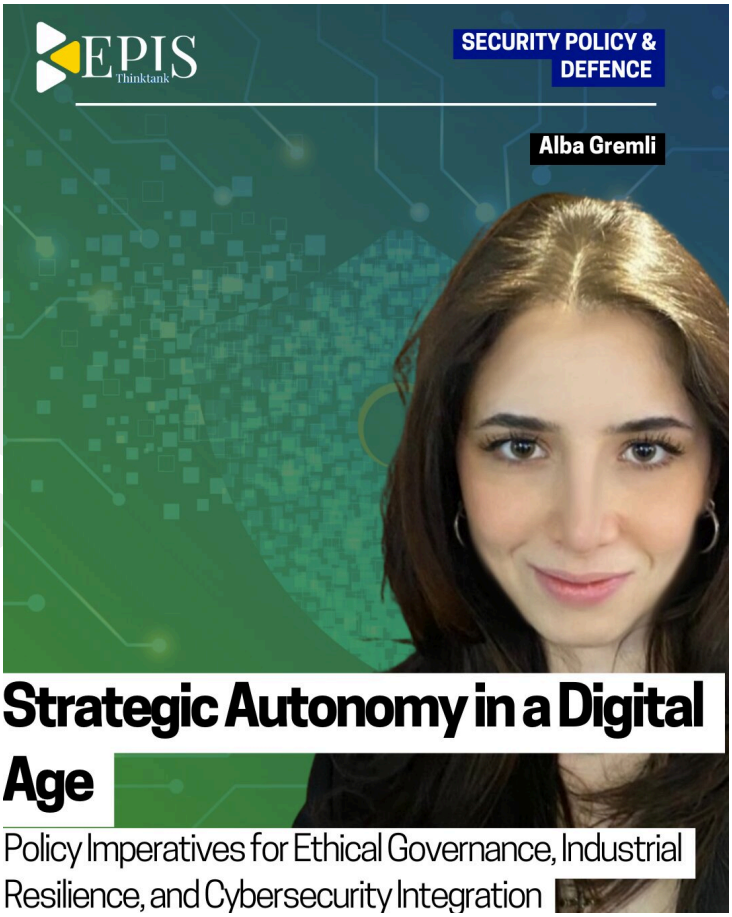
Strategic Autonomy in a Digital Age

27 DECEMBER 2025

Alba Gremli



EPIS Think Tank
Alba Gremli Torres

The twenty-first century has witnessed an unprecedented acceleration in technological innovation, fundamentally altering the nature of security, defense, and geopolitics. Across the European horizon, these changes reveal themselves through a stark reality: the existance 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 defense 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 European industrial base, addresses the inseparability of cybersecurity from traditional defense, and finally highlights the necessity of forging a shared strategic imagination. In doing so, it embraces the complexity of the topic.

Governance and ethics must form the foundation of any strategy that seeks to harness emerging technologies for the purposes of defense 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 respects human dignity and oversight? What institutional architecture is necessary to hold developers, procurers and military commanders to account when a semi-autonomous drone make mistaakes or lethal force is directed without human consent? These questions do not come with the 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. By prioritizing a human-centric, risk-based model, the EU sets itself apart from frameworks that valorize 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. Absent rules for the battlefield, allows for ambiguity to grow and ethical continuity to fracture. Accordingly, policy makers 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 defense policy. Such a body might audit algorithms, review procurement choices, rule on objections, and publish sanitized reports summarizing 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 publics that are hesitan 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. The same consensus must extend to security: fairness, explicability, and contestability belong in the framework of defense as much as they do in the are 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 defense 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.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, channeled 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. Such openness empowers citizens to hold governments responsible without undermining operational security. Europes 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. These are not idealistic fantasies but practical acts of leadership; the EUs 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, 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. Yet even in these laudable efforts, nuance is necessary. Ethics cannot be enforced like rules, as they change with time and place. In practice, when 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 rhetoric.

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.

Resilience at an industrial level stand 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 Europes dependence on foreign sources for critical inputs leaves its sovereignty fragile. The chips that sustain our communication networks, the batteries that mobilize vehicles, the specialized rare earth minerals that constitute sensors, and the

processors that enable complex analytical tasks are barely manufactured within the borders of Europe.

The framework of resilience requires an economic policy that pivots towards both sufficiency and innovation, rejecting monopolies but recognize that diversification, stockpiling, reshoring and the creation of strategic industrial clusters are pragmatic hinders 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 and the Critical Raw Materials Act mark important first steps, signaling the world the 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 Funds 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 defense-relevant R&D. Moreover, public-private partnerships (PPPs) must be encouraged to accelerate innovation. A cohesion among government, business, and research units should be institutionalized and entrusted with concrete goals like to invent, manufacture and ultimately distribute 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 are 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 with strategic long-term goals.

Lastly, a coherent industrial strategy should also address sustainability and climate interdependencies, understanding that future steel manufacturers, chip plants, and AI data centers will be both harmful to the environment but can alslo 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 obstables 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 monrhtly 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 in into the continent. Trade agreements and investment screening can help further Europe into the right direction. To embed a unified plan, a concrete framework of specialization should be prioritized. Member states should focus on their capabilities, whether that's quantum photonics or green munition technologies. 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 prioritize projects that connect this plan into cohesive networks underwritten by a shared vision of the common good and goal.

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 by 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 requiring companies to report every upstream tier of their supply chains. Moreover, financing instruments like green bonds can be tied to defense projects on the condition that the entire supply chain complies with environmental and labor 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. 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 defense grid that monitors the flow of goods, anticipates disruptions, and dynamically reroutes shipments. Building resilience in from the start ultimately diminishes cost and effort at the end.

Cybersecurity integration comprises the third policy imperative, recognizing 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 to 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 translates into windows of opportunity for those who would inflict harm and puts the continent at a disadvantage. A unified European cybersecurity posture must be more than an alignment of technical standards, but rather it must embody a cultural reorientation that appreciates the interdependence of all critical functions that European countries have to offer. 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 defense, but implementation cannot be enacted without unified political will. 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. 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 schemes 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.

References

AI Act (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. European Commission.European Defence Fund (2020). Establishing the European Defence Fund: Regulation (EU) 2021/697 of the European Parliament and of the Council on the European Defence Fund. Official Journal of the European Union.European Chips Act (2022). Proposal for a Regulation of the European Parliament and of the Council: A European Chips Act: Chips for Europe Initiative. European Commission.Critical Raw Materials Act (2023). Proposal for a Regulation by the European Parliament and of the Council on Establishing a Framework for Ensuring the Supply of Critical Raw Materials. European Commission.NIS2 Directive (2022). Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS2). European Parliament and Council.Parisini, E. (2023). Patterns of European Defence Digitalization: Institutional Absorption and Fragmentation. Journal of European Integration Studies, 42(1), 67-88.Csernatoni, R. (2022). Technological Sovereignty: Europe's Endeavour in Defence and Security. Carnegie Eu-

rope Working Paper.DIGITALEUROPE (2022). Europe's Defense Future Depends on Digitalization. Policy Paper.Versailles Declaration (2022). A Joint Commitment to Strengthen European Defence. European Council.Strategic Compass (2022). For Security and Defence – For a Europe that protects. Council of the European Union.Bosticco, Riccardo, et al. "Critical Raw Materials and EU's Open Strategic Autonomy – ITSS Verona." ITSS Verona, 7 Nov. 2022, www.itssverona.it/critical-raw-materials-and-eus-open-strategic-autonomy. Accessed 17 Nov. 2025.Csernatoni, Raluca. "Charting the Geopolitics and European Governance of Artificial Intelligence." Carnegieendowment.org, 6 Mar. 2024, carnegieendowment.org/research/2024/03/charting-the-geopolitics-and-european-governance-of-artificial-intelligence?lang=en.—. "Myth, Power, and Agency: Rethinking Artificial Intelligence, Geopolitics and War." Minds and Machines, vol. 35, no. 3, 11 Aug. 2025, https://doi.org/10.1007/s11023-025-09741-0.—. "The EU's AI Power Play: Between Deregulation and Innovation." Carnegie Endowment for International Peace, 20 May 2025, carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en.Digital Europe. THE EXECUTIVE BRIEF: BOOSTING EUROPEAN DIGITAL DEFENCE INNOVATION. Feb. 2025.Emanuele Parisini. "Governing Artificial Intelligence in the Defence Sector: A Comparative Analysis of EU and US Institutions." Global Public Policy and Governance, vol. 5, 6 June 2025, https://doi.org/10.1007/s43508-025-00115-x.

EU Commission. European Defence – Readiness 2030. 19 Mar. 2025.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, 14 Sept. 2023, digital-strategy.ec.europa.eu/en/policies/nis2-directive. European Council. "Cyber Defence." Consilium, Mar. 2025, www.consilium.europa.eu/en/policies/cyber-defence/.

European External Action Service. "A Strategic Compass for Security and Defence | EEAS Website." Www.eeas.europa.eu, 2022, www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.

European Parliament. BRIEFING Post-European Council Briefing. Mar. 2022.

Israel, Karl-Friedrich. "Europe's Strategic Dependence on China – GIS Reports." GIS Reports, 10 Dec. 2025, www.gisreportsonline.com/r/europe-dependence-on-china/.

Sylvia, Noah. Emerging Insights European Digital Defence Priorities in an Uncertain World. 2025.

—. "European Digital Defence Priorities in an Uncertain World." Rusi.org, 25 Mar. 2025, www.rusi.org/explore-our-research/publications/emerging-insights/european-digital-defence-priorities-uncertain-world.