About the Article

How can the EU achieve strategic autonomy in defense amid technological disruption and geopolitical rivalry? Europe must adopt three interdependent policies: ethical governance for emerging technologies, industrial and supply chain resilience, and integrated cybersecurity to secure its defense ecosystem. By aligning these points through investment, collaboration, and unified standards, the EU can become a key player and increase its sovereignty.

About the Author

Alba Gremli is a dual citizen from Switzerland and Spain, and speaks 4 languages fluently. She has obtained a Bachelor's degree in Global Governance, Economics & Legal Order, with a focus on international security and politics. Alba is working as a Public Affairs Associate in Zurich, aiding the company in assessing global and national political impacts and managing the company's transition in changing global affairs.

1. Introduction

The twenty-first century has witnessed an unprecedented acceleration in technological innovation, fundamentally altering the nature of security, defence, and geopolitics. Across the European horizon, these changes reveal themselves through a stark reality: the existence of automated decision-making, the fragility of supply chains, the invisibility of cyber domains, and the geopolitical tensions emanating from distant theatres like Ukraine and the Indo-Pacific. Where once the conception of strategic autonomy settled for narrow definitions of military self-reliance, today the European Union and its member states are pressed to articulate a broader vision. This vision must no longer pivot solely around technology as an end in itself, nor around separate technologies like artificial intelligence, geotechnology, or cybersecurity. Instead, it must consolidate around concrete policy imperatives: how to govern innovation ethically, how to build resilient industrial foundations, how to integrate digital defence capabilities seamlessly, and how to cultivate a strategic culture that binds a diverse continent together. The narrative aims to shift debates away from a list of technologies and towards an articulation of clear policy recommendations. It begins by framing governance and ethics as the bedrock of a legitimate and credible strategy, then considers the resilience of the European industrial base, addresses the inseparability of cybersecurity from traditional defence, and finally highlights the necessity of forging a shared strategic imagination. In doing so, it embraces the complexity of the topic.

2. Governance and Ethical Frameworks

Governance and ethics must form the foundation of any strategy that seeks to harness emerging technologies for the purposes of defence and security while remaining true to the values for which Europe stands. The notion of strategic autonomy could become hollow if it were detached from ethical reflection; autonomy and power are meaningless if cast aside from democratic accountability, human rights and the rule of law. How do we ensure that decision-making processes respect human dignity and oversight? What institutional architecture is necessary to hold developers, procurers and military commanders to account when a semi-autonomous drone makes mistakes or lethal force is directed without human consent? These questions do not come with clear answers, but they are nonetheless asked and have to be answered. The European Union has confronted these questions through the codification of the AI Act and through the establishment of parliamentary committees dedicated to the subject of artificial intelligence in a digital age (European Parliament, 2022). By prioritising a human-centric, risk-based model, the EU sets itself apart from frameworks that valorise raw capability over respect for human rights. Yet the explicit exclusion of military applications from the AI Act exposes a vulnerability, placing strategic uses of algorithmic tools in a regulatory grey zone. The absence of rules for the battlefield allows for ambiguity to grow and ethical continuity to fracture. Accordingly, policymakers should extend the scope of regulation to address military contexts, devising standards for transparency and proportionality that apply irrespective of technology and landscape. Everyone from civil society activists to software engineers should sit at the table, their voices informing deliberative processes that yield binding codes of conduct. Europe could stand up an independent observatory monitoring the deployment of automated systems within the defence policy. Such a body might audit algorithms, review procurement choices, rule on objections, and publish sanitised reports summarising its activity. By doing so, it could balance the necessities of secrecy with the imperatives of accountability. Independent ethical advisory boards, commissioned by the Council, the European Parliament or even NATO, can review classified programs and publish the essential lessons to the public that are hesitant to accept anything less than openness. Within these frameworks, normative innovation can expand. Experience with the General Data Protection Regulation suggests that value-laden law can originate from a broad consensus

about human dignity and privacy (gdpr.eu, n.d.). The same consensus must extend to security: fairness, explicability, and contestability belong in the framework of defence as much as they do in the area of business. Algorithms reflect their creators, and they mirror unconscious biases rooted in gender, ethnicity and class. When translated into lethal or coercive contexts, those biases risk perpetuating injustice and worsening the universal quality of the underlying mission. Thus, policies requiring diverse design teams, mandating bias audits, and implementing corrective measures are not optional niceties; they are essential components of a moral and ethical regime. The EU could legislatively mandate that all advanced defence prototypes undergo independent bias testing prior to acquisition. Simultaneously, the practice of deliberative democracy should be extended into the security sphere. In a democratic landscape, citizen assemblies might be convened to weigh in on the use of autonomous weapons, framing the underlying debate as one about the kinds of societies we choose to build. Repeated review cycles would insulate policy from obsolescence, reflecting the accelerating pace of technological change and the emergence of unanticipated consequences. Revisitations would allow for frameworks and policies to be reviewed consistently, rather than once a crisis hits. Ethical reflection must remain supple enough to shape innovation rather than trailing behind it. Interrogating the relationship between emerging technologies and international humanitarian law is indispensable (Short, 2025). Do long-standing principles of distinction, proportionality and necessity retain their force when executors are algorithms or when attacks emanate from non-state actors that reject international conventions? The European approach should be anchored in the strongest possible commitment to human rights and to humanitarian ideals, integrating these norms into every stage of research, development, testing and deployment. Member states should embed obligations into their procurement contracts requiring respect for humanitarian law. Independent compliance officers could report directly to the European Court of Human Rights. Victims of algorithmic error must receive access to justice, redress and rehabilitation, channelled through impartial tribunals that command trust across cultural and national boundaries. The friction between secrecy and democratic legitimacy demands institutional innovation: parliamentary committees with high-level clearances can bridge the gap between elected representatives and technical experts. Transparency reports, released periodically with necessary redactions, can expose aggregate statistics about errors and anomalies, highlighting the flaws that lurk beyond public view (Short, 2025). Such openness empowers citizens to hold governments responsible without undermining operational security. Europe's normative power can be amplified through coalitions: coordinated dialogues with transatlantic partners, negotiations at the United Nations to enshrine norms against indiscriminate autonomous weapons, and coalitions of like-minded states can press adversaries to accept minimum standards (Sylvia, 2025 March). These are not idealistic fantasies but practical acts of leadership; the EU's influence on data protection law and climate regulation demonstrates that normative leadership can shape the entire landscape beyond its borders. Finally, institutional architectures must be redesigned to promote flexibility and responsiveness in the face of uncertainty: agile decision-making, networks of regulators and academics, and protocols that reflect public health emergency mechanisms could underpin an ethical regime capable of weathering storms. Sharing best practices through a European ethics repository lowers the cost of learning from mistakes and propagates high standards across the continent, something the EU has strived to do in other fields (European Parliament, 2022). Yet even in these laudable efforts, nuance is necessary. Ethics cannot be enforced like rules, as they change with time and place (Short, 2025). In practice, when

Dual-use innovation:
Technologies developed for civilian purposes that can also be applied in military or defense contexts. It bridges commercial and defense sectors (e.g., chips, batteries).

European states negotiate with allies whose own ethical compass differs from Europe's, reconciling differences becomes crucial. Dialogue with partners beyond the Union must be predicated on respect, as ethical partnerships should be born out of mutual self-understanding beyond formal treaties. Scholars and regulators from different parts of the world should work together to probe the underside of innovation: cross-disciplinary research could explore not only the promise of technologies but their hidden toll on social cohesion, privacy and political legitimacy. Continuous training for judges, lawyers and soldiers about the philosophical underpinnings of autonomy and dignity can prevent situations where those tasked with combat remain ignorant of the ethical standards they are obliged to uphold. This would strengthen the international rule of thumb and build a more cohesive policy landscape on the ethical use of technology. The answers to the previously asked questions cannot be rhetorical. In the end, ethical governance is crucial to hold European and international autonomy together, and without it, any growth built on technology alone collapses into fragmentation and unethical competition.

> **"Building the European Defense Technological and Industrial Base, investing in dual-use innovation, and diversifying supply chains will secure Europe's technological sovereignty and economic strength."**

3. Industrial and Supply Chain Resilience

Resilience at an industrial level stands as the second pillar in the project of European strategic autonomy. The vulnerabilities exposed by the Covid-19 pandemic, by supply-chain disruptions coming from tensions with China and by the attack of Ukraine demonstrate that Europe's dependence on foreign sources for critical inputs leaves its sovereignty fragile (Sylvia, 2025). The chips that sustain our communication networks, the batteries that mobilise vehicles, the specialised rare earth minerals that constitute sensors, and the processors that enable complex analytical tasks are barely manufactured within the borders of Europe (Israel, 2025).

The framework of resilience requires an economic policy that pivots towards both sufficiency and innovation, rejecting monopolies but recognising that diversification, stockpiling, reshoring, and the creation of strategic industrial clusters are pragmatic hedges against coercion. A strategy of industrial resilience starts by mapping dependencies, pursuing transparency along the value chains and quantifying risks rather than pretending that market forces alone will provide for European security. The European Chips Act (European Commission, 2022) and the Critical Raw Materials Act (European Commission, 2023) mark important first steps, signalling the world's will to invest in domestic production and to develop capacities across the upstream segments of critical industries. But such initiatives demand long-term commitment beyond reactive announcements. The European Defence Fund's budgetary envelope for 2021–2027 represents one of the few institutional vehicles for joint investment in borderline technologies, but it must be scaled upward and complemented by incentives that encourage private capital to grow into defence-relevant R&D. Moreover, public-private partnerships (PPPs) must be encouraged to accelerate innovation. A cohesion among government, business, and research units should be institutionalised and entrusted with concrete goals like inventing, manufacturing, and ultimately distributing into the markets. The dual-use nature of many strategic goods offers opportunities for economies of scale, but only if the partnership between civilian and military sectors is unified. Additionally, procurement policies should highlight modular architectures that can be adapted for civilian markets and vice versa. The European Defence Technological and Industrial Base can flourish only if it is in partnership with commercial ambitions and strategic long-term goals (European External Action Service, 2022). Lastly, a coherent industrial strategy should also address sustainability and climate interdependencies, understanding that future steel manufacturers, chip plants, and AI data centres will be both harmful to the environment and can also be sources of

resilience and key components in a sustainable economy. For industrial resilience, the areas of technological leadership, diversification, and environmental stewardship should come together to build a strong industrial policy that brings together these areas in a way that its resilience lies not in single industries but in the whole network. This could also come with the downside of the industries being overly dependent; however, with the right policy framework, this can be mitigated. Resilience is embedded in understanding risk to mitigate and assess future risks. Thus, it is important to be risk-averse and watch out for bureaucratic obstacles and one-sided interests that can hinder innovation and leave the continent to be a follower rather than a leader. To hinder this, concrete roadmaps with monthly or yearly goals and agreed budgets must be set in place. Geopolitically, Europe must navigate between superpowers, like the U.S. and China, through reciprocal partnerships that let capital and technology flow into the continent (Parisini, 2025). Trade agreements and investment screening can help steer Europe in the right direction. To embed a unified plan, a concrete framework of specialisation should be prioritised. Member states should focus on their capabilities, whether that's quantum photonics or green munition technologies (Csernatoni, 2024). By focusing on each nation's strength, Europe can increase its resilience together through collaboration rather than individual strategies. Institutions such as the European Investment Bank and national development agencies should prioritise projects that connect this plan into cohesive networks underwritten by a shared vision of the common good and goal.

Figure 1: Relationship of the EU regarding rare earths and raw Materials

Complementary to ethics, economic resilience compels us to question the architecture of supply networks. For example, the extraction of rare earth metals often occurs in nations with lax environmental standards. Europe cannot achieve resilience at the expense of human rights or sustainable goals that aren't present in other continents. Therefore, policy must bind ethics and sustainability into resilience strategies. This could take the form of binding due diligence laws that require companies to report on every upstream tier of their supply chains. Moreover, financing instruments like green bonds can be tied to defence projects on the condition that the entire supply chain complies with environmental and labour norms. At the same time, small and medium enterprises (SMEs) should be woven into the industrial policy. On that note, regional incubators, matched funding schemes, and capacity-building programmes enable SMEs to contribute meaningfully to national security, embedding resilience within communities across Europe (European Commission, 2025). This also highlights infrastructure rebuilding, which offers another canvas for resilience. Rather than merely rebuilding war-torn infrastructure like bridges or tunnels, with the right policies, they can be transformed into sensors and actuators within a smart defence grid that monitors the flow of goods, anticipates disruptions, and dynamically reroutes shipments. Building resilience from the start ultimately diminishes cost and effort at the end.

4. Integrated Cyber and Digital Defence

Cybersecurity integration comprises the third policy imperative, recognising that the digital environment is one

of the principal domains of twenty-first-century coercion and confrontation. Cyberspace has evolved into a fifth domain alongside land, sea, air, and space. The fragmentation of national cyber policies across Europe, the uneven distribution of capabilities, and the absence of a common threat picture translate into windows of opportunity for those who would inflict harm and put the continent at a disadvantage. A unified European cybersecurity posture must be more than an alignment of technical standards; rather, it must embody a cultural reorientation that appreciates the interdependence of all critical functions that European countries have to offer (Csernatoni, 2025 May). Cybersecurity cannot be delegated to a handful of specialists but should rather be highlighted centrally in all decision-making, procurement, training and operations. The NIS2 Directive and the Cybersecurity Strategy chart legal contours for Europe's digital defence, but implementation cannot be enacted without unified political will (European Parliament, & Council of the European Union, 2022). The military sphere is frequently overlooked despite being especially exposed. Integrated command and control systems, battlefield sensors, and even basic logistics rely upon networks that are targets for disruptions. Thus, Europe must invest in the human capital necessary to detect, prevent, and respond to cyber threats. Moreover, the cultivation of a skilled cyber workforce demands early education and lifelong training. For that, cyber ranges, simulation centres, and updated education systems should be expanded across the continent and should be complemented by credentials recognised by all countries and tied to career progression in national militaries and civilian administrations. Additionally, information sharing should expand beyond rhetorical commitments. Interoperable platforms and the development of trust allow countries to work together and build a unified European system. Establishing common incident response protocols, joint exercises, and rapid-reaction cyber units contributes to an emergent collective European cyber identity (European External Action Service, 2022). This also includes data protection, which overlaps with cybersecurity. The GDPR, when suitably interpreted, can guide the ethical collection of threat intelligence and secure the depot that underpins analytical campaigns. Additionally, a shared vocabulary of cyber concepts could be created and constantly updated to reflect the pace of innovation. Moreover, a common certification scheme for components, software and services would raise the baseline of resilience and create a market premium for security-by-design. Interconnection in cyberspace remains notoriously difficult, as devising mechanisms to gather credible evidence for state-sponsored attacks without compromising civil liberties becomes, in many ways, a national matter.

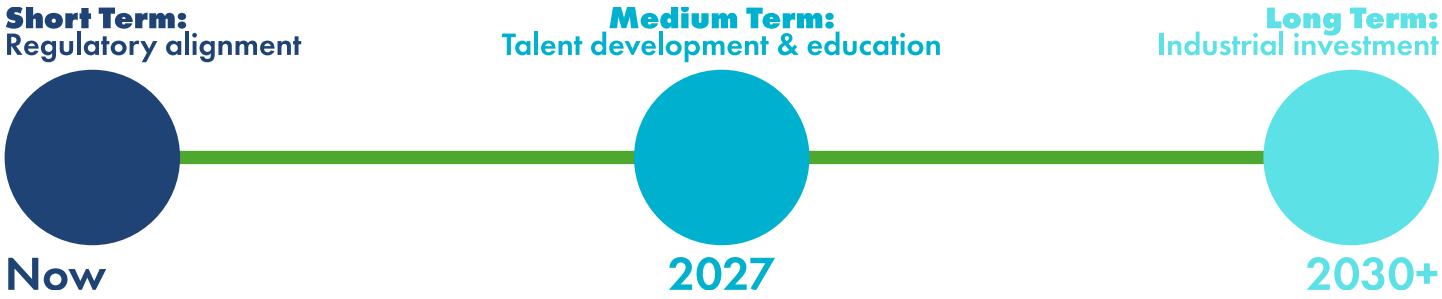

Figure 2: European Strategic Autonomy – Key Steps

5. Conclusions

Europe's pursuit of strategic autonomy in defence is no longer aspirational; it is an urgent necessity shaped by technological disruption, geopolitical rivalry, and hybrid threats. Three policy imperatives stand out as decisive for the future. First, ethical governance and oversight must anchor innovation, ensuring that artificial intelligence and emerging technologies align with democratic values and international law. Without robust standards and accountability, autonomy risks becoming hollow power. Second, industrial and supply chain resilience is critical to reduce dependency on external actors. Building the European Defence Technological and Industrial Base, investing in

dual-use innovation, and diversifying supply chains will secure Europe's technological sovereignty and economic strength. Third, integrated cybersecurity must become a core defence pillar, with harmonised standards, skilled workforce development, and rapid-response capabilities to counter escalating digital threats. These priorities are interdependent: governance shapes trust, resilience underpins capability, and cybersecurity ensures continuity. By committing to these policies with sustained investment and coordination, the EU can transform fragmentation into unity and vulnerability into strength. Strategic autonomy is not a static goal but a dynamic process—one that demands vision, collaboration, and unwavering resolve to safeguard Europe's security and values in an increasingly contested world.

References

Csernatoni, R. (2024, March 6). Charting the geopolitics and European governance of artificial intelligence. Carnegie Endowment for International Peace.
https://carnegieendowment.org/research/2024/03/charting-the-geopolitics-and-european-governance-of-artificial-intelligence

Csernatoni, R. (2025, May 20). The EU's AI power play: Between deregulation and innovation. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation

European Commission. (2022). Proposal for a regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (European Chips Act) (COM/2022/46 final). https://eur-lex.europa.eu

European Commission. (2023). Proposal for a regulation of the European Parliament and of the Council establishing a framework for ensuring the supply of critical raw materials (COM/2023/160 final). https://eur-lex.europa.eu

European Commission. (2025, March 19). European Defence: Readiness 2030. https://defence-industry-space.ec.europa.eu

European External Action Service. (2022). A strategic compass for security and defence. https://www.eeas.europa.eu

European Parliament. (2022, March). Post-European Council briefing. https://www.europarl.europa.eu

European Parliament, & Council of the European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu

GDPR.eu. (n.d.). What is GDPR, the EU's new data protection law? GDPR.eu. https://gdpr.eu/what-is-gdpr/

Israel, K.-F. (2025, December 10). Europe's strategic dependence on China. GIS Reports.
https://www.gisreportsonline.com/r/europe-dependence-on-china/

Parisini, E. (2025). Governing artificial intelligence in the defence sector: A comparative analysis of EU and US institutions. Global Public Policy and Governance, 5. https://doi.org/10.1007/s43508-025-00115-x

Short, L. (2025, July 11). Ethics in AI: Why it matters. Harvard Division of Continuing Education, Professional & Executive Development. https://professional.dce.harvard.edu/blog/ethics-in-ai-why-it-matters/

Sylvia, N. (2025). Emerging insights: European digital defence priorities in an uncertain world. Royal United Services Institute.

Sylvia, N. (2025, March 25). European digital defence priorities in an uncertain world. Royal United Services Institute.
https://www.rusi.org/explore-our-research/publications/emerging-insights/european-digital-defence-priorities-uncertain-world

EUROPEUM

INSTITUT PRO EVROPSKOU POLITIKU
INSTITUTE FOR EUROPEAN POLICY

WHO ARE WE?

EUROPEUM is a Prague and Brussels-based think-tank dedicated to **advancing European integration** and shaping Czech and EU policymaking.

OUR PROGRAMMES

- **Just Europe** *"Integration must be socially just and lead to the convergence of living standards"*
- **Green Europe** *"Our goal is an ambitious climate policy that considers both the planet and its citizens"*
- **Global Europe** *"EU's strong position*
- *in its neighborhoods and partnerships with global actors are key to maintaining position in a changing world"*

WHAT DO WE DO?

Research
Our research and outputs include over **100** policy papers, analyses, reports and other publications yearly

Projects
We partake in projects focused on topics ranging from green and just transformation, digitalisation, migration or EU enlargement up to security or media freedom

Café Evropa

JUSTGREEN

Events and education
We yearly bring important topics into over **80** public debates, workshops, routables and international conferences.

Think Visegrad
Representing Think Visegrad Platform in Brussels

Establishing **network** of partners to maximize the influence of independent research based advocacy

EUROPEUM Brussels Office

EUROPEUM was the first think tank from Central Europe to expand into the heart of the European Union. Our motivation was to follow the debates on the EU agenda closely and to contribute to strengthening the voice of the Czech Republic and other Central and Eastern European countries.

Scan the QR code for more info!