euobserver.com/202965/why-is-the-eu-struggling-to-scale-artificial-intelligence/

44 Owen Carpenter-Zehe. "Why Is the EU Struggling to Scale Artificial Intelligence?" EUobserver (February 13th, 2026) https://euobserver.com/202965/why-is-the-eu-struggling-to-scale-artificial-intelligence/

45 Shahlaei, C. A., Berente, N., "An Analysis of European Data and AI Regulations for Automotive Organizations," July 2024, arXiv:2407.11271. 1–15 https://arxiv.org/pdf/2407.11271

46 Source: Own elaboration based on Stanford Institute for Human-Centered AI, AI Index Report 2025 (United States and China), and European Commission / EISMEA data (European Union) https://hai.stanford.edu/assets/files/hai_ai_index_report_2025.pdf, https://eismea.ec.europa.eu/eismea-datahubs_en

The Commission's own June 2026 Technological Sovereignty Package — covering semiconductors, AI, cloud and open source — is itself an admission that regulation alone won't close this gap, and that industrial investment now has to follow[47].

2.2 WHAT ARE THE MAIN DEPENDENCIES? INFRASTRUCTURE, TALENT, DATA, PLATFORMS

These dependencies aren't separate problems — they build on each other, starting with the physical layer underneath everything else: infrastructure. Cloud computing is the clearest example. Despite repeated EU efforts — first national "champions," then pan-European projects like Gaia-X, originally pitched as an "Airbus for AI" — the market is still dominated by non-European players[48]. This isn't simply a lack of effort: between 2017 and 2022, European cloud providers' market share fell from 29 percent to 15 percent and has remained broadly stable since. In 2024, AWS, Microsoft and Google together accounted for around 70 percent of the European cloud market[49]. The same logic applies to computing power and chips: The EU accounts for around 9 percent of the global semiconductor market, leaving it dependent on third-country suppliers in key segments[50].

A. Infrastructure and data

Telecommunications networks constitute another layer of Europe's critical digital infrastructure. The deployment of advanced 5G networks and the future transition towards 6G will influence Europe's capacity to develop connected industries, autonomous systems and AI-enabled services at scale. This makes the security, resilience and competitiveness of European telecommunications infrastructure an increasingly important component of digital sovereignty. The challenge is not simply coverage, but capability: Europe needs networks capable of supporting increasingly demanding industrial and mission-critical applications. At the same time, the strategic importance of telecommunications makes network security, trusted supply chains and resilience against disruption essential considerations.

This infrastructure gap shapes who controls Europe's data. The EU leads the world on data protection through the GDPR, but most European data still sits on non-EU infrastructure, which exposes it to foreign legal regimes — notably US law, which can compel access to data held by US companies even when the servers are physically in Europe[51]. AWS and Microsoft have expanded sovereign-cloud offerings designed to strengthen data residency and operational control in Europe. These services mitigate parts of the sovereignty problem, although ownership structures and exposure to non EU-legal regimes remain subjects of policy debate[52] . The same dependency extends directly into AI: training large models requires enormous amounts of data, and US tech firms have spent years accumulating exactly that kind of data at scale, giving them a head start European companies cannot easily match[53].

B. Talent

Behind all of this sits a human dependency: talent. The picture here is more nuanced than a simple "brain drain" story. Europe remains, overall, a net recipient of tech talent, and a majority of European AI founders choose to build from Europe rather than relocate[54]. The real issue is narrower: it's senior, experienced specialists — in AI, cybersecurity, semiconductors — who keep leaving for the US, pulled by salaries that are often far higher[55]. Layered on top of this is a more basic skills gap: just over half of EU adults had basic digital skills in 2023, which limits the pipeline of future specialists long before the brain-drain issue even comes into play.

C. Platforms

Finally, **there are the platforms people use every day** — search engines, social media, operating

47 Reyhan Dalaman. "The EU's Tech Sovereignty Package and the Future of European Digital Power," Digital Watch Observatory (June 10th, 2026) https://dig.watch/updates/the-eus-tech-sovereignty-package-and-the-future-of-european-digital-power .

48 Antonio Calcara. "European Cloud Computing Policy: Failing in Europe to Succeed Nationally?" West European Politics 49, no. 4 (April 30th, 2025): 994–1028, https://doi.org/10.1080/01402382.2025.2491962

49 Antonio Calcara. "European Cloud Computing Policy: Failing in Europe to Succeed Nationally?" West European Politics 49, no. 4 (April 30th, 2025): 994–1028, https://doi.org/10.1080/01402382.2025.2491962

50 European Commission. "Cloud Computing," Shaping Europe's Digital Future, European Commission (updated June 3rd, 2026) https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

51 Frances Burwell and Kenneth Propp. "Digital Sovereignty: Europe's Declaration of Independence?" Atlantic Council (February 2026) https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-europes-declaration-of-independence/.

52 Frances Burwell and Kenneth Propp. "Digital Sovereignty: Europe's Declaration of Independence?" Atlantic Council (February 2026) https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-europes-declaration-of-independence/.

53 Owen Carpenter-Zehe."Why Is the EU Struggling to Scale Artificial Intelligence?" EUobserver (February 13th, 2026) https://euobserver.com/202965/why-is-the-eu-struggling-to-scale-artificial-intelligence/

54 Atomico. "State of European Tech 2025 Report: Europe Faces a Decisive Decade to Define Its Technological Leadership" Capital-Riesgo.es (2025) https://capital-riesgo.es/en/articles/state-of-european-tech-2025-report-europe-faces-a-decisive-decade-to-define-its-technological-leadership/

55 Nicklas Lundblad. "Digital Sovereignty: Can Europe Afford It?" CEPA (October 29th, 2025) https://cepa.org/article/digital-sovereignty-can-europe-afford-it/.

systems, app stores, marketplaces — **almost all of which are owned by a small number of US (and a few Chinese) companies. This isn't just an economic dependency; it's a strategic one.** A unilateral service change or shutdown by a dominant non-EU platform can still have direct effects on European public life. The EU has significant regulatory levers through instruments such as the DMA and DSA, but it does not control the underlying infrastructure or corporate decisions of those providers.

2.3 CAN THE EU ACHIEVE DIGITAL SOVEREIGNTY?

Given everything above, full digital self-sufficiency for the EU isn't realistic — and most policymakers no longer pretend otherwise. The Declaration for European Digital Sovereignty, adopted by all EU Member States in November 2025 around the Berlin Summit on European Digital Sovereignty, frames digital sovereignty around reducing strategic dependencies while preserving technological choice and international cooperation[56]. In other words, **the goal isn't to build a European version of everything; it's to make sure Europe isn't dangerously dependent on any single outside actor for the things that matter most** — and to be able to choose its partners rather than have dependency forced on it.

This approach is consistent with the EU's established concept of 'open strategic autonomy': remaining open to global trade and cooperation while reducing critical dependencies[57]. This is a genuine shift from the EU's older instinct, which was to regulate first and worry about industrial capacity later. The Commission's June 2026 proposal for a Chips Act 2.0 builds on the original Chips Act, which mobilised more than €52 billion in public and private investment and created an estimated 46,000 direct and indirect jobs— real progress, even though Europe still depends on others for the most advanced chip manufacturing[58]. The same logic applies to the proposed Cloud and AI Development Act (CADA), which aims to at least triple EU data-centre capacity within five to seven years[59].

This is also why **sovereignty can't be only about regulation, and can't be only about investment either — it has to be both at once.** Rules like the GDPR or the AI Act protect citizens and set global standards, but they don't, by themselves, build a single chip fab or train a single AI engineer. At the same time, investment without rules risks recreating the same concentrated, unaccountable power structures the EU is trying to move away from, just under European ownership instead of American or Chinese. The real balancing act is holding three things together at once: security, meaning not depending on outside actors for critical systems; competitiveness, meaning actually being able to build and sell technology at scale; and the EU's founding commitment to fundamental rights and democratic oversight, which distinguishes its model from both the US's market-driven approach and China's state-controlled one[60].

So, can the EU achieve digital sovereignty? Probably not in the sense of total independence — and it doesn't need to. The more realistic and arguably healthier goal is selective: identify which dependencies are genuinely dangerous (sensitive data, defence systems, critical infrastructure), reduce exposure where it matters most, and accept continued cooperation everywhere else. Whether the EU manages this will depend less on writing new rules and more on whether it can finally turn its research, its market size and its industrial base into technology it actually owns.

3 SECURITY IMPLICATIONS

3.1 HOW IS AI TRANSFORMING DEFENCE AND MILITARY CAPABILITIES?

Artificial Intelligence (AI) is no longer a futuristic concept but a present-day operational reality acting as a **massive force multiplier in the military domain.** It is fundamentally altering the speed, scale, and character of modern warfare. According to the European Parliamentary Research Service (EPRS), the integration of AI applications extends far beyond the public imagination of autonomous weapons; it permeates the entire spectrum of mi-

56 Council of the European Union. "Declaration for European Digital Sovereignty" (December 5th, 2025) https://table.media/assets/europe/declaration-for-european-digital-sovereignty_final.pdf

57 "The EU's Tech Sovereignty Package and the Future of European Digital Power," Digital Watch Observatory, op. cit.

58 "The EU's Tech Sovereignty Package and the Future of European Digital Power," Digital Watch Observatory, op. cit.

59 European Commission."Cloud Computing," Shaping Europe's Digital Future European Commission(updated June 3rd, 2026) https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

60 Clotilde Bômont. "Autonomy Is Not Autarky: But Is the EU's New Digital International Strategy's Focus on Partnerships Enough?" European Union Institute for Security Studies (June 13th, 2025) https://www.iss.europa.eu/publications/commentary/autonomy-not-autarky-eus-new-digital-international-strategys-focus.

litary operations, from logistics and backend administration to frontline combat capabilities[61].

Primarily, AI is revolutionising military logistics and sustainment. Armed forces generate vast amounts of data regarding equipment wear and tear, supply consumption, and environmental conditions. AI algorithms analyse this data to enable "predictive maintenance." Instead of replacing parts on a fixed schedule or waiting for them to break in the battlefield, AI predicts exactly when a component (such as a tank engine or a fighter jet avionics system) will fail, allowing for preemptive replacement. This drastically reduces downtime, lowers maintenance costs, and ensures a higher state of operational readiness. Furthermore, AI optimises complex supply chains, ensuring that troops receive ammunition, fuel, and medical supplies efficiently, even in highly volatile environments.

On the tactical level, AI is transforming the deployment of unmanned systems. However, a critical distinction must be made between AI-assisted systems (which maintain a human-in-the-loop) and fully autonomous systems (which operate independently). This autonomy is vividly demonstrated through the concept of "swarm intelligence".

Drawing inspiration from biological ecosystems, swarm technology allows multiple unmanned aerial vehicles (UAVs), unmanned surface vessels (USVs), or ground robots to communicate and coordinate their actions in real-time without constant human input. If one drone in the swarm is destroyed, the AI instantaneously reconfigures the rest of the swarm to complete the mission. This capability can easily overwhelm traditional enemy air defences, which are designed to track and intercept a limited number of high-value targets rather than hundreds of cheap, coordinated, autonomous assets.

Crucially, AI is reshaping Command and Control (C2) structures by enabling "information superiority." Modern conflicts are multi-domain operations (land, sea, air, space, and cyber). AI systems can fuse data from all these domains, providing military commanders with a comprehensive, real-time Common Operating Picture (COP). By processing battlefield data faster than any human cognitive capacity, AI accelerates the OODA loop (Observe, Orient, Decide, Act). In warfare, the side that can complete this decision-making cycle faster inevitably gains the tactical advantage, outmanoeuvring the adversary before they can even comprehend the changing battlefield dynamics.

3.2 WHAT ARE THE RISKS? CYBER THREATS, NETWORK VULNERABILITIES, MISUSE OF AI AND STRATEGIC DEPENDENCE

Despite the undeniable tactical advantages, the rapid militarisation of AI introduces severe, multifaceted vulnerabilities that threaten national and European security. These risks can be categorised into **cyber threats, ethical misuse, and structural geopolitical vulnerabilities.**

Firstly, the intersection of AI and cyberspace creates an exceptionally volatile threat environment. The ENISA Threat Landscape report highlights that AI significantly lowers the barrier to entry for cyberattacks while simultaneously increasing their sophistication. Malicious state and non-state actors leverage Machine Learning (ML) to automate and scale up phishing campaigns, using generative AI to craft highly convincing, targeted social engineering attacks in multiple languages. Furthermore, AI enables the development of self-mutating malware (polymorphic malware) that can alter its code to evade traditional, signature-based[62] antivirus detection systems. AI algorithms are also deployed to scan critical infrastructure networks autonomously, identifying and exploiting zero-day vulnerabilities at speeds that human cybersecurity teams cannot match.

Secondly, there is a profound risk regarding the ethical and legal misuse of AI, particularly concerning Lethal Autonomous Weapons Systems (LAWS). The deployment of weapon systems capable of selecting and engaging targets without human intervention raises critical questions about compliance with International Humanitarian Law (IHL), specifically the principles of distinction (between combatants and civilians) and proportionality. The potential loss of "meaningful human control" over the use of force creates an accountability gap: if an autonomous system commits a war crime, assigning legal responsibility becomes highly complex. Additionally, authoritarian regimes may misuse AI for mass surveillance, predictive policing, and domestic suppression, contradicting democratic values.

61 Jacopo Bellasio et al., Innovative Technologies Shaping the 2040 Battlefield (Bruselas: European Parliamentary Research Service, 2021), 12, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690038/EPRS_STU(2021)690038_EN.pdf.

62 European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2023. (October 2023) ISBN: 978-92-9204-645-3, DOI: 10.2824/782573

The growing dependence of European economies and public services on digital connectivity also expands the potential impact of cyberattacks against telecommunications networks. Disruption to critical communications can have cascading effects across energy, transport, financial services, public administration and emergency response. Network resilience must therefore be understood not only as a telecommunications issue, but as a component of European security and critical infrastructure protection.

Finally, Europe faces a critical, systemic risk of strategic dependence. As outlined by the EPRS in its analysis of digital sovereignty, the EU currently lacks the industrial capacity to produce the foundational technologies required for advanced AI[63]. European defence sectors heavily rely on non-EU vendors for critical hardware—most notably advanced microchips and semiconductors manufactured in Asia—and cloud computing infrastructure dominated by US hyperscalers. This reliance creates severe supply chain vulnerabilities and the risk of "vendor lock-in." In a scenario of geopolitical crisis or trade warfare, the EU's defence capabilities could be severely compromised if foreign entities decide to restrict access to their proprietary technology or if their home governments impose extraterritorial sanctions. Achieving "open strategic autonomy" is therefore not merely an economic goal for the EU, but a paramount security imperative[64].

3.3 HOW DO EMERGING TECHNOLOGIES AFFECT INTELLIGENCE AND DECISION-MAKING?

Emerging Disruptive Technologies (EDTs), particularly the combination of AI, quantum computing, and advanced sensors, **are revolutionising the intelligence cycle and the nature of military decision-making.** The European Defence Agency (EDA) emphasises that future conflicts will be increasingly data-driven, making the ability to process and understand information the ultimate strategic asset[65].

In the realm of Intelligence, Surveillance, and Reconnaissance (ISR), AI is an indispensable tool. Modern intelligence agencies collect colossal amounts of Big Data daily: high-resolution satellite imagery, synthetic-aperture radar (SAR) data, intercepted communications (SIGINT), and endless streams of open-source intelligence (OSINT) from social media. Human analysts cannot physically process this volume of information. AI algorithms, particularly computer vision and Natural Language Processing (NLP), can sift through terabytes of data in seconds to detect anomalies, identify enemy troop movements, or translate and summarize intercepted communications, extracting actionable insights and predicting adversarial behaviour.

However, **the integration of AI into critical decision-making processes introduces profound operational risks, most notably the "black box" problem.** Many advanced deep learning models lack explainability (explainable AI or XAI). This means that while an AI system might provide a highly accurate recommendation—such as identifying a building as a high-value military target—the human commander cannot see the logical steps the algorithm took to reach that conclusion. Relying on a system without understanding its rationale creates a severe dilemma for commanders who bear the ultimate moral and legal responsibility for lethal actions.

Furthermore, **AI models are vulnerable to "data poisoning" and adversarial machine learning**. If an adversary subtly manipulates the training data or the operational environment (for instance, altering physical signs or camouflage to confuse computer vision algorithms), the AI might confidently provide incorrect intelligence, leading to disastrous military miscalculations.

Ultimately, the sheer speed of AI-driven intelligence and decision-making risks undermining crisis stability. When opposing militaries both deploy AI systems to automate their responses, there is a distinct danger of unintended conflict escalation. This phenomenon, often termed a "flash war," occurs when algorithms react to each other's actions in milliseconds, escalating a minor border incident into a full-scale conflict faster than human political and military leaders can intervene to de-escalate. Therefore, **balancing the speed of AI with the necessity of human judgment remains the greatest challenge in modern military doctrine.**

63 Tambiama Madieg, "Digital Sovereignty for Europe" European Parliamentary Research Service (EPRS) (July 2020) https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

64 Ibid.

65 European Defence Agency (EDA). "Driven by global threats, shaped by civil high-tech" European Defence Matters (2021) Issue 22 ISSN: 2443-5511 DOI: 10.2836/696496

PROPOSALS

Proposal 1

A.

Technology priorities for the EU: dual-use AI and quantum as the domains requiring most urgent EU-level investment and coordination

The question this proposal seeks to solve is not which technology is the most interesting or the most economically fulfilling, but rather, which ones are the most strategically crucial. As it has been highlighted, the European Union is in a turning point in time, where it is surrounded by conflict, but the Union finds itself lacking in the matter of technological innovation[1]. In this context, two areas of technology emerge as non-negotiable.

Dual use AI, with priority on intelligence, surveillance, and reconnaissance (ISR), decision-support, and counter-disinformation. The Russia-Ukraine conflict has demonstrated how operational and central AI can be to conflicts; from its use in deepfakes of political figures, to its integration in combat systems and using it to make decisions on the battlefield, but also to predict the enemies future actions, as Washington did months before Russia, invaded Ukraine [2]. The lesson from this is not that now warfare is dependent on AI, but instead, nations without sovereign AI capacity are dependent on third party platforms – a dependency that carries operational and political risks. Under Article 2(3), the AI Act excludes AI systems only insofar as they are placed on the market, put into service or used exclusively for military, defence or national-security purposes. Recital 24 clarifies that systems used for non-excluded purposes, including civilian, law-enforcement or public-security purposes, remain subject to the Regulation[3]. While this preserves state sovereignty, it means the EU exercises no collective oversight over how AI is developed or deployed for defence purposes within its territory. Prioritizing dual use AI systems, meaning systems that can be applied to both civilian and military contexts, would allow the EU to build genuine industrial capacity while keeping governance authority in European hands, consistent with Recital 24's acknowledgement that dual-use systems fall within scope when deployed in civilian contexts[4]. This means directing a dedicated allocation within the European Defence Fund (EDF) towards AI application in ISR, logistics, and warfare tools to counter disinformation.The EDF 2026 Work Programme allocates €1 billion to collaborative defence R&D across 31 topics, including AI-enabled capabilities, cyber technologies and quantum-secured tactical networks[5]. Because the EDF finances defence-oriented research and development, civilian technologies must be adapted to defence requirements through mechanisms such as EUDIS spin-in calls[6].

Quantum computing, as the enabling infrastructure for future secure communications. The Quantum Europe Strategy identifies quantum as foundational for encryption, secure communications, and computational advantages within the military[7]. For now the EU holds the advantage of possessing the resources required to spearhead this field, in terms of talent and startups and companies, but this position is slowly slipping as adversaries are also advancing[8]. The matter does possess a certain urgency, as the attacks "Harvest now, Decrypt later" have demonstrated; quantum computing will eventually compromise current

1 European Commission. Why Europe Is Losing the Race for Innovation(April 10th, 2024) https://ec.europa.eu/newsroom/eismea/items/826237/en.

2 José Pardo De Santayana. "Artificial Intelligence and the War in Ukraine." Artificial Intelligence in Geopolitics and Conflicts (2024) https://www.defensa.gob.es/documents/2073105/2278118/la_inteligencia_artificial_y_la_guerra_de_ucrania_2024_dieeea81_eng.pdf.

3 European Union. 2024. "Regulation - EU - 2024/1689 - EN - EUR-Lex." Europa.eu. June 13, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

4 "Recital 24 | EU Artificial Intelligence Act." 2016. Artificialintelligenceact.eu. 2016. https://artificialintelligenceact.eu/recital/24/.

5 "EDF Work Programme 2026." 2025b. Defence Industry and Space. December 17, 2025. https://defence-industry-space.ec.europa.eu/edf-work-programme-2026_en.

6 European Commission. 2025. "European Defence Fund (EDF) - Official Webpage of the European Commission. - European Commission." Defence-Industry-Space.ec.europa.eu. 2025. https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en.

7 "Quantum Europe Strategy: Quantum Europe in a Changing World" https://ec.europa.eu/newsroom/dae/redirection/document/117890

8 ibid

encryption standards, exposing sensitive data across all fields, including classified intelligence[9][10]. Prioritizing investments in quantum resistant cryptography, as well as in domestic quantum efforts, is a threat to responsive expenditure with a time limited window. The EDF 2026 work Programme already calls for the development of quantum secure networks, now what is missing is a coordinated member states commitment to quantum as a strategic priority, similar to what the EU did previously with semiconductors, notably with the Chips Act[11].

B.

How to strengthen Innovation and Industrial Capacity?

As we have established, Europe's problem is not the lack of talent or research, but the structural inability to translate innovation into deployed capability at scale[12].

Reform the EDF-PESCO pipeline to reduce fragmentation and enforce delivery. PESCO's initial phase succeeded in establishing cooperation between member states but fell short on the delivery of tangible outputs[13]. As the EDA Annual Report 2025 highlights, the European Defence Technological and Industrial Base (EDTIB) remains fragmented among member states, with duplicated investments and limited interoperability[14]. PESCO's next phase should introduce binding delivery timelines, mandatory interoperability standards for AI and digital systems, and a review mechanism conditioning continued funding on consistent output rather than mere participation in EU wide programs. The European Defence Industry Programme (EDIP) with €1.5 billion allocated for 2026-2027, provides the financial instrument to jumpstart these additional recommendations; governance and proper allocation are the missing elements[15]. Simultaneously, the EU should lower barriers to entry for defence-tech SMEs and startups, which face disproportionate compliance costs relative to more established companies; by contrast, U.S. defence-tech startups benefit from greater financial support due to deeper private funding[16]. The EUDIS open call initiative is a step in the right direction; to build on this further, using the AI Act's existing provisions under Articles 57-63 for regulatory sandboxes for civilian use AI, and extending these provisions to defence-adjacent applications, as long as their use can also be applied to civilians, to make them dual use systems, would be a greater step[17]. This would allow SMEs and startups to test systems under supervised conditions before full regulatory obligations apply, and at the same time, protect them from the heavy bureaucratic load the EU imposes on AI systems, while ensuring that systems entering the defence market meet minimum governance standards.

Close the research-to-commercialisation gap through coordinated EU venture mechanisms. European universities and research centres generate competitive output across AI, quantum, and cybersecurity.[18] The gap is financial rather than intellectual: European scale-up capital remains thinner and more fragmented than in the United States, despite new EU-level instruments such as EIC STEP Scale Up, the 2026 EIC STEP Scale Up Defence call and the Scaleup Europe Fund.[19] Rather than creating a new fund, the EU should scale and coordinate these existing instruments to provide growth-stage capital to strategic and dual-use technology companies under clear technical, financial and governance conditions.[20] This would allow the EU to have a similar model of public-private financing that the United States and China already have.

9 "Harvest Now, Decrypt Later: Quantum Security Risk." n.d. Palo Alto Networks. Accessed June 23, 2026. https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl#how.

10 ibid

11 "EDF Work Programme 2026." 2025b. Defence Industry and Space. December 17, 2025. https://defence-industry-space.ec.europa.eu/edf-work-programme-2026_en.

12 "Quantum Europe Strategy: Quantum Europe in a Changing World" https://ec.europa.eu/newsroom/dae/redirection/document/117890

13 Latici, Tania. 2020. "AT a GLANCE Plenary -October II 2020." https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/659280/EPRS_ATA(2020)659280_EN.pdf.

14 "Annual Report 2025" https://www.eda.europa.eu/docs/default-source/applicants/eda-2026-annual-report-2025_web.pdf

15 "EDIP | Forging Europe's Defence." 2026. Defence Industry and Space. 2026. https://defence-industry-space.ec.europa.eu/eu-defence-industry/edip-forging-europes-defence_en.

16 Chinn, David, and Jakob Stöber. 2025. "European Defense Tech Start-Ups: In It for the Long Run?" McKinsey & Company. February 12, 2025. https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/european-defense-tech-start-ups-in-it-for-the-long-run.

17 European Union. 2024. "Regulation - EU - 2024/1689 - EN - EUR-Lex." Europa.eu. June 13, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

18 "Quantum Europe Strategy: Quantum Europe in a Changing World" https://ec.europa.eu/newsroom/dae/redirection/document/117890

19 "The Scale-Up Gap Financial Market Constraints Holding Back Innovative Firms in the European Union ECONOMICS -THEMATIC STUDIES." n.d. Accessed July 19, 2026. https://www.eib.org/attachments/lucalli/20240130_the_scale_up_gap_en.pdf.

20 "About | Nato Innovation Fund." 2024. Nato Innovation Fund. https://www.nif.fund/about/.

C.

What Policies and Investments are needed?

Advance the negotiations on the proposed Cybersecurity Act 2 and strengthen coordination with the existing EU cyber-resilience framework. In January 2026, the Commission proposed a revised Cybersecurity Act (COM(2026) 11), which would reinforce ENISA's role and the EU cybersecurity certification framework. The EU Cybersecurity Reserve already exists under the Cyber Solidarity Act, while ENISA launched the European Vulnerability Database in May 2025 under the NIS2 framework.[21,22] These upgrades demonstrate a European collective effort made towards improving cyber defence capabilities. Beyond the CSA2, the EU should progressively develop a unified defence command with operational capacity, separate from ENISA's civilian mandate and nested within the ReArm Europe framework, as it targets similar concerns from a different perspective.[23] The EU's ambition for strategic autonomy is not credible without the capacity to deter, attribute, and respond to cyberattacks on critical infrastructure. Particular attention should be given to the resilience of telecommunications networks and other critical digital infrastructure. The EU's cybersecurity framework should ensure high and consistent security standards while avoiding unnecessary fragmentation and maintaining the conditions needed for continued investment and innovation in advanced connectivity.

Establish a structured cooperation framework for intelligence sharing. Intelligence remains the most guarded national prerogative in the EU, with Article 4(2) TEU affirms that national security is the sole responsibility of each member state.[24] This is a legitimate constraint, but it does not preclude structure cooperation among willing member states. Article 4(2) TEU confirms that national security remains the sole responsibility of each Member State. Cooperation among willing states is still possible, but Article 20 TEU does not create a new EU competence in national intelligence. A voluntary intergovernmental arrangement among participating Member States could establish common classification standards and data-sharing protocols, while using EU INTCEN as an analytical coordination hub within its existing mandate.[25] The Ukraine war has demonstrated both the value of shared strategic intelligence and the operational cost of its fragmentation; political will is high, and should not be wasted.[26]

D.

How to Balance Security, Competitiveness, and Regulation?

The framing question contains a premise worth challenging: security, competitiveness and regulation are not necessarily in tension. The tension emerges only when they are poorly managed or institutionally isolated. The EU regulatory model-the AI Act, the GDPR, The Cyber Resilience Act-have established Europe as the global standard centre for technology governance. The challenge now is ensuring that these regulatory frameworks support rather than constraint the industrial landscape they govern.

Three principles should guide this balance.

First, regulation as a strategic asset, not as an administrative burden. All the frameworks listed throughout the proposals, are instruments of market definition, that advantage European actors building according to these standards. A company that is AI act and CSA2 compliant can access the EU markets that a noncompliant foreign competitor cannot. This way, properly designed regulation is a competitive advantage, but only when it is conceived with industrial strategy in mind and not as a standalone governance exercise.

Second, security carve-outs must not become governance gaps. Article 2(3) excludes AI systems only insofar as they are used exclusively for military, defence or national-security purposes. Civilian, law-enforcement and public-security uses remain within the AI Act's scope where the Regulation applies entirely. As the EPRS 2025 notes, it is governed, but by fragmented national rules. The EU should develop a parallel governance framework for military AI, drawing on NATO's Principles of Responsible Use for Artificial Intelligence in Defence, as a baseline, and establish it as a binding instrument among member states. The goal is not to

21 "Commission Strengthens EU Cybersecurity Resilience and Capabilities." 2026. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_105.

22 "Proposition de Règlement Relatif Au Règlement de l'UE Sur La Cybersécurité." 2026. Bâtir L'avenir Numérique de l'Europe. 2026. https://digital-strategy.ec.europa.eu/fr/library/proposal-regulation-eu-cybersecurity-act.

23 Clapp, Sebastian, Martin Höflmayer, Elena Lazarou, and Marianna Pari. 2025. "ReArm Europe Plan/Readiness 2030." https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769566/EPRS_BRI(2025)769566_EN.pdf.

24 "EUR-Lex - 12012M004 - EN - EUR-Lex." 2025. Europa.Eu. https://eur-lex.europa.eu/eli/treaty/teu_2012/art_4/oj/eng.

25 "EUR-Lex - 12016M020 - EN - EUR-Lex." 2016. Europa.Eu. https://eur-lex.europa.eu/eli/treaty/teu_2016/art_20/oj/eng.

26 "Joint Security Commitments between the European Union and Ukraine." 2024. Consilium.Europa.Eu. June 27, 2024. https://www.consilium.europa.eu/media/oredhmis/eu-ukraine-security-commitments-en.pdf.

extend civilian AI rules to defence context through which they were not designed, but that defence AI should have its own rules.[27]

Third, sovereignty is a collective project not a national one. As we have established, no member state can achieve meaningful technological sovereignty alone. The scale required in cloud infrastructure, AI, and semiconductor manufacturing exceeds any in the national industrial base. The solution as the EU has been doing is shared infrastructure, pooled research investment, and coordinated export controls on dual-use technologies. Initiatives like, ReArm Europe framework and the Defence Industry Transformation Roadmap Show that there is a will, and there are actions taken towards this. The gap remains in the institutional architecture that is supposed to deliver, but is lacking on that front.

The EU stands at an important moment, where the regulatory achievements are substantial, and industrial and infrastructural vulnerabilities are also equally real. The proposals of this section are institutionally grounded and are calibrated for these political moments, to build on existing tools and leverage the unprecedented appetite for European defence integration and target the specific gaps the analytical sections of this brief have identified.

Recommendations

Recommendation 1:

Technology priorities for the EU: dual-use AI and quantum as the domains requiring most urgent EU-level investment and coordination

Problem	Europe's lack of sovereign AI forces reliance on foreign technology and infrastructure, increasing risk.
Intervention	EDF funds, and EUDIS mechanisms can be used to fund European AI and quantum technology.
Actors	European Commission, EDF; EUDIS, European Defence Agency and EU Member States.
Immediate	Allocate current EDF funds for dual-use AI and launch spin-in calls for quantum-secure communication networks, as the risk of "Harvest now, Decrypt later" is only increasing.
Structural	Enact an EU-wide strategy and bridge the gap between civilian/military AI R&D by leveraging existing regulations like the AI Act Recital 24.
Expected outcome	Further European strategic autonomy in dual-use AI, and a sovereign, quantum-resistant communication channels (→ crucial for future military needs).

Recommendation 2:

Take advantage of existing regulations to strengthen innovation and industrial capacity.

Problem	The defence base is fragmented amongst the countries, combined with PESCO's slow timeline, and the heavy compliance costs, EU tech startups refrain from scaling in the EU.
Intervention	Shorten PESCO timeline using EDIP funding, and launch a European Tech Sovereignty Fund, similar to NATO's.
Actors	European Defence Agency, European Commission, EUDIS, EU Member states, EU Entrepreneurs.
Immediate	Use the EDIP funding to streamline PESCO's timeline, and deploy dual-use regulatory sandboxes to protect startups from bureaucratic requirements.
Structural	Institute EU digital interoperability standards across member states, and establish a sovereign public-private venture fund for startups requiring capital.
Expected outcome	Accelerated R&D, reduced SME compliance issues, and retention of strategic Tech in the EU.

27 Clapp, Sebastian. 2025. "Defence and Artificial Intelligence." https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf.

Conclusion

In conclusion, **the rapid integration of artificial intelligence and emerging technologies into critical sectors has irreversibly transformed the dynamics of global security and economic competitiveness.** For the European Union, the current geopolitical climate underscores the urgent need to transition from a predominantly regulatory stance to one that actively fosters industrial and technological capability. While absolute digital independence is neither feasible nor necessary, the EU must aggressively pursue open strategic autonomy by mitigating its critical dependencies in infrastructure, data, and technological platforms. By prioritizing targeted investments in dual-use technologies and quantum computing, reforming structural pipelines to reduce market fragmentation, and building unified frameworks for resilience and cybersecurity, Europe can successfully bridge the gap between theoretical innovation and practical deployment. Ultimately, securing Europe's future demands the recognition that technological regulation, economic competitiveness, and strategic resilience are intrinsically linked. **Only through unified, collective action can the European Union ensure it remains a sovereign actor capable of upholding its democratic values and strategic interests in an increasingly volatile global order.**

TECHNOLOGY AND FUTURE SECURITY

TECHNOLOGY & FUTURE SECURITY

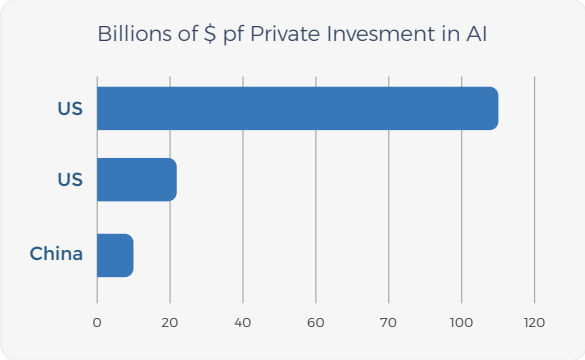
AI

AI & Quantum are the core industries that need development in the EU.

Yet, they are majoritarily controlled by American companies; AWS, Azure, Google cloud

The EU is a pioneer in Technology Regulation, while also possessing one of the world's largest internal and most cohesive markets.

So why is the EU still behind the US, despite all it has?



TECHNOLOGY AND ITS IMPACT ON SECURITY

Real-time AI integration in Ukraine, Gaza, and Iran highlights the centrality of ISR, drone swarms, and predictive logistics.

This, coupled with the increase of attacks like "Harvest now, Decrypt later", until quantum is fully developed and accessible, are real threats for the security of the EU.



Proposals

1. Technology priorities for the EU: dual-use AI and quantum as the domains requiring most urgent EU-level investment and coordination
2. Reform crucial organs of the EU to reduce the red-tape that surrounds innovation
3. Strategically increase investments, by making a European endeavour to simplify the process for entrepreneurs from all the EU.

The crucial part is balancing Security, Competitiveness and Regulation.

Glossary of abbreviations

AI	Artificial Intelligence
AR	Augmented Reality
ATR	Automatic Target Recognition
AWS	Amazon Web Services
CSA2	Cyber Security Act 2 (Commission proposal)
EDA	European Defence Agency
EDF	European Defence Fund
EDTs	Emerging Disruptive Technologies
EDIP	European Defence Industry Programme
ENISA	European Agency for Cybersecurity
EPRS	European Parliamentary Research Service
EU	European Union
EUDIS	EU Defence Innovation Scheme
FPV	First Person View
FRONTEX	European Border and Coast Agency
GDPR	General Data Protection Regulation
IHL	International Humanitarian Law
INTCEN	European Union Intelligence and Situation Centre
ISR	Intelligence, Surveillance and Reconnaissance
IoT	Internet of the Things
LAWS	Lethal Autonomous Weapons
NATO	North Atlantic Treaty Organization
NLP	Natural Language Processing
OODA	Observe, Orient, Decide, Act
OSINT	Open-source intelligence
PLA	The People's Liberation Army
PNT	Positioning, Navigation and Timing
PSYOPs	Psychological Operations
PESCO	Permanent Structured Cooperation
SAR	Synthetic-Aperture radar
SMEs	Small and medium-sized enterprises
SIGINT	Signals intelligence
US	United States
VR	Virtual Reality



EQUIPO EUROPA



FOCAL CHAPTER 3

CLIMATE, HEALTH AND HUMAN SECURITY

REDEFINING EU SECURITY: CLIMATE, HEALTH AND INTERCONNECTED RISKS

Authors: Noemí Puértolas Puyal, Adriana Ruiz Adán, Camila Guandinango Ramos, Carolina Matias Carvalho.
Reviewers: María Vallejo Fernández and María Villaverde Temes.

Forum on the Future of the EU
EUROPEAN SECURITY in a Changing World

EXECUTIVE SUMMARY

his paper examines how the European Union's security policy should evolve to address increasingly interconnected environmental, health and societal risks. It argues that traditional security approaches, centred primarily on territorial defence and military capabilities, are no longer sufficient to respond to contemporary challenges such as climate change, migration, public health emergencies and vulnerabilities affecting critical infrastructure. Rather than existing as separate policy domains, these threats interact across sectors, generating effects that undermine the resilience, stability and strategic autonomy of the European Union.

The paper analyses the current legal and institutional framework across four key areas within the EU: climate security, migration, health security and critical infrastructure protection. While the Union has progressively developed comprehensive legal instruments and governance mechanisms in each domain, the analysis identifies persistent structural weaknesses, including institutional fragmentation, uneven implementation across Member States, divergent national priorities and limited integration between policy sectors.

The study further demonstrates that many current security challenges share common characteristics: they are transnational, mutually reinforcing and rooted in systemic vulnerabilities rather than isolated events. Climate change acts as a threat multiplier for migration, health risks and infrastructure resilience.

Building on this analysis, the paper proposes a more integrated European security architecture based on resilience, prevention and cross-sectoral coordination. It recommends strengthening common risk assessment and early-warning systems, improving information sharing, harmonising implementation across Member States, and embedding climate, migration, health and infrastructure considerations within a coherent strategic framework.

Keywords

European security; Climate security; Migration; Health security; Critical infrastructure; Resilience.

INTRODUCTION

Robert Schuman articulated **the foundations of the European Union as the idea of war becoming "merely unthinkable, but materially impossible"** [1]. This foundational vision placed interdependence at the centre of European security: peace was to be secured not primarily through deterrence, but through structural integration. Over time, this internal logic has expanded outward, progressively shaping the European Union's role as a security actor in an increasingly unstable global environment.

Seventy-five years later, Roberta Metsola states that "Europe must be responsible for its own security" [2]. Yet the meaning of security in the European context has become increasingly complex. Traditional, state-centric frameworks based on territorial defence and military capability are increasingly insufficient to capture today's threats, which are often systemic, diffuse, and mutually reinforcing.

This paper therefore argues for complementing a territory-based approach with a systemic perspective, as Europe's security challenge lies not only in what crosses its borders but in what propagates through its systems. Accordingly, the following sections analyse climate change, migration, health, and critical infrastructure as structural threats to European security, examining for each the current EU approach, existing vulnerabilities, and factors shaping future policy development, before concluding with recommendations for an EU security framework capable of addressing these interconnected challenges.

Affects →	Climate	Migration	Health	Critical Infrastructure
Climate		High	High	High
Migration	Medium		High	Medium
Health	Low	Medium		High
Critical Infrastructure	High	Medium	High	

Low
Medium
High

Source: own-elaboration

Figure 0: Heatmap of Threat Interdependence

1 European Union, "Schuman Declaration (9 May 1950)," official text, EU Historical Archives / CVCE

2 European Parliament. "Plenary Speech by Roberta Metsola on European Security." Verbatim Report of Proceedings. European Parliament Official Archives, 2025.

1 CLIMATE CHANGE AS A STRUCTURAL THREAT

1.1 CURRENT EU APPROACH

The European Union currently addresses climate change through a solid legal and strategic framework, progressively built through the transition from soft law to hard law instruments[3]. This process is reflected in the consolidation of binding legislation such as the European Climate Law, the EU Emissions Trading System (EU ETS) and Regulation (EU) 2023/1115 on deforestation-free products, alongside the European Green Deal as the Union's overarching policy strategy. Likewise, Article 191 TFEU[4] enshrines fundamental principles such as precaution, prevention, and the "polluter pays" principle, which guide the Union's climate action.

In the field of security, strategic documents such as the Strategic Compass explicitly recognise climate change as a threat multiplier, while the EU Climate Adaptation Strategy identifies growing risks for critical infrastructure, public health, ecosystems, and the economy. The EU has also strengthened its response capacity through the Civil Protection Mechanism, which coordinates interventions against wildfires, floods, and other climate-related disasters. Externally, climate diplomacy has become a pillar of the Union's international action[5], particularly in vulnerable regions such as the Sahel, the Mediterranean, or the Arctic. All of this is articulated within a multilevel governance system in which competences are shared between the EU, Member States, and regional and local authorities, under a framework reinforced by the Aarhus Convention[6], which guarantees public participation and access to environmental information.

This growing integration reflects the progressive recognition of climate change as a cross-cutting issue within EU policy-making, where environmental action, resilience planning, and security considerations increasingly overlap. In this sense, climate policy is no longer confined to environmental regulation but is progressively embedded in broader governance and security frameworks at Union level.



Figure 1: Evolution of the EU Security framework
Source: own-elaboration

1.2 MAIN VULNERABILITIES

Despite these advances, **significant structural problems persist that limit the full integration of climate change into European security policy.** Institutional fragmentation is one of the main obstacles[7], as there is no unified climate security framework capable of coherently coordinating environmental, energy, defence, health, and external action policies.

The implementation of climate norms also remains uneven across Member States [8], and monitoring and enforcement mechanisms continue to be insufficient, especially at the international level, where many agreements lack effective sanctions. Legal uncertainty surrounding environmental principles such as precaution, non-regression, or climate justice further complicates their integration into security and defence policies. Added to this are the limitations arising from shared competences and the principle of subsidiarity, which slow down decision-making in climate emergencies and generate significant disparities in territorial resilience.

3 René Javier Santa María Arinas, "La respuesta internacional," in Curso Básico de Derecho Ambiental General (Bizkaia: Instituto Vasco de Administración Pública / Herri-Arduralaritzaren Euskal Erakundea, n.d.), 32.

4 European Union, Treaty on the Functioning of the European Union (TFEU), Article 191 (consolidated version, EUR-Lex), accessed June 23, 2026, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12008E191:ES:HTML

5 Teresa Fajardo del Castillo, "Conclusiones," in La diplomacia del clima de la Unión Europea, ed. Alejandro del Valle Gálvez (Madrid: Editorial Reus, n.d.).

6 Organization of American States, Acceso a la información y desarrollos del Convenio de Aarhus, accessed June 23, 2026, https://www.oas.org/es/sla/ddi/docs/acceso_informacion_desarrollos_convenio_aahrus.pdf

7 Oriol Casanovas and Ángel J. Rodrigo, Compendio de Derecho Internacional Público (1994).

8 Alenza García, José Francisco. 2001. Manual de Derecho Ambiental.

Externally, the EU faces **growing vulnerabilities linked to instability in neighbouring regions** affected by droughts, food insecurity, and climate-induced displacement[9], as well as its dependence on critical raw materials and supply chains exposed to global disruptions.

1.3 CONDITIONING FACTORS

The effectiveness of EU climate security policy is conditioned by economic diversity among Member States, differing energy dependencies, technological capacities, and political priorities. Global interdependence further constrains European strategic autonomy, particularly in relation to critical minerals and energy transitions.

Climate change also acts as a threat multiplier for other structural challenges. Environmental degradation contributes to migration pressures, increases risks to public health, and exposes the vulnerability of critical infrastructure. As a result, climate security cannot be treated in isolation but must be understood as a cross-cutting factor affecting the broader European security architecture.

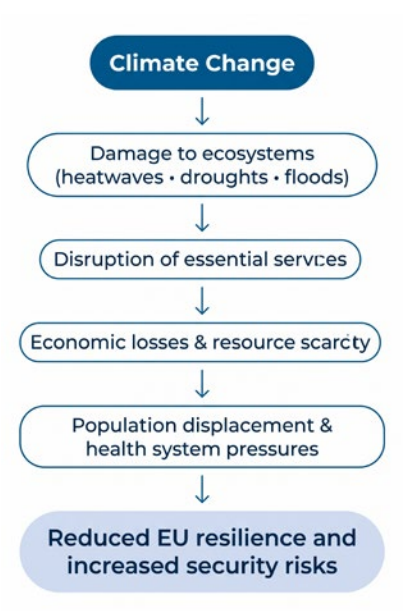


Figure 2: Cascading Effects of Climate Change on European Security

Source: own-elaboration

2 MIGRATION AS A STRUCTURAL THREAT

Since the beginnings of European integration, **migration has represented one of the most pressing and complex branches of EU policy**. Due to Southern European countries' proximity to historically unstable areas, fluctuating migration crises have repeatedly threatened European shelter capacities. These fluctuations are not isolated crises but symptoms of broader structural imbalances, including conflict, inequality, climate stress and governance gaps.

2.1 CURRENT EU APPROACH

Having experienced the 2015–2016 asylum crisis, when the EU registered about 1.26 million first-time asylum applicants in 2015 and 1.20 million in 2016, as well as the mass displacement caused by Russia's full-scale invasion of Ukraine in 2022, **the EU has since overhauled its migration and asylum framework.**

This legal framework started off as a foundational approach to international protection, guided by six legal instruments[10]: the Eurodac Regulation, the Temporary Protection Directive, the Reception Conditions Directive, the Dublin Regulation replacing the 1990 Dublin Convention, the Qualification Directive, and the Asylum Procedures Directive. It was subsequently reformed following the Hague Programme in 2005[11], and again in 2015 to increase the efficiency and fairness of the protection system despite peaking migratory flows[12].

During Ursula von der Leyen's first mandate, the Commission proposed the Pact on Migration and Asylum in 2020. The Pact entered into force in June 2024 and entered into application on 12 June 2026. In February 2026, the Council formally adopted the first EU-wide list of safe countries of origin and revised the rules governing the safe third country concept. Under the latter, Member States may, subject to specified conditions, declare

9 European Commission, "Press release," European Commission Press Corner, accessed June 25, 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3492.

10 European Union Agency for Asylum. Review of The evolution of the Common European Asylum System (CEAS), 2024. https://www.euaa.europa.eu/sites/default/files/2024-06/2024_CEAS_timeline-v8.pdf.

11 European Union Agency for Asylum. Review of The evolution of the Common European Asylum System (CEAS), 2024. https://www.euaa.europa.eu/sites/default/files/2024-06/2024_CEAS_timeline-v8.pdf.

12 European Union Agency for Asylum. Review of The evolution of the Common European Asylum System (CEAS), 2024. https://www.euaa.europa.eu/sites/default/files/2024-06/2024_CEAS_timeline-v8.pdf.

certain asylum applications inadmissible without examining their substance[13].

2.2 MAIN VULNERABILITIES

The figure illustrates **the uneven distribution of migration across the EU**. Southern[14] and lower-income[15] Member States, particularly Spain (1.08M migrants out of a total of 4.15M), receive disproportionately high numbers of arrivals compared to the rest of the EU, creating **unequal procedural and administrative burdens.**

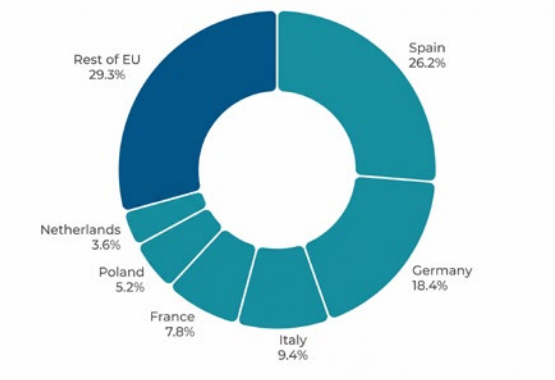


Figure 3: Total migrant inflows into the EU, 2024
Source: own-elaboration, with data from Eurostat (2024)

Although the EU often frames migration as an overwhelming challenge, the data suggest otherwise. In 2025, the EU received 669,365 first-time asylum applications, 26.6% fewer than in 2024. The principal challenge highlighted here is therefore not simply the absolute number of applications but their distribution and the administrative capacity of Member States. Notwithstanding, **treating migration as a developing-country problem and founding poorer societies in an attempt to reduce migration will not avoid millions of inflows arriving in Europe each year.** As de Haas states, economic development usually leads to a short-term increase in migration, as aspirations and capabilities of citizens increase in relation to affording the costs and risks of emigrating[16][17]. This contradicts the logic underlying much of the EU's external migration policy, which frames development aid to origin countries as a containment tool.

Beyond the development stage, **migration drivers rarely act in isolation**: conflict, economic inequality and climate stress interact rather than accumulate, with the IPCC and IOM describing climate change as a "threat multiplier" for mobility that intensifies existing inequality and conflict rather than displacing people on its own[18]. Containment and deterrence policies compound these pressures, straining relations with transit states[19], fuelling social polarisation within Member States, and generating human rights costs, from pushbacks to ECtHR condemnations[20][21], that have eroded public trust, as reflected in the NGO and academic criticism surrounding the 2024 Pact[22].

2.3 CONDITIONING FACTORS

The effectiveness of EU migration policy is conditioned, first, by a structural dependency inherent to the externalization model itself. **By outsourcing border enforcement** to countries such as Morocco, Tunisia and Turkey, **the EU transforms migration pressure into diplomatic vulnerability**. These states become gatekeepers whose cooperation can be withdrawn or instrumentalised during bilateral disputes[23], as illustrated by the 2021 Ceuta crisis.

Divergent interests among Member States further condition the Union's capacity to respond coherently. Frontline states such as Spain, Italy and Greece bear a disproportionate share of arrivals and consequently favour stronger solidarity mechanisms, whereas other Member States remain comparatively isolated from these pressures. Poland and Hungary's opposition to the Pact's man-

13 Directorate-General for Migration and Home Affairs. Review of Commission Welcomes Political Agreement on First EU List of Safe Countries of Origin and New Rules to Facilitate the Application of the Safe Third Country Concept. Migration and Home Affairs, December 19, 2025. https://home-affairs.ec.europa.eu/news/commission-welcomes-political-agreement-first-eu-list-safe-countries-origin-and-new-rules-facilitate-2025-12-19_en.

14 Eurostat. Review of Immigration by Broad Group of Country of Previous Residence. Europa.eu, 2025. https://ec.europa.eu/eurostat/databrowser/view/MIGR_IMM12PRV__custom_7737977/bookmark/map?lang=en&bookmarkId=87378501-31e9-4e43-8f9c-dea6fdff1028&c=1696843667748.

15 S. Galan. "GDP per Capita EU Member States 2024| Statista." Statista, June 20, 2025. https://www.statista.com/statistics/1373462/gdp-per-capita-eu-member-states-2024/?srsltid=afmboorc5xqys3kksdtmsoqpagafqu6-q0bphrfdsmdldfde3wxyx-nw.

16 De Haas, Hein. "Center on Migration, Citizenship and Development 2007 Migration and Development: A Theoretical Perspective," 2007. https://heindehaas.org/wp-content/uploads/2015/05/de-haas-2007-comcad-wp-migration-and-development-theory.pdf.

17 Hein de Haas. How Migration Really Works. Hachette UK, 2023.

18 Mcauliffe, and Ceriani Cernadas. "World Migration Report 2026." International Organization for Migration (IOM), 2026. https://publications.iom.int/books/world-migration-report-2026.

19 Chireno, Giulianna. "Morocco'S Diplomatic Leverage: Influencing Relations with Spain and the EU ," 2025. https://ipr.blogs.ie.edu/wp-content/uploads/sites/574/2025/05/Moroccos-Diplomatic-Leverage_-Influencing-Relations-with-Spain-and-the-EU.pdf.

20 Euromed Rights. "ECHR'S Condemnation of Cyprus' Pushbacks to Lebanon - EuroMed Rights." EuroMed Rights, October 8, 2024. https://euromedrights.org/publication/echrs-condemnation-of-cyprus-pushbacks-to-lebanon/.

21 Refugee Rights Europe. "Pushbacks and Rights Violations at European Borders." Refugee Rights Europe, July 2020. https://refugee-rights.eu/wp-content/uploads/2020/07/RRE_PP_Pushbacks_English.pdf.

22 Jouni Häkli, Gintarė Kudžmaitė, and Kirsi Pauliina Kallio. "Devaluing Personhood: The Framing of Migrants in the EU'S New Pact on Migration and Asylum." Transactions of the Institute of British Geographers 49, no. 4 (February 13, 2024). https://doi.org/10.1111/tran.12676.

23 Martini, Lorena Stella, and Tarek Megerisi. "Road to Nowhere: Why Europe's Border Externalisation Is a Dead End." European Council on Foreign Relations, December 14, 2023. https://ecfr.eu/publication/road-to-nowhere-why-europes-border-externalisation-is-a-dead-end/.

datory solidarity mechanism illustrates persistent political divergence among Member States, even though the relevant Pact legislation was adopted by a qualified majority in the Council.

A third conditioning factor concerns the climate-migration intersection as a future risk rather than a resolved one. As discussed above, IPCC projections indicate rising displacement risks across Africa, particularly in the Sahel[24], suggesting that Mediterranean migration pressures are likely to intensify. Finally, a demographic contradiction runs beneath the EU's entire migration policy: **while an ageing workforce increasingly requires migrant labour to sustain economic productivity, the Union's policy architecture still remains built almost exclusively around exclusion and deterrence**[25].

3 HEALTH AS A STRUCTURAL THREAT

Large-scale and irregular mobility flows also interact with public health systems, particularly in terms of surveillance capacity and cross-border disease transmission.

3.1 CURRENT EU APPROACH

Health security has become a central component of the European Union's security agenda. According to the briefing paper "Enhancing health security", for the Public Debate on the Future Health Priorities of the European Union (2024), health security is defined by all the activities and measures taken on a global, national, regional and local scale, to protect populations from emerging health threats. These activities and measures focus on the prevention, detection, and response to a diverse cluster of the mentioned threats.

Currently, the EU approaches health security through the framework of the European Health Union, which was significantly strengthened following the COVID-19 pandemic. It aims to **improve cooperation among Member States, ensure the availability of medical supplies, and enhance preparedness and response capacities**. Key instruments include the strengthened mandate of the European Centre for Disease Prevention and Control (ECDC) under Regulation (EU) 2022/2370, the reinforced crisis-preparedness role of the European Medicines Agency (EMA) under Regulation (EU) 2022/123, the Health Emergency Preparedness and Response Authority (HERA), and Regulation (EU) 2022/2371 on serious cross-border threats to health[26]. This Regulation established the Union Prevention, Preparedness and Response Plan and reinforced mechanisms for surveillance, risk assessment, early warning, and coordinated action among Member States.

The Health Security Committee, established under Decision No. 1082/2013/EU and reinforced by Regulation (EU) 2022/2371[27], plays a crucial role in coordinating prevention, preparedness, and response planning for serious cross-border health threats. In addition, **EU health security policy focuses on three key areas**: surveillance systems capable of detecting threats at an early stage, resilient health systems that can continue providing essential services during crises, and research and development aimed at improving diagnostics, treatments, and vaccines.



Figure 4: EU Health Security cycle
Source: own-elaboration

24 IPCC. "Summary for Policymakers." Climate Change 2023: Synthesis Report. Contribution of Working Groups I, II and III to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change. Geneva, Switzerland: IPCC, 2023. https://doi.org/10.59327/IPCC/AR6-9789291691647.001.

25 Draghi, Mario. 2024. The Future of European Competitiveness. Publications Office of the European Union5. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en.

26 European Union, Regulation (EU) 2022/2371 of the European Parliament and of the Council on serious cross-border threats to health, EUR-Lex, https://eur-lex.europa.eu/eli/reg/2022/2371/oj/eng.

27 European Union, Regulation (EU) 2022/2371 of the European Parliament and of the Council on serious cross-border threats to health, EUR-Lex, https://eur-lex.europa.eu/eli/reg/2022/2371/oj/eng.

3.2 MAIN VULNERABILITIES

Despite these advances, several challenges remain. The COVID-19 pandemic exposed significant differences in preparedness levels among Member States and demonstrated that **the effectiveness of EU-level action depends heavily on national capacities**. Delays in identifying outbreaks, uneven healthcare resources, differences in national responses and persistent inequalities affecting lower-income communities can undermine a coordinated European reaction. Furthermore, health threats do not respect national borders, making purely national solutions insufficient. The success of EU health security policy therefore depends not only on European coordination but also on effective global cooperation[28].

3.4 CONDITIONING FACTORS

Several additional factors condition the effectiveness of EU health security. The EU Global Health Strategy highlights that health outcomes are increasingly influenced by broader challenges, including climate change, environmental degradation, biodiversity loss, antimicrobial resistance, demographic change, and social inequalities. Vulnerable populations are often disproportionately affected by health crises, revealing persistent inequalities in access to healthcare and essential medical services[29]. Moreover, **global interconnectedness through travel, trade, and migration increases the speed at which health threats can spread across borders**.

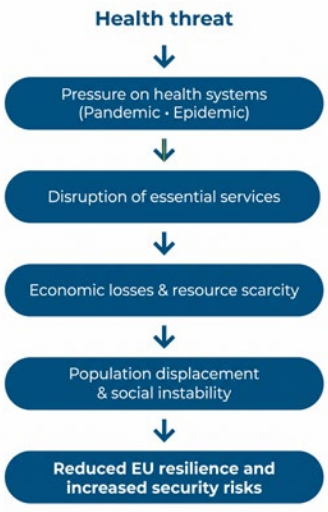


Figure 5: Cascading Effects of Health Threats on European Security Source: own-elaboration

4 INFRASTRUCTURE AS A STRUCTURAL THREAT

The resilience of health systems itself depends on critical infrastructure, particularly digital, logistical and energy networks.

4.1 CURRENT EU APPROACH

In an ever more interconnected, globalised world sustained by physical and digital networks, **infrastructure protection has emerged as one of the EU's main security pillars.** As defined by Renda (2010), critical infrastructure comprehends the structural backbone "whose failure would result in substantial damage to society and/or the economy"[30], which includes fields such as those of energy, communications, banking, transportation or public government services, among others.

The increasing interdependence that characterises today's international society relies on a network of infrastructures that serves citizens, businesses and governments in industrialised economies. Critical Infrastructure Protection (CIP)[31] is thus essential to guarantee the well-functioning of energy supplies, water distribution, healthcare, bank safety, transport services, etc., concerning potential risks that may threaten security at domestic and international levels.

Additionally, due to recent technological advances including the emergence of AI, the transformation of social media into regular information sources or the rise of new models of e-commerce, teleworking and data brokering, information structures have grown into indispensable elements for economic, social and political survival.

For decades, **critical infrastructure protection at EU level has been targeted by a fragmented and inefficient approach,** hampering coordination between Member States and harmonised implementation. In 2008, the first legal instrument tackling critical infrastructure protection was established, known as the European Critical Infrastructure Directive. This directive only applied to the energy and transport sectors, establishing a com-

28 Mauer, Scarpetti, and Wismar, A Public Debate on the Future Health Priorities of the European Union: Outcomes, Insights and Ideas for Action. Copenhagen: WHO Regional Office for Europe / European Observatory on Health Systems and Policies, 2024, pp. 72–74

29 European Commission. International Health Security / Global Health Strategy Report 2022. 2023. (https://health.ec.europa.eu/system/files/2023-10/international_ghs-report-2022_en.pdf

30 Renda, Andrea. Protecting Critical Infrastructure in the EU: CEPS Task Force Report. 2010. https://cdn.ceps.eu/wp-content/uploads/2010/12/Critical%20Infrastructure%20Protection%20Final%20A4.pdf.

31 The abbreviated form CIP will be used from now on to refer to "Critical infrastructure protection"

mon procedure for the designation of critical entities and linking owners and operators. In 2022, the CER Directive was adopted to ensure the provision of essential services during major disruptions, including natural disasters, terrorist attacks, medical emergencies or hybrid threats[32].

Notwithstanding, **Member States are at different stages in the implementation and development of robust CIP policies.** Both critical infrastructure assets and the partnerships that support their operation are distributed across the European Union. Member States maintain distinct relationships with private operators and multinational companies, while essential infrastructure networks themselves span multiple national jurisdictions.

Table 1: Comparative CER Directive and NIS2 Directive

Aspect	CER Directive	NIS2 Directive
Focus	Physical resilience	Cybersecurity
Sectors	11 essential sectors	18 critical sectors
Risk	All relevant natural and man-made risks, including hybrid and public-health threats	Cyber threats
Objective	Continuity of services	Network security
Main actors	Critical entities	Essential and important entities

Source: own-elaboration

4.2 MAIN VULNERABILITIES

As the Global Risks to the EU 2026 puts it, **the most plausible and potentially harmful threat to EU security is a disruptive hybrid attack on critical infrastructure,** such as damage to subsea networks or large-scale power outages. The report underscores the EU's unpreparedness regarding energy, digital and transport systems, and predicts future damages against European cables, pipelines or networks that will inevitably force the strengthening of EU resilience measures[33]. Besides a major hybrid attack directly targeting EU critical infrastructure, some of the most concerning risks identified in Global Risks to the EU 2026 include cyber threats, natural disasters, Russia's war against Ukraine and the scenario of a future US withdrawal from security guarantees to European allies. In this regard, Member States' responses are unaligned and, in many cases, contradictory.

On the one hand, risk perception asymmetries lead to policy coordination challenges in terms of CIP. The security environment within the EU is characterised by different threat perceptions among Member States. Eastern European countries, given their proximity to Russia, prioritise military and territorial security concerns, while Western and Mediterranean countries may place less emphasis on these risks due to their geographical distance. These differing priorities can hinder the development of a unified and comprehensive CIP framework that effectively addresses the full spectrum of threats and can be translated into coherent national-level measures[34].

On the other hand, as of 29 April 2026, the Commission had referred Bulgaria, France, Luxembourg, the Netherlands, Poland, Spain and Sweden to the Court of Justice of the European Union for failing to transpose and notify the CER Directive fully. creating a fragmented legal landscape that leaves the EU vulnerable to cascading failures and coordinated hybrid attacks. Transposition mismatches ultimately entail regulatory gaps, rapid propagation of damages due to interconnectedness, and the inefficiency of outlined responses to security threats[35]. Moreover, the lack of a centralised execution perpetuates national breaches in implementation and allows for enforcement black holes that hinder collective action in CIP.

4.3 CONDITIONING FACTORS

The European Union has been working towards the construction of a resilient CIP policy by allocating 200 million euros in total project cost[36].

32 European Union. Directive (EU) 2022/2557 of the European Parliament and of the Council. Official Journal of the European Union, December 27, 2022.

33 Anghel, Veronica. Global Risks to the EU 2026. European University Institute, 2026 https://doi.org/10.2870/1351636

34 Slakaityte, Veronika, and Izabela Surwillo. Protecting EU's Critical Infrastructure: The Fight Intensifies in the Cyber Realm. Danish Institute for International Studies, October 23, 2024. (https://www.diis.dk/en/research/protecting-eus-critical-infrastructure-the-fight-intensifies-in-the-cyber-realm).

35 Lekatis, George. The Critical Entities Resilience Directive (CER). n.d. (https://www.critical-entities-resilience-directive.com/).

36 Levak, Jelena, Anita Britvec, and Krishna Chandramouli. Critical Infrastructure Protection Challenges and Best Practices in the Public Administration Sector: A 2030 Outlook. June 11, 2025.

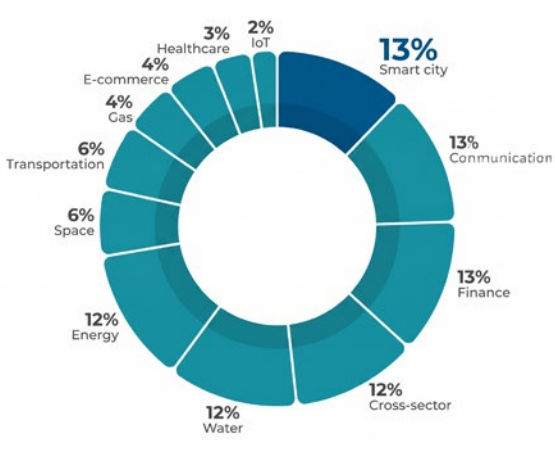


Figure 6: Financial allocation by CIP area
Source: own-elaboration

As previously mentioned, the CER Directive was adopted in 2022 to introduce a comprehensive framework aimed at enhancing the resilience of critical entities across eleven key sectors (energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space, production, processing and distribution of food) to non-cyber risks. Moving beyond the narrower concept of critical infrastructure protection, it adopts a resilience-oriented perspective focused on ensuring the continuity of essential services throughout the entire crisis cycle, including prevention, response and recovery. Under the Directive, critical entities must assess potential risks, adopt measures to strengthen resilience, and notify authorities of major disruptions to their operations. In addition, the establishment of the Critical Entities Resilience Group (CERG) provides a mechanism for supporting the Commission, fostering coordination among Member States, and encouraging information sharing on issues related to the Directive's implementation[37].

Concurrently, the NIS2 Directive was also adopted in 2022 to set the EU's primary cybersecurity framework, implementing common requirements for entities operating in eighteen critical sectors. Aside from establishing security obligations, it **encourages Member States to develop national cybersecurity strategies and strengthen cooperation mechanisms for addressing cross-border cyber incidents.** Cybersecurity, in this context, entails protecting network and information systems and mitigating the impact of cyber threats on users and other affected stakeholders[38].

In June 2024, the Council adopted a Recommendation establishing the EU Critical Infrastructure Blueprint to improve coordination in response to cross-border incidents disrupting critical infrastructure with significant cross-border relevance[39]. Furthermore, the 2022 Council Recommendation was integrated to enhance preparedness, coordinated response mechanisms, information sharing and cross-border cooperation in order to reinforce the resilience of critical infrastructure across the EU. By promoting an all-hazards approach and complementing the CER and NIS2 Directives, it strengthens the protection and continuity of essential services against physical, cyber and hybrid threats[40].

Nevertheless, the EU-CIP White Paper (2025) still identified serious gaps in risk modelling and scenario planning, crisis coordination across local, national and EU levels, and legacy systems and supply chain security. Altogether, these vulnerabilities reflect the need for accurate assessment at both national and EU levels in order to efficiently target potential disruptions;: the urgency for cross-sectoral, horizontal regulations that combine collective needs with stakeholder perspectives, and the importance of securing all links of the European supply chains[41].



Figure 7: Cascading Effects of Critical Infrastructure on European Security .Source: own-elaboration

37 European Commission, "First Biennial Work Programme of the Critical Entities Resilience Group 2025-2026," n.d.

38 European Commission, "Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) | Shaping Europe's Digital Future," digital-strategy.ec.europa.eu, September 14, 2023, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

39 Directorate-General for Migration and Home Affairs, "Critical Infrastructure Blueprint Adopted to Strengthen the EU's Capacity to React to Cross-Border Disruptive Incidents," Migration and Home Affairs, June 26, 2024, https://home-affairs.ec.europa.eu/news/critical-infrastructure-blueprint-adopted-strengthen-eus-capacity-react-cross-border-disruptive-2024-06-26_en

40 Council of the European Union, "COUNCIL RECOMMENDATION of 8 December 2022 on a Union-Wide Coordinated Approach to Strengthen the Resilience of Critical Infrastructure ," December 8, 2022.

41 Levak, Jelena, Anita Britvec, and Krishna Chandramouli. "Critical Infrastructure Protection Challenges and Best Practices in the Public Administration Sector: A 2030 Outlook". June 11, 2025.

EMERGING STRATEGIC CHALLENGE: SUPPLY CHAINS AND CIRCULAR ECONOMY

Beyond climate, migration, health and critical infrastructure, **an emerging structural vulnerability cuts across all four domains: the European Union's dependence on external suppliers for critical raw materials (CRMs) and the fragility of the supply chains that sustain its green and digital transitions**. Rare earth elements, lithium, cobalt and other strategic inputs are indispensable for renewable energy technologies, electric vehicles, semiconductors, defence systems and medical equipment — meaning that a disruption in this domain does not remain contained but propagates directly into climate policy, infrastructure resilience and health system capacity.

The Union currently relies heavily on a small number of third-country suppliers for these materials, with China holding a dominant position across several stages of extraction, processing and refining. To address this, the EU adopted the Critical Raw Materials Act (CRMA) in 2024, setting 2030 benchmarks under which Union capacity should approach or reach 10% of annual consumption or extraction, 40% for processing and 25% for recycling, while no more than 65% of the Union's annual consumption of each strategic raw material at any relevant stage of processing should come from a single third country[42]. The Commission has since approved dozens of strategic projects across Member States and partner countries to accelerate these goals, and in December 2025, the Commission adopted the RESourceEU Action Plan, which announced further measures to retain critical secondary raw materials in the EU, including proposed restrictions concerning rare-earth permanent-magnet scrap and targeted measures concerning aluminium scrap[43].

Circular economy policy is closely intertwined with this supply security agenda. The EU's recycling rate for critical raw materials remains marginal compared to the ambition set out in the CRMA, exposing a structural gap between the Union's stated targets and its current industrial capacity. The forthcoming Circular Economy Act, planned for the third quarter of 2026, is expected to include measures aimed at increasing the recovery of critical materials from waste streams and reducing reliance on primary imports[44].

This emerging challenge illustrates the same structural pattern identified throughout this chapter: fragmented governance, uneven Member State capacities, and a mismatch between the pace of policy ambition and the pace of implementation. Just as climate change, migration, health and infrastructure vulnerabilities interact and reinforce one another, supply chain fragility acts as an underlying condition that can amplify each of the four structural threats analysed above. Securing critical supply chains and accelerating circularity should therefore be treated not as a separate industrial policy question, but as a foundational layer of EU security architecture.

42 European Union (2024) Regulation (EU) 2024/1252 of the European Parliament and of the Council establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724 and (EU) 2019/1020 (Critical Raw Materials Act). Official Journal of the European Union.

43 European Commission (2025) RESourceEU Action Plan – Strengthening the EU's Access to Critical Raw Materials. Brussels: European Commission.

44 European Commission (forthcoming 2026) Circular Economy Act. Brussels: European Commission.

POLICY PROPOSALS

Previous analysis shows that the EU main challenge is not the lack of security instruments, but the fragmented governance of increasingly interconnected risks. Climate change, migration, health emergencies and critical infrastructure vulnerabilities interact across sectors, requiring a more integrated and preventive approach to security. Building on these findings, this section presents two complementary proposals aimed at strengthening the EU's capacity to anticipate, coordinate and respond to complex transnational threats.

Recommendation 1

STRENGTHENING INTEGRATED RISK ASSESSMENT AND PREVENTION

The European Union should strengthen its capacity to anticipate and prevent interconnected security risks by integrating climate, migration, health and critical infrastructure considerations into a common risk assessment framework. Contemporary security threats are increasingly interconnected, requiring preventive governance capable of identifying cross-sectoral vulnerabilities before they escalate into crises.

I. Integrate climate risk assessments into all security planning, ensuring that policies, missions and programmes systematically evaluate the implications of extreme climate events, environmental degradation and resource scarcity. Climate change should be recognised as a cross-cutting security risk that influences migration, public health and the resilience of critical infrastructure.

II. Greater investment is needed in common indicators, shared monitoring systems and interoperable early-warning mechanisms. Although advanced tools such as Copernicus already exist, their integration into security decision-making remains limited. Similarly, surveillance systems in the health sector should continue to be strengthened to improve the early detection of cross-border threats.

III. Adopt a long-term approach to migration governance by incorporating climate, conflict and demographic risk assessments into migration planning. Anticipatory planning would improve preparedness for future migration pressures while supporting more resilient migration management.

IV. Risk assessment methodologies for critical infrastructure should be further harmonised across Member States to better anticipate cascading failures affecting interconnected European systems. Improved information sharing and joint preparedness exercises would strengthen cross-border coordination and facilitate more effective responses during complex crises.

The overall objective is to move from reactive crisis management towards a preventive security model based on shared situational awareness, early warning and coordinated action. Successful implementation of this proposal should build on existing EU instruments and agencies rather than creating new institutional structures. Strengthening cooperation between the European Commission, relevant EU agencies and Member States through common methodologies, interoperable information systems and regular joint risk assessments would improve the Union's capacity to anticipate and respond to interconnected threats. A gradual implementation, supported by shared standards and continuous monitoring, would facilitate coordination while making efficient use of existing resources.

Recommendation 1: Strengthening integrated risk assessment and prevention

Problem	Fragmented risk assessment limits anticipation of interconnected threats.
Intervention	Integrate risk assessment, monitoring and early-warning systems across sectors.
Actors	European Commission, EU agencies, Member States.
Immediate (0–18 months)	Common indicators, shared data and joint risk assessments established.
Structural (2–5 years)	Improved prevention and cross-sector coordination.
Expected outcome	Earlier detection and greater EU resilience.

Recommendation 2

REINFORCING GOVERNANCE AND IMPLEMENTATION

The European Union should reinforce the implementation of existing security frameworks through stronger coordination, greater policy coherence and a governance model centred on resilience. Rather than creating new legal instruments, the priority should be to improve the integration and consistent implementation of existing policies across Member States.

I. Develop a European Climate Security Strategy to provide a common framework integrating climate considerations into defence, energy, health, civil protection and external action policies.

II. The implementation of the New Pact on Migration and Asylum should be strengthened through a stronger solidarity mechanism that distributes responsibilities more equitably among Member States while improving the operational capacity of frontline countries.

III. Health security should continue evolving towards a more integrated model by strengthening health systems, reducing disparities in preparedness, enhancing cross-border coordination and consolidating the One Health approach.

IV. Critical infrastructure protection requires stronger cross-sectoral and cross-border coordination through harmonised regulatory approaches, more consistent implementation of the CER and NIS2 Directives, and closer cooperation between public authorities, private operators and EU institutions.

Together, these measures would reduce institutional fragmentation, improve policy coherence and strengthen the resilience of the European security architecture. The implementation of this proposal requires sustained political commitment and close cooperation among EU institutions, Member States and relevant stakeholders. Rather than introducing new legislation, efforts should focus on ensuring the consistent application of existing frameworks, improving cross-sectoral coordination and promoting the exchange of best practices. Regular monitoring and evaluation would help identify implementation gaps, strengthen accountability and support the gradual development of a more coherent and resilient European security architecture.

Conclusion

The European Union has progressively expanded its understanding of security beyond its traditional focus on territorial defence, increasingly recognising climate change, migration, public health and critical infrastructure resilience as essential components of its strategic agenda. This evolution reflects the growing complexity of the current security environment, in which risks are increasingly transnational and interconnected, capable of affecting societies, economies and institutions. Despite significant legislative and institutional progress, these challenges continue to be addressed through fragmented governance structures that struggle to match the systemic nature of emerging threats.

The analysis demonstrates that **climate change, migration, health emergencies and critical infrastructure vulnerabilities should not be understood as isolated policy issues, but as mutually reinforcing structural risks.** Climate change intensifies migration pressures, threatens public health and increases the exposure of essential infrastructure. Migration reflects broader geopolitical, environmental and socio-economic dynamics rather than constituting a discrete crisis. Health emergencies rapidly cross national borders and depend upon resilient infrastructure and effective governance. Disruptions to critical infrastructure can trigger widespread social, economic and political instability. Collectively, these interdependencies reveal the need for a more coherent European security framework.

Although the European Union has developed robust legal instruments in each of these policy areas, persistent disparities in implementation, institutional fragmentation, divergent national priorities and insufficient coordination continue to constrain its overall effectiveness. Addressing these problems requires more than the creation of additional policy instruments; **it demands a shift towards an integrated resilient model that places prevention, preparedness and systemic governance at the centre of European security.**

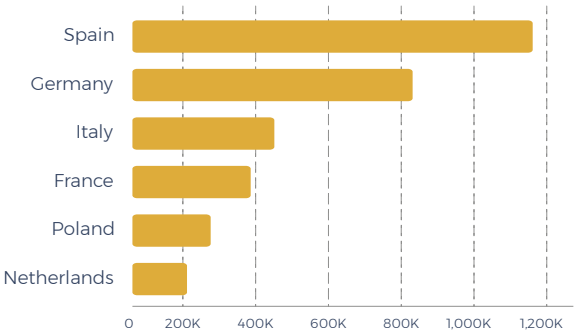
Strengthening coordination among Member States, harmonising implementation, enhancing common risk assessment and early-warning mechanisms, and embedding climate, migration, health and infrastructure resilience within a unified strategic framework will be essential to improve the EU's capacity to anticipate and manage future crises. In an era characterised by complex and interconnected risks, **Europe's security will ultimately depend not only on its ability to restrain conventional threats, but also on its capacity to govern with interdependence, strengthen resilience and develop coherent responses to the structural challenges that increasingly define today's security landscape.**

CLIMATE

The European Union currently addresses climate change through a solid legal and strategic framework, progressively built through the transition from soft law to hard law instruments.

- European Green Deal
- European Climate Law
- Emissions Trade System
- Regulation 2023/1115

INMIGRANTS



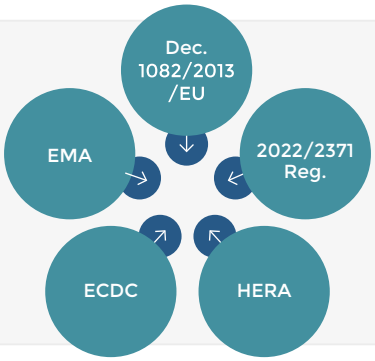
MIGRATION

Spain, Germany, Italy, France, Poland and Netherlands receive a significant overload of inflows compared to other Member States. Yet,

65% of refugees and asylum seekers remain in neighbouring countries to their home country

HEALTH

Health policy in the EU has rapidly consolidated, being COVID-19 a policy change driver these past years. A common framework was established under the European Health Union focused on improving cooperation among Member States, ensuring the availability of medical supplies, and enhancing preparedness and response capacities.



200M
FOR A COMMON PROJECT

- CER Directive
- NIS 2 Directive

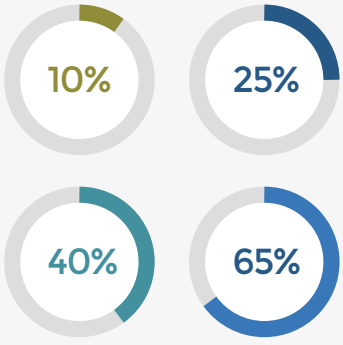
CRITICAL INFRASTRUCTURE PROTECTION

CIP remains one of the strongest cooperation challenges of the Union. Despite increasing threats, Member States continue posing difficulties towards uniform implementation.

Nonetheless, a common Critical Entities Resilience Group has been established together with a common regulatory framework that aims to harmonise Member States' preparedness towards imminent challenges.

SUPPLY CHAINS AND CIRCULAR ECONOMY

The European Union holds a strong dependence on external suppliers for critical raw materials aggravating the fragility of the supply chains that sustain its green and digital transitions. To address this, the EU adopted the Critical Raw Materials Act (CRMA) in 2024, setting targets for 2030: at least 10% of strategic raw material consumption extracted domestically, processed within the Union, 25% sourced from recycling, and no more than 65% of any single strategic material imported from one third country.



Glossary of abbreviations

AI	Artificial Intelligence
CER	Critical Entities Resilience
CERG	Critical Entities Resilience Group
CIP	Critical Infrastructure Protection
CRMA	Critical Raw Materials Act
CRM(s)	Critical Raw Material(s)
ECDC	European Centre for Disease Prevention and Control
ECtHR	European Court of Human Rights
EMA	European Medicines Agency
EU	European Union
EU-CIP	European Union Critical Infrastructure Protection
EU ETS	European Union Emissions Trading System
EUDR	European Union Deforestation Regulation
Eurodac	European Asylum Dactyloscopy Database
HERA	Health Emergency Preparedness and Response Authority
IPCC	Intergovernmental Panel on Climate Change
IOM	International Organization for Migration
NIS2	Network and Information Security Directive 2
TFEU	Treaty on the Functioning of the European Union
WEEE	Waste Electrical and Electronic Equipment



CONCLUSION *OF THE POLICY PROPOSALS DOCUMENT*

These Policy Briefs are the result of the work of more than 40 young writers who have spent months shaping what constitutes the academic foundation of the Forum and its very essence: giving voice to young people's proposals so that they reach decision-makers in Europe.

Although the seven Policy Briefs in this *V Edition of the Forum on the Future of the EU*, "European Security in a Changing World", address different areas, **they all reach a common conclusion:** the European Union no longer faces a world in which interdependence alone guarantees peace. The founding logic of the Schuman Declaration, which sought to make war "materially impossible", remains valid within the Union's borders; outside the Union, however, **that very interdependence has become a source of vulnerability when it is not accompanied by the Union's own capabilities.**

Russia's war of aggression against Ukraine, the rivalry between the United States and China, the crisis in the Strait of Hormuz and the dispute over Greenland have confirmed that **the European Union must learn to "speak the language of power"**, as Borrell put it, while taking care not to give up what defines it.

Yet the most frequently reiterated conclusion throughout this document is that Europe's main shortcoming lies not in its existing instruments, **but in how they are used. The EU has demonstrated a remarkable ability to design tools, but all analyses point to the same gap between ambition and implementation.** This pattern stems from the Union's tendency to build capabilities without first resolving the political decisions needed to use them. The result is **an architecture that is sound on paper but slow in practice**, oscillating between moments of cohesion driven by crisis and a return to the lowest common denominator once the urgency subsides.

In terms of **governance**, the analysis of the institutional architecture shows that the unanimity rule in the Common Foreign and Security Policy is not merely a procedural issue, but also shapes the substance of decisions. Between 2011 and 2025, there were 45 vetoes, a third of which occurred in the last year and a half, and 19 of which were cast by Hungary. **Beyond the formal veto, the mere threat of one influences negotiations before any vote takes place.**

As the Policy Briefs point out, **unanimity is not inherently slow**. In the days following the 2022 invasion, the EU froze approximately €210 billion in assets held by the Central Bank of Russia and excluded seven Russian banks from the SWIFT system in just one week. **The decisive factor is therefore the extent to which the threat is commonly perceived.** The main problem is that this perception is uneven, since the eastern flank sees Russia as an existential threat, whereas the southern flank is more concerned with instability across the Mediterranean, and this divergence makes a shared sense of urgency harder to sustain.

When it comes to **defence**, the Policy Briefs **point to a paradox**, as unprecedented financial mobilisation coexists with persistent structural fragmentation. This increases maintenance costs, hinders interoperability and prevents economies of scale. Furthermore, the Policy Briefs agree that **the relationship with NATO is (and should be) one of complementarity rather than competitio**n. They also agree that dependence on NATO currently defines the real limits of European strategic autonomy. The debate over a European army is, therefore, less useful than the fundamental question: **whether the EU can gradually transform scattered national efforts into a credible collective capability.**

Beyond defence, **economic security has become as important a dimension as the military one**. In mapping out asymmetric dependencies, the document identifies an underlying tension between the EU's role in setting the rules of the digital game and its lack of the technology with which it is played. Its normative power is a strategic asset, but regulating is not the same as producing. The analyses therefore reach the pragmatic conclusion that full sovereignty is neither realistic nor necessary. Instead, they call for a **selective approach** that reduces genuinely dangerous dependencies, diversifies rather than decouples, and preserves openness wherever it does not compromise the capacity to act.

Dependencies are not merely economic, and the Policy Briefs show that **threats are interlinked**. Climate change acts as a multiplier on migration, health and critical infrastructure, while dependence on critical raw materials cuts across all these areas. **Migration illustrates the need to refine our analysis:** the problem is not so much the volume as its unequal distribution and the administrative capacity of states. Externalising border control, for its part, creates a new dependency which third countries can use as a means of exerting pressure.

The analysis also warns that **the response to these threats may become part of the problem**. Hybrid threats exploit the openness of democratic societies, and **the temptation to respond with exceptional, opaque or disproportionate measures may normalise a form of "emergency governance" that undermines the rule of law**. Informal intelligence-sharing forums operate outside parliamentary oversight, the attribution of attacks once again requires unanimity, and democratic oversight has not kept pace with the new powers. Legitimacy thus emerges as the Union's strategic centre of gravity. With 51% of Europeans trusting the EU, the highest level since 2007, and the figure rising to 59% amongst young people, **Eurobarometer data provide a solid foundation on which to build.**

Beyond its borders, the Union is called to apply the same logic of diversification advocated in the economic sphere. The Policy Briefs present partnerships and enlargement as parts of the same strategy. **Africa** must move from being a recipient of aid to becoming a partner and co-author of a shared agenda. **Latin Americ**a, with the EU–Mercosur agreement provisionally in force since May 2026, is a natural ally for diversifying supplies. The **Indo-Pacific** is now a strategic necessity, and in the Arctic the window of opportunity to exert influence is closing. Enlargement, meanwhile, has ceased to be a technical process and has become a geopolitical issue. **The question is no longer just whether the candidate countries are ready for the Union, but whether the Union can afford to leave them out.**

Taken together, these elements paint a picture of a Union that possesses almost everything needed to be a credible security actor: a large single market, financial capacity, regulatory power, a solid industrial base, legal instruments and growing public support. **What remains is to turn these assets into effective capabilit**y. This requires coherence across policy areas that continue to operate in isolation, swift implementation, the political will to make use of existing resources, and a shared strategic vision amongst states with differing perceptions of the threat.

With consensus on the diagnosis, an unprecedented mobilisation of resources and renewed political momentum, **the current situation presents an opportunity**. Experience warns us, however, that **such windows close when the sense of urgency fades.** The pressing challenge is not so much to define what sort of actor Europe wishes to be as to demonstrate that it can act as such without renouncing the values that give meaning to the European project.

Young people are not merely recipients of this challenge but part of the answer: they trust the Union more than the average European does, and they will live with the consequences of the decisions taken today. These policy briefs show that they are willing and able to help shape them.

María Villaverde Temes

Policy Proposals Coordinator of the V Edition of Forum on the Future of the EU







This document was prepared by Equipo Europa partners and collaborating organizations. The copyright for this edition has been assigned to Equipo Europa. The content of this publication is the sole responsibility of its authors and does not necessarily reflect the views of Equipo Europa or its co-llaborating or funding organizations. The information contained in this document may be reproduced in whole or in part, provided that the source is cited.

Forum on the Future of the EU 2026, European Security in a Changing World, Equipo Europa.

© Equipo Europa, 2026



hablamos deeuropa

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN
SECRETARÍA DE ESTADO PARA LA UNIÓN EUROPEA

Co-funded by the European Union

ie UNIVERSITY
SCHOOL OF POLITICS, ECONOMICS & GLOBAL AFFAIRS

Iberdrola

BASF We create chemistry

KONRAD ADENAUER STIFTUNG

ERICSSON

Renault Group Fundación España

Friedrich Ebert Stiftung

ecoembes El poder de la colaboración

Deloitte.

Microsoft

S2GRUPO

INDRA GROUP