



**Università
di Genova**

**DIPARTIMENTO DI SCIENZE POLITICHE
E INTERNAZIONALI**

**Corso di Laurea Magistrale in:
Security and International Relations**

**AI as an Instrument of Geopolitical Power: the Role of the European Union between
Regulation and Strategic Competition**

The Political System of the European Union. Foreign and Defense Policy in Europe

Relatore

Chiar.mo Prof. Fabrizio Coticchia

Candidata

Erika Franci

**ANNO ACCADEMICO
2025/2026**

Index

Introduction.....	3
Chapter I - Artificial Intelligence as a New Dimension of International Power	5
1.1 Technology and Power in International Relations.....	6
Technology through Realism	6
Technology as Material Capability	8
Artificial Intelligence as a Material Capability	10
Technology through Liberalism	13
Technology through Constructivism.....	16
Technological Security Dilemma.....	17
Technology as a Structural Factor in the Redistribution of Power	19
1.2 AI and the Transformation of Security.....	21
Cybersecurity and Automated Intelligence	22
Autonomous Weapon Systems.....	24
AI and Intelligence	26
1.3 The Global AI Competition: The United States and China	27
The United States: Innovation and Technological Leadership.....	28
China: State-led Development and Technological Sovereignty.....	31
The Militarization of Artificial Intelligence and the Global Semiconductor Race	32
Chapter II - The European Union's AI Strategy: From Regulation to Geopolitical Influence.....	36
2.1- The Evolution of the European Union as a Regulatory Power.....	37
The Brussels Effect: From Market Power to Global Standards	40
Digital Sovereignty and Strategic Autonomy.....	41
2.2 The AI Act: Structure and Political Logic	45
General-Purpose AI: A Late but Decisive Addition.....	54
Governance: Ambition Meets Administrative Capacity	56
Implementation Timeline: A Staggered and Politically Contested Calendar.....	59
2.3 Fields in Which the EU Uses AI as a Political Asset	63
Industrial Policy.....	64
Cybersecurity.....	64
Defence, Within the Limits of EU Competence.....	66
Protection of Fundamental Rights	68
External Action and Global Standard-Setting	69

<i>Chapter III - Regulation as an Instrument of Geopolitical Power: Limits and Potential of the EU</i>	71
3.1 The Brussels Effect in the Technological Domain	71
Critical Counter-Arguments: Why AI May Not Replicate the GDPR Precedent	73
Concrete Evidence of Emulation: A Mixed and Partial Picture	76
3.2 The EU as a Geopolitical Technology Actor	79
Defence Fragmentation	79
The Absence of an EU 'Big Tech' and the Compute-and-Cloud Dependency	80
Analysis: The Normative Model's Advantages, Structural Limits, and the Rights-Security Tension	83
3.3 Future Scenarios	84
Scenario (a): EU as Global Regulatory Leader	85
Scenario (b): EU Marginalised Between the United States and China	86
Scenario (c): EU as 'Normative Balancer'	87
Conclusion	90

Introduction

Artificial Intelligence has moved, within the space of a few years, from a subject of technical and ethical debate to a central variable in the distribution of power among states. The United States and China compete openly for leadership in frontier development, semiconductors and military applications, while the European Union, lacking comparable industrial champions, has staked its claim to relevance on a different instrument: regulation. The European Union has produced the world's first comprehensive legal framework for AI, the AI Act, and has repeatedly framed that framework not merely as consumer protection but as a geopolitical project, one intended to export European standards the way the GDPR is credited with having done for data protection. This thesis asks whether that project can succeed: is the governance of artificial intelligence sufficient to make the European Union a relevant geopolitical actor in the technological domain, or does regulatory power without a matching industrial and military base amount to influence on paper only?

Answering this question requires treating AI simultaneously as a technology and as an object of international relations theory, and the thesis is organised accordingly. Chapter I situates artificial intelligence within the main theoretical traditions of International Relations Realism, liberalism and constructivism and argues that AI is best understood as a material capability in the classical sense, one that is already redistributing power between the United States, China and other actors; this chapter also examines AI's transformation of security, from cyber operations to autonomous weapons, and surveys the current state of US-China technological competition. Chapter II turns to the European Union specifically, tracing its evolution as a regulatory power and the logic of the Brussels Effect, before analysing the structure and political compromises built into the AI Act and the fields; industrial policy, cybersecurity, defence, fundamental rights, external action in which the Union tries to use AI governance as a political asset. Chapter III is where the argument is tested against the evidence: it assesses how far the Brussels Effect travels in the AI domain, measures the EU's underlying capability base in defence, compute and cloud infrastructure, and sets out three scenarios for the Union's future trajectory before answering the thesis's central question directly.

Methodologically, the thesis combines a theoretical framework drawn from International Relations with a qualitative analysis of primary sources EU legislation, official communications and strategic documents and secondary literature from international relations,

EU studies and security studies, updated where possible with data and developments through 2026.

The argument defended across the three chapters is not that European regulatory power is irrelevant, nor that it is sufficient on its own, but that its geopolitical weight is conditional: real, but bounded by the capability gap the thesis documents, and dependent on a link between regulatory credibility and enforcement capacity that later chapters make explicit.

Chapter I - Artificial Intelligence as a New Dimension of International Power

The interaction of power and technology has always been of primary importance in International Relations. While classical theories emphasize material power - be it military, economic, or territorial - technology impacts the offense and defence of various strategies, security dilemmas, and control over international order (Waltz, 1979)¹. From the Industrial Revolution to the development of nuclear technology, history has shown how major technologies have shifted power: industrial capacity redrew the hierarchy of the great powers in the nineteenth century, and nuclear weapons redefined deterrence and status after 1945 (Gilpin, 1981). Artificial Intelligence (AI) is the most recent of such technologies, and it will alter the nature of military and economic power, control, and persuasion. We will first locate AI in the most important IR theories to appreciate its impact.

The argument of this chapter is that AI should be read primarily as a material capability in the classical sense, one that is redistributing the balance of power between the United States, China, and other actors, rather than as a purely technical or purely normative phenomenon; this is essentially the view already put forward by Gilpin (1981) for technology in general and by Horowitz (2018) for AI specifically, and the rest of the chapter builds on their work. This premise is what sets up the rest of the thesis: if AI really does function as a capability that reshapes power in this way, then the European Union's regulatory choices, discussed in Chapters II and III, can be read as a strategic response to a material transformation, and not only as an ethical or bureaucratic exercise. The rest of this chapter builds this argument through realism, liberalism and constructivism, before turning to security and to the US-China competition.

The theories of international relations are placed within a dynamic international context that therefore intersects with changes, highlighting how technology is infiltrating the power dynamics between states, in an era marked by technological change and transformation. Classical theories give us the basis for understanding power, but they do not yet have a defined framework with respect to technology, for this reason it is perceived as a limitation towards the

¹ Morgenthau, H.J. (1948). *Politics Among Nations: The Struggle for Power and Peace*. New York: Knopf.

development of a greater knowledge of the relationships between power, theories, and technology.

1.1 Technology and Power in International Relations

International relations and the state's power are analysed and divided into various categories and schools, where classical theories are the main pillar for the understanding the international system, how it works and how power and sovereignty is shared through states and institutions.

These theories are used by scholars, experts and diplomats, to addressing policies and cooperation between different orders.

Historically, the intersection of technology and power has been significant in the study of International Relations. Major technological innovations have historically shifted the distribution of capabilities among states and have altered military, economic, and political power. To understand the impacts of contemporary technologies, such as artificial intelligence, on modern international politics, one must analyse the main theories of power. Theories of International Relations provide different frameworks for understanding the role technology has on state behaviour, and patterns of international politics of both strategic cooperation and competition. Consequently, the theories of realism, liberalism, and constructivism provide complementary views for understanding the role of changing technology on the power structures of international politics.

Technology through Realism

According to the theory of realism, first developed by Hans Morgenthau (1948) and later reformulated in structural terms by Kenneth Waltz (1979), states are in a position where the main aim is to acquire and increase as much power as possible, since well-being resides in it, and the greater the power acquired, the easier it is to obscure the action of countries without or having less power in the international system; This theory is also based on competition within the international context strongly marked by power and influence.

There are therefore different pillars for which realist theory is based, one of them is undoubtedly self-preservation, a value in which a state should focus more, since gaining power is perceived as a social, economic, and political imperative.

Furthermore, the realist nature, contrary to the idealist one, highlights how states cannot always reach moral ground, but that on the contrary, a more concrete approach can reside more in deception and violence, somehow legitimized by promoting national interests, focusing primarily on defence and leaving in the background the morality perceived by international relations.²

Before turning to Mearsheimer, it is worth locating him within the broader realist family. Morgenthau's classical realism grounds the competitive drive for power described above in human nature itself. Neoclassical realism, most clearly formulated by Gideon Rose³ (1998), agrees that states seek power but adds that domestic-level factors, such as leaders' perceptions, state institutions and society, filter how that material power is actually converted into foreign policy; this matters for AI because it suggests that a state's ability to turn AI capability into geopolitical power also depends on internal choices, not on the technology alone. Kenneth Waltz then moved the realist paradigm onto more purely structural ground. In *Man, the State, and War*, Waltz⁴ (1959) organizes explanations of conflict and state behaviour into three "images", the individual, the state, and the international system, and argues that the third image, the anarchic structure of the international system itself, is what ultimately conditions state behaviour; this structural move is what gives rise to neorealism. Mearsheimer builds directly on this structural starting point, but pushes it towards a more pessimistic, power-maximizing conclusion.

Mearsheimer's theory of realism emphasizes how international relations are actually placed in a quasi-anarchic system, in which military and offensive resources are essential, since there is never certainty that states can actually refrain from using them, for this reason integrity and defence are subordinated to possession and the use of defensive deterrent.

Mearsheimer is a great supporter of hegemony supported by maximizing power, favouring security through the potential for war, according to the theory of the "Tragedy of the Great Power Politics", in which states are incessantly engaged in conflicts to ensure security.⁵

Mearsheimer is a realist, more precisely a proponent of the offensive realist theory, which takes its cue from the defensive realist theory of Kenneth Waltz. Offensive realism holds that,

² Waltz, K.N. (1979). *Theory of International Politics*. Reading, MA: Addison-Wesley Publishing Company.

³ Rose, G. (1998). Neoclassical Realism and Theories of Foreign Policy. *World Politics*, 51(1), pp.144–172. doi:10.1017/S0043887100007814.

⁴ Waltz, K.N. (1959). *Man, the State, and War: A Theoretical Analysis*. New York: Columbia University Press.

⁵ Mearsheimer, J.J. (2001). *The Tragedy of Great Power Politics*. New York: W.W. Norton & Company.

because no state can ever be fully certain of the intentions of others, the safest strategy is to maximize relative power and pursue hegemony whenever the opportunity arises; this is what separates Mearsheimer from Waltz, who instead argues that states should seek only an appropriate amount of power (a balance), since acquiring too much power can itself provoke other states into forming counter-balancing coalitions.

Although both have similarities in theories, they differ on the position of anarchy within the international context; Waltz's theory has central the role of the balance of power, in which states create alliances, especially with weaker states, so as to be able to balance the power of stronger states.

Waltz, therefore, also believes it is necessary to invest in his military power (internal balance) but at the same time he knows that the alliance between states is able to counter the stronger power (external balance), for this reason the distribution of power is also a fundamental element in order to achieve international results; Waltz also recognizes the importance of international institutions, but he does not believe they are the main actors, states are and remain the major decision-makers.

In short, realism should be read here as one paradigm with three connected layers: classical realism (Morgenthau), which locates the drive for power in human nature; neoclassical realism (Rose), which adds that domestic politics and leaders' perceptions filter how material power is actually converted into foreign policy; and neorealism (Waltz, and through him Mearsheimer and Gilpin), which locates that same drive in the structure of the international system itself. It is this last, structural layer that offers the clearest entry point for thinking about a material capability like Artificial Intelligence, and it is the one this chapter relies on going forward.

Technology as Material Capability

While both Waltz and Mearsheimer incorporate power and security into their frameworks of international relations, their theories centre on the actions of states in an anarchic environment and the distribution of capabilities. However, focusing on the distribution of power in absolute or static terms is not enough to account for the gradual evolution of power structures. In this sense, Robert Gilpin develops a realist theory and provides a more constructive model. In Gilpin's view, the changing international power configuration is linked to economic and technological development, and these elements are the underlying sources of state capabilities and the determinants of changes in the system.

Unlike Waltz, who focuses on the international system's structure, Gilpin focuses on the evolution of power. Here, technological change is important, as it leads to economic changes that affect the global power balance.

To understand the change in international relations and the advent of technology, it is important to analyse how technology becomes an integral part of resources, a multiplier of state forces, which is why his research focuses mainly on the economic and technological aspect and not merely on the distribution of power.

Gilpin incorporates economic efficiency and technological advancement as primary factors that drive states to upset the balance of world power; as noted above with Waltz's structural account, here the same underlying idea takes a dynamic form. When looking at the current state of the world, Artificial Intelligence is more than a tool or technology; It's a gamechanger for the way nations view wealth and military might. According to Gilpin, the uneven progress of disruptive technology will increasingly change the balance of power at a rate differentiated by the nations of the world. Gilpin's writings were produced prior to the rise of artificial intelligence, but his focus on technological and economic change as the engines of power transitions offers a useful lens for understanding AI as a source of systemic transformation. Gilpin's line of thinking allows for greater flexibility than his predecessors. It offers the theoretical support needed to consider AI neither as a new tool nor as a new weapon, but as the geopolitical game changer of a new hegemonic cycle.

Gilpin's most important studies and works focused on the analysis of industrial and technological policies, analysing and comparing a technological gap between the United States and European states (1968), emphasizing how technological problems are connected to the economic sphere and not purely political.

His analysis starts from understanding how the nature of power has changed over time and history, and how the great powers have found themselves in positions of decline, everything related to power dynamics.

Gilpin had certain research questions, based on change technology and efficiency were posited as two indissoluble factors in the modern age, in an era in which international needs meet growing material well-being.⁶

⁶ Neumann, I.B. and Ole Wæver (2005). *The Future of International Relations*. Routledge.

This is precisely where Gilpin's realism connects theory to technology: he also states that power changes according to the decline of great powers and in which "competition risks degenerating into technological wars" (Neumann and Ole Waever, 2005). Gilpin was a neorealist, but differentiated by the approach he used to do research, his utilitarian methodology and his ahistorical assumptions led him to write about change, about a third phase of the industrial revolution, in which the advent of industries led to the change of the commercial system, in which "economic efficiency and political power were increasingly interconnected", Analysing again how the situation of Russia under Gorbachev was also marked by a change of a technological nature, in which, falling behind with industrial progress, the Soviet economy declined, not keeping up with the innovation of Western countries despite being a country with a considerable but inefficient industry, thus contributing to the end of the Cold War.

Based on the evolution of power, technology, and international change, we see the flexibility of realism in contrast to the rigidity of Waltz's structuralism. Gilpin's ideas on the role of economic and technological changes in driving power supply a useful lens for assessing contemporary changes.

As we see, throughout the course of history the greatest state of technological revolutions has altered the distribution of capabilities among states. From the Industrial, Nuclear, to the Digital, technological supremacy has meant economic, military, and political dominance. Technological gaps have meant the ascendancy of new powers and the decay of old hegemonic powers.

According to Gilpin, power is dynamic and technology is not an external factor, but increasingly, one of the vital determinants of international order. So, among the disruptive technologies of the present, power distribution may never again be the same as it is today. Of all the technologies of the present age, Artificial Intelligence (AI) may be the most important of all in defining economic, military, and political power.

Artificial Intelligence as a Material Capability

Usually, artificial intelligence means any system that can perform cognitive functions such as learning, recognizing patterns, making predictions, or making decisions. AI is seen as a strategic technology across numerous industries because of its potential to change the nature of global politics. AI is universally applicable to civil and military functions.

Following Gilpin's work on technological change, modern scholars are seeing Artificial Intelligence as a new form of national power. Horowitz (2018) argues that AI is a general-purpose technology that has implications beyond the military domain, including economic growth, intelligence, and the shifting balance of power. More recently, Anthony King⁷ (2025) develops this line of thought further, arguing that AI is fusing the military and technology sectors into what he calls a new “military-tech complex”, in which the leading edge of military power increasingly depends on commercial AI firms rather than on defence industries alone.

Realism can be applied to technology and in modern contexts, since taking into account the main factor that sees anarchy and competition as the main structural form of international relations, Artificial Intelligence is denoted as a component, civilian and military, that can change the balance of power, as already noted above with Gilpin, though here the relevant mechanism is diffusion rather than differential growth. This introduces the concept of Dual Use Technology, which was born in the civilian sector and then transferred to the military field, making the diffusion on an extremely rapid scale, exponentially compared to technology of an exclusively military nature.

From a realistic point of view, AI is interpreted as a fundamental technology, capable of changing the rhythms and adoption of this technology for the great powers, trying to militarize it, not exclusively by will, but all the more as a strategic and competitive move, in a context where falling behind involves a perception of greater fragility and weakness.

As Horowitz points out, technology has had a significant impact in history, and that it depends strictly on the capabilities of states; before arriving at artificial intelligence, it is right to remember how a hundred years ago technologies such as printing made it possible to influence political life, consequently creating a new political activity⁸; nuclear weapons and deterrents were the new concept of defence, also increasing destructive capabilities, but technology has an impact on society also related to the sender who addresses it in some way, again taking the press as an example, the activity related to it depended above all on the incentives present and behind the political movements; this is to highlight how AI should be perceived rather as the

⁷ King, A. (2025). *AI, Automation, and War: The Rise of a Military-Tech Complex*. Princeton, NJ: Princeton University Press.

⁸ Eisenstein, E.L. (1979). *The Printing Press as an Agent of Change: Communications and Cultural Transformations in Early-Modern Europe*. Cambridge: Cambridge University Press.

driving force of a more complex system and tracing it back to a weapon can be reductive, because the range of action is much wider than the action of a weapon.

The competition that is created in order to have more AI-related resources is comparable to the competition that was created at the end of the nineteenth century for steel and chemicals, and this would also reduce the advantages of the "first mover", including other states in the balance of power than the United States and China.

The problem related to artificial intelligence clearly results in its being an extremely modern vehicle, not comparable for example to the first tank used in history, and therefore producing different initial effects, there is a need to adapt pre-existing theories on military technology and innovation.

Horowitz's theory is called Adoption Capacity Theory, which will allow us to understand how new developments on AI might take shape and enter the balance of power. The theory also argues that the speed with which a military innovation spreads and its effect on the balance of power depend on the financial and organizational requirements necessary for its adoption. Financial factors include unit costs and whether the technology is commercially available or exclusive to the military. Organizational factors relate to the extent to which adoption interferes with core military tasks or affects the status of key elites (e.g., fighter pilots). Since this theory focuses on major military innovations, it needs an adjustment to be applicable to current artificial intelligence.⁹

Legacy military technologies and Artificial Intelligence are similar in some respects, but the comparison only really holds along specific dimensions, which are worth spelling out. Historically, military technologies have been developed along national lines. Civil innovations, as they have been developed, have been commercially adopted, or even embedded, within military systems. For AI, there are several cross-cutting issues. First, dual-use technologies are developed and possessed by all states. Reluctant states, too, to "keep up." AI poses significant challenges that extend beyond military considerations. In general, the development of AI requires consideration of the broader systems of politics and the economy. Second, fully developed AI requires the work of institutions and systems of interdependence and

⁹ Horowitz, M.C. (2018). *Artificial Intelligence, International Competition, and the Balance of Power - Texas National Security Review*. [online] Texas National Security Review. Available at: <https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/>.

international governance. AI, more than some legacy military technologies, requires a cooperative approach to development.

Even with an emphasis on competition, power, and technology, realism fails to explain some aspects. Instead of focusing only on conflict and capability distribution, liberal theories prefer to focus on interdependence, institutions, and how international cooperation manages developing technologies.

Technology through Liberalism

It is right to emphasize how realism is useful for defining the behaviour of states and how they compete on emerging technologies, trying to acquire more power, but not explaining the process of spreading AI in a more concrete way, precisely because the latter has as its characteristic a strong interconnection between states unlike traditional weapons, and therefore there are more actors involved, of which states, but also international institutions and organizations, for this reason liberal theories, provide us with a better understanding and a perspective more oriented towards cooperation and interdependence as essential elements of the international system.

Liberalism, unlike realism, involves several actors in the international arena and not only states; Robert Keohane and Joseph Nye are scholars and great supporters of the idea that our system of international relations is made up by several connections, from which more reactions arise through channels of connection, in which military force is not the only one to act, we must take into account the economic and technological dimension. The realist perspective is therefore useful for understanding this emerging technological nature.

Previously, military structures were mostly controlled by the state, even if the private sector was never entirely absent: companies such as Lockheed, Boeing and General Motors were already deeply involved in war production during the Second World War, when arms manufacturing grew from roughly 1% to about 40% of US GDP¹⁰, but that involvement remained largely subordinate to state direction. Today, by contrast, the implementation of artificial intelligence is created and led by private companies such as Google, Microsoft, OpenAI, NVIDIA and Amazon, central holders of technological innovation at this time,

¹⁰ Higgs, R. (1995). *World War II and the Military-Industrial-Congressional Complex*. [online] The Independent Institute. Available at: <https://www.independent.org/article/1995/05/01/world-war-ii-and-the-military-industrial-congressional-complex/>.

placing themselves on the same level as states, for everything related to research, and finding new figures and resources, for this reason the technological developments in question cannot be considered state centric.

If we take into question Keohane and Nye's theory of interdependence, we can observe the multitude of channels of interaction, and a lack of hierarchy, and a weak and minimal military dependence, as an instrument of power.

The technological systems concerning AI, depend on a global supply chain, and infrastructures, international cooperation, public and private actors, for these reasons states cannot guarantee such a supremacy and independent of the international system itself.

Liberal theories state that institutions have the task of decreasing uncertainties and increasing cooperation, since they implement rules and guidelines that allow states to act in a more coordinated way with respect to their policies.¹¹

Within today's policies, the technological component is also expressed through governance mechanisms characterized by the transactional nature of AI, and the risks associated with it.

For this reason, the development of AI is the subject of debate for international organizations, in which on the one hand its use is encouraged and in multilateral forums it becomes the object of interest and ambiguity, since it requires the implementation of ethical principles and regulatory standards.

International organizations such as the OECD, UNESCO, UN, G7 and the EU, are the main promoters of the development of a line of principles related to AI. Cooperation between states and institutions regarding common guidelines reflects one of the liberal principles, namely cooperation, to mitigate technological competition, and promote principles of sharing.

But it should also be pointed out that liberalism highlights the essentiality of the economic factor and interdependence.

Technological ecosystems are interconnected and integrated, leading to innovation from cross-sector collaboration, involving government, business, university, and research communities. Knowledge, investment, and talent form cross-border networks, shattering barriers of

¹¹ Keohane, Robert O. (1984), *After Hegemony*.

geopolitical concern. This leads to interrelated forms of cooperation and competition in technology on a global scale.

Much of technological governance rests on the role liberalism places on non-state actors. Corporations are active participants in formulating guidelines and standards in the field of Artificial Intelligence due to their sway in the technology and business communities. Many researchers and experts work to establish guidelines for risk, as well as opportunities for international discourse in the field of AI.

Interdependence leads to more forms of competition and creates vulnerabilities. Countries must still try to secure their technological and strategic interests, but the state of innovation and the networks of global production mean these goals must also be flexible. This results in the same forms of cooperation and competition in current technological governance.

While realism focuses on the competition of Artificial Intelligence, liberalism shows that cooperation, institutions, and integrated networks of state and non-state actors rely on the same technology: concrete examples include the OECD AI Principles (2019), adopted by over forty countries, the Global Partnership on AI (GPAI), and the UN's High-Level Advisory Body on AI, all of which show states and non-state actors negotiating shared rules rather than simply competing for advantage. Focusing solely on the geopolitical competition of AI ignores the networks of global technology and governance frameworks. This creates the foundation for a constructivist view, where means and ideas shift focus away from institutions and material capabilities. Although liberalism offers insight into the significance of institutions, cooperation, and interdependence in the management of Artificial Intelligence, it lacks the tools to explain how the technologies become politically significant. Artificial Intelligence is characterized very differently at the global level. Rather, different states, institutions, and societies ascribe different values, identities, and expectations to it. The framing of AI as a potential economic opportunity, a national security concern, or a potential means for the achievement of technical sovereignty is only partially a function of the distribution of capabilities or the organization of institutions. Thus, the Constructivist approach, as opposed to the Realist or the Liberal, offers a politically meaningful interpretation of Artificial Intelligence by placing ideas, norms, and identities and the role of discourse at the centre.¹²

¹² Keohane, Robert O. and Nye, Joseph S. (1977), *Power and Interdependence*.

Technology through Constructivism

The social construction of reality, which consists of ideas and shared meanings and social norms, represents a different approach to international relations as opposed to the exclusive domination of material means, as believed by Realism, or the competition of power, or the cooperation and institutions of Liberalism. In contrast to these latter, Constructivism argues the importance of how political phenomena are assigned meanings by actors. This is also the approach followed by Calderaro and Craig¹³ (2020) in their work on the transnational governance of cybersecurity, which shows how norms and capacity-building around a digital technology are shaped as much by discourse and unequal participation as by material capabilities. In this sense, Alexander Wendt (1992) argues that "anarchy is what states make of it," and therefore international structures are not predetermined.

From a constructivist view, Artificial Intelligence cannot be seen as a neutral technology, or a material means of achieving power, a point that is crucial for this thesis, since it means AI's political significance cannot be read off its technical properties alone. Rather, its importance is dictated by the identities and dominant narratives. From a constructivist view, it is important to consider the political values and the culture of the different political actors who interpret Artificial Intelligence in diverse ways, e.g. from the perspectives of economic growth, national security, or technological sovereignty. Therefore, the political meanings of Artificial Intelligence are defined by the social interpretations given to it, rather than the technology itself.

Constructivists emphasize the role of social norms in international relations. In Artificial Intelligence, different ethical frameworks are starting to be reflected in global discourse on governance.

Norms play a vital role in influencing international behaviour, and constructivist scholars study this relevance. In the context of Artificial Intelligence, the international discourse has started to incorporate ethics, the establishment of standards, and the frameworks of governance. Debates on the trustworthy AI, transparency of algorithms, and the presence of humans in the centre of the AI design and governance discuss the ideas and norms to define the legitimate or

¹³ Calderaro, A. and Craig, A. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*. [online] Available at: https://cybilportal.org/wp-content/uploads/2020/10/CalderaroCraigTWQ_Transnational-governance-of-cybersecurity-policy-challenges-and-global-inequalities-in-cyber-capacity-building.pdf.

the acceptable use of technologies. These norms are actively constructed and supported by international organizations and communities of professionals, and they determine the frameworks of governance at the international level.

Narratives have become a crucial element in contemporary technological competition. Multiple actors present a myriad of competing visions of Artificial Intelligence. The United States frequently represents AI in the context of innovative leadership and the AI governance market. In contrast, the Chinese narrative relies on national rejuvenation and the self-sufficiency of technologies. Meanwhile, the European Union increasingly positions itself as a supporter of trustworthy and human-centered AI. These narratives heavily influence how actors position themselves in the global technological order and help shape preferences and identities.

In the competition for Artificial Intelligence, countries and organizations vie to shape ideas and to assert their influence and legitimacy. To correctly perceive this competition, purely material theories are to be disregarded. Instead, the relevance and importance of the social and political phenomena through which new technologies come to be defined is to be considered. The contemporary international order and the increased competition present a technological security dilemma. This situation is to be perceived in the context of the competition of technologies. It may be useful to consider how AI technologies acquire meaning over time.

Technological Security Dilemma

The theoretical frameworks discussed previously acknowledge that with every technological shift comes changes to state power, and subsequently, changes to state behaviours. The introduction of Artificial Intelligence poses challenges to traditional security concerns. As first described by John Herz (1950), the security dilemma concerns the situation in which, in the absence of a superordinate authority, states must provide for their own security. As no-state actor can be sure of the intentions of another state, actions taken to increase security cause competitors to feel threatened and to instigate security and trust-destroying actions in return.

According to Herz, this situation is a structural feature of the anarchic international system.¹⁴ The quest for security and self-preservation, although defensive, may create a situation of greater security dilemmas for other states. This situation of security dilemma and self-preservation instigates fear of the unknown and promotes a race to arm among states.

¹⁴ Herz, J.H. (1950). Idealist Internationalism and the Security Dilemma. *World Politics*, 2(2), pp.157–180.

In the case of Artificial Intelligence, the situation becomes more acute. Unlike other military technologies, Artificial Intelligence is unique in that it can be used for multiple purposes, and it rapidly diffuses and permeates the civil, commercial, and military domains. Even the furtherance of a state's Artificial Intelligence capabilities to enhance economic competitiveness and resilience may be construed by other states as an attempt to gain a competitive edge. As a result, innovation becomes a means of furthering competitiveness and a source of greater insecurity.

Robert Jervis (1978) expanded on the work of Herz, assessing how the security dilemma modifies with relationships of offensive and defensive capabilities.¹⁵ Jervis demonstrated that the security dilemma becomes more pronounced in instances when defensive and offensive technologies are hard to distinguish, and, when, offensive capabilities are perceived to be more dominant. The more difficult it is to distinguish offensive and defensive capabilities, the more likely states are to act competitively.

Artificial intelligence is the most exemplary case of this situation. It is easy to adapt civilian algorithms for AI to military AI.

Most AI algorithms have dual (and sometimes multiple) uses. As capabilities continue to reveal a dual-use nature in automated systems, surveillance, and even decision-making and control systems, states may view research and development in allied and non-allied states alike with growing concern.

As already discussed above, AI is a general-purpose, dual-use technology; the point that matters here is that this same feature also makes the AI security dilemma diverge from traditional models of arms racing, since the relevant competitors now include private industry and multinational firms alongside states.¹⁶

Therefore, old school military tactics alone will not aid understanding of technological rivalry.

The blend of uncertainty, fast pace of change, and the inability to differentiate between offensive and defensive capabilities creates a technological security dilemma. AI both creates

¹⁵ Jervis, R. (1978). Cooperation under the Security Dilemma. *World Politics*, 30(2), pp.167–214.

¹⁶ Horowitz, M.C. (2018). *Artificial Intelligence, International Competition, and the Balance of Power* - Texas National Security Review. [online] Texas National Security Review. Available at: <https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/>.

new material power and adds to the existing structural framework that creates mistrust and escalates geopolitical rivalry.

As Booth and Wheeler (2008) note, security dilemmas are not certain, but about the state in question, or the outcome of the dilemma, depend on the state of the interpreters and the behaviour of the others.¹⁷ However, in a world of growing technological interdependence and strategic rivalry, new uncertainties are added to international relations by Artificial Intelligence and sustain the belief that having the upper hand in technology is a core element of a state's security. Thus, AI produces a technological security dilemma that will most probably influence the future power relations and the strategies of the global powers.

Technology as a Structural Factor in the Redistribution of Power

The theoretical perspectives analysed in this section share several commonalities. They converge in their understanding that, while technologically driven changes do not represent simple means at the disposal of states, technology is a structural phenomenon that will impact the distribution of power in the international system. From the Industrial Revolution, through the development of nuclear weapons and information technologies, and now with the development of Artificial Intelligence, we see the most significant changes in competition and ranking among states.

From a Realist perspective, technologies shape the distribution of power and the nature of relationships among states. From Liberal approaches, the technologies, the institutions, the networks, and the inter- and trans-national structures that dominate the regulation of technologies and their innovations, represent the most significant structures. From a Constructivist approach, it is the meanings, the ideas, the narratives, and the technologies' politics and the norms that are dominant in the regulation of technologies. Taking all these approaches into account, we can say that the technologies and their innovations are integrated into the most complex political and economic structures.

Robert Gilpin has a valuable perspective on the relationship between technologies and innovations and their impact on the international arena. For Gilpin (1981), of all the dimensions of power, in the international arena, technologies and their innovations, and the economic

¹⁷ The Security Dilemma: Fear, Cooperation and Trust in World Politics, Ken Booth and Nicholas J. Wheeler (Basingstoke, UK: Palgrave Macmillan, 2008), 272 pp., \$112 cloth, \$38 paper. (2009). *Ethics & International Affairs*, 23(1), pp.82–82. doi:https://doi.org/10.1111/j.1747-7093.2009.195_1.x.

structures that integrate them, are the most significant. Since the unevenness and disparities in the international system are an inherent characteristic of the technological innovations, the emerging technologies and their innovations are the most significant factors in altering the distribution of power in the international system.

The impact of technology on global hierarchies and the balance of power further illustrates the fluidity of power. Power and resources have both quantitative and qualitative aspects. Advanced technology and the reorganization of military, economic, and strategic systems can shift the relative distribution of power. Because of this, power should be viewed as an adaptable construct defined by how well a state can embrace and use innovative technologies.

Artificial Intelligence, or AI, provides an example of this fluid relationship with technology. As Horowitz (2018) states, AI has the potential to improve a state's productivity, competitiveness, and even its ability to wage war. Interestingly, AI differs from other technologies with military applications because it can be developed in the civilian sector and is reliant on data, advanced microchips, and a highly educated workforce. Because of this, innovating AI requires a partnership between governments, the private sector, universities, and international networks.

The unbalanced growth of AI has created a new order of states with differing levels of power. The scale of the gap is striking: in 2024 alone, private AI investment reached \$109.1 billion in the United States compared to \$9.3 billion in China and \$4.5 billion in the United Kingdom, and cumulatively, between 2013 and 2024, the United States attracted \$470.9 billion against China's \$119.3 billion¹⁸. States that adapt AI to improve their economies and increase their national security will become more powerful and competitive. AI is fundamentally different from other technologies because it has the potential to reshape the international order and the distribution of power among states. If Artificial Intelligence is one of the main strategic technologies today, it is necessary to understand how it is shaping the contemporary concept of security.

These figures, however, should not be read as a straightforward promise of economic transformation, and it is worth pausing on the sceptical position that has been put forward by Daron Acemoglu, awarded the Nobel Prize in Economic Sciences in 2024. In his macroeconomic assessment of artificial intelligence, Acemoglu estimates that 'total factor

¹⁸ Stanford Institute for Human-Centered AI (2025). *The 2025 AI Index Report*. [online] Available at: <https://hai.stanford.edu/ai-index/2025-ai-index-report>.

productivity (TFP) effects within the next 10 years should be no more than 0.66%%', corresponding to an increase in GDP of about 1.16%% over the same period, and he insists that 'the aggregate effects from AI are likely to be modest'¹⁹. He also warns that 'AI is predicted to widen the gap between capital and labor income'²⁰, which means that the distributive consequences of the technology may turn out to be more significant than the growth it generates. This perspective matters for the argument developed here for two reasons. First, it shows that the enormous investment figures cited above are not, in themselves, evidence of a proportional shift in economic capability, so the competition between great powers over artificial intelligence is at least partly a competition over expectations and prestige rather than over already realised productive capacity. Second, it suggests that the political salience of artificial intelligence in international relations does not depend on its measured macroeconomic return, but on the belief, widely shared among governments, that whoever leads in this technology will lead in the next phase of the international order. For this reason, the analysis that follows treats artificial intelligence as a material capability whose strategic weight is real but whose economic promise remains contested.

1.2 AI and the Transformation of Security

Since the beginning of modern societies, the tools and methods used to protect the state from external threats have evolved steadily with innovations in warfare and industry. In more recent centuries, the balance of threats to state security has changed with more recent innovations, such as information technology (IT). While all these innovations have proven to be disruptive to strategic security and defence systems, Artificial Intelligence (AI) combines the characteristics of all previous disruptive innovations.

As stated in the previous paragraph, AI is a General-Purpose Technology (Bresnahan & Trajtenberg, 1995; Horowitz, 2018); here this matters specifically because its dual-use capability means AI does not leave a clear distinction between threats of war and peace or threats to external and internal security, that is, AI systems and algorithms developed for civilian use easily become tools of war and threats to state security.

¹⁹ Acemoglu, D., (2024). "*The Simple Macroeconomics of AI*", NBER Working Paper No. 32487, National Bureau of Economic Research, pp. 29-34; published in *Economic Policy*, 40(121), pp. 13-58 [online] Available at: https://www.nber.org/system/files/working_papers/w32487/w32487.pdf.

²⁰ Ibid., p. 36.

AI continues to disrupt security in all its forms, especially in its economic and military dimensions. It has completely changed the traditional concept of security. This includes the protection of critical digital infrastructures, the ability to manage large volumes of data, and the resilience of increasingly interconnected technological systems.

In this case, competition between states is no longer confined to the military sphere. The competition extends across the digital, cognitive, and informational spheres. Here, speed to advanced technologies and the ability to innovate are of greater importance (Nye, 2011; Gilpin, 1981).

Artificial Intelligence must be understood in the context of an international setting of rapid change in security and cannot be reduced to a technological tool. This paragraph attempts to describe this transformation by focusing on four specific areas:

the rapid transformation of defensive and offensive cyber capabilities, the creation of new challenges and opportunities in the use of military force through Autonomous Weapons Systems; the new frontiers of AI systems integrated into the Intelligence domain, with the automation of analysis and decision-making; and finally, hybrid warfare and algorithmic warfare, which clearly illustrate that contemporary competition between states is also conducted on the cognitive and informational fronts. These areas exemplify the ways in which AI is changing security from a military concept to a multidimensional reality that has a greater impact on the geopolitical order of the global system.

Cybersecurity and Automated Intelligence

After analysing how AI is able to play an ambivalent role in the civilian and military spheres, it is good to appropriately analyse all the dimensions in which it can act, and change the modern fate of security, minimizing the distinction between peace and conflict.

It is good to start by better understanding the field of cybersecurity, and how significant the impact of AI is on Cybersecurity.

Cybersecurity is everything related to IT systems, practices and defence of digital infrastructures, aimed at protection and cybersecurity, which consequently results in national security, since many infrastructures are involved, such as public administration, transport, digital infrastructure and services, finance, and manufacturing (ENISA THREAT

LANDSCAPE, 2025), making the state more prone to vulnerabilities, which can take a political, economic and strategic turn.²¹

For this reason, AI plays a fundamental role, since it is a tool capable of strengthening security measures, being fast and being able to detect threats in real time, also leaving more time for analysts to focus on other more complex activities.²²

For this number of reasons, AI plays a fundamental role in cyber defence, enabling the detection, prediction and mitigation of threats, also developing predictive systems, and predicting attacks that also come from malware, as demonstrated by machine learning technologies; AI could change a dynamic note, that of the Defender's Dilemma, in which AI could also help professionals in the field.²³

As highlighted by international reports, the ENISA Threat Landscape Report and the Microsoft Digital Defence Report, the use of AI in cybersecurity has now become an essential component for the world of security and digital defence strategies.

In the same way that it can harm, AI is also an offensive tool, the same tools used in defence can be used to create strategies and attacks on state and non-state structures. Studies conducted by Brundage (2018) show that automation, cost reduction, and high access to AI-based tools can emphasize the impact of cyber threats, increasing the speed of attacks.²⁴

This dual function of AI creates a sort of strategic competition within cyberspace, which creates a similar digital arms race, in which cyber resilience becomes almost mandatory, strategically speaking, inducing states to defend themselves and prevent cyber-attacks, putting cybersecurity and national security on the same level.

Citing organizations such as NIST, AI Risk Management Framework (2023), and the NATO Cooperative Cyber Defence Centre of Excellence, it is highlighted how it has become of essential importance to create new approaches and develop integrated systems of technological

²¹ ENISA THREAT LANDSCAPE. (2025). Available at: <https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf>.

²² Fortinet. (2019). *AI in cybersecurity: Key benefits, defense strategies, and future trends*.

²³ AT A GLANCE Digital issues in focus. (n.d.). Available at: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762292/EPRS_ATA\(2024\)762292_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762292/EPRS_ATA(2024)762292_EN.pdf).

²⁴ Brundage, M. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. [online] Available at: <https://arxiv.org/pdf/1802.07228>.

innovation and that it also points to international cooperation to address current and future challenges within the cyber dimension.

Autonomous Weapon Systems

The new technological systems are also composed of Autonomous Weapon Systems (AWS),²⁵ systems capable of working autonomously in recognizing targets, searching for and identifying targets and employing force; being a purely recent resource, there is no official definition, but the International Committee of the Red Cross defines them as "Any weapon system with autonomy in its critical functions—that is, a weapon system that can select (search for, detect, identify, track or select) and attack (use force against, neutralize, damage" (ICRC, 2021).

The peculiar feature of these systems lies not only in the automation of military operations, but in the development that AI is having towards the latter, capable of replacing even people's decision-making process, in rapid and complex contexts. As King (2025) argues, autonomous weapon systems are one of the clearest illustrations of how far the military-tech complex has already advanced, since their targeting and decision-making functions increasingly rely on commercial AI research rather than on dedicated defence R&D alone.²⁶

For this reason, machine learning and pattern recognition algorithms allow these autonomous systems to process larger amounts of data, finding a multitude of threats in a much shorter period than humans (Horowitz, 2018). To better understand the autonomy of these systems, two categories are divided: Human-in-the-Loop, a system in which the final decision is directly up to the human being, especially when related to the use of force, while in Human-on-the-Loop systems the system remains free to act, and the human being holds a supervisory role, in which he can intervene if necessary, and finally Human-out-of-the-Loop systems,²⁷ in which autonomy is maximum, and is placed to identify and acquire objectives, without being stopped or controlled by a human being (Arkin, 2009).

These terms and this type of classification are clearly used in the scientific literature, and within the United Nations, precisely to try to differentiate and understand how and in what form human control over autonomous systems is exercised.

²⁵ ICRC (2016). *Views of the ICRC on autonomous weapon systems*. [online] International Committee of the Red Cross. Available at: <https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system>.

²⁶ King, A. (2025). *AI, Automation, and War: The Rise of a Military-Tech Complex*. Princeton, NJ: Princeton University Press.

²⁷ Arkin, R. (2009). *Governing Lethal Behavior in Autonomous Robots*. CRC Press.

Ethically, this broad form of autonomy creates debates, and clearly leaving a word on the use of force to an algorithm remains a particular question, especially when it comes to respect international law, questioning the reliability of an algorithm in being able to comply with such important rules, when there is the life of the people in question, the distinction between combatants and civilians cannot be confused, how the proportionality of the attack must not exceed; From the moment one of these systems may go against humanitarian law, it becomes problematic to identify the person responsible in legal terms²⁸, since the responsibility could fall on the commander, the producer of the system, the programmer, or the state that authorizes this system. (Unoda.org, 2026)

These ethical and legal concerns have not stayed confined to academic debate: since 2013, the Campaign to Stop Killer Robots, a coalition of over 160 non-governmental organizations across 65 countries, has pushed for an international ban or strict regulation on fully autonomous weapons, arguing that removing meaningful human control from the use of force is both a moral and a legal problem.²⁹

Despite the doubts and problems, it is also good to underline the positive sides and the advantages connected to them, automation increases the speed of the decision-making process and is excellent in identifying targets, and these skills are fundamental in the international field, as they are the object of power multiplication, on the offensive and defensive level.

The AWSs are therefore systems born because of the strategic competition between great powers; therefore, essential in order not to fall behind in the technological field, similarly as happened with the introduction of nuclear weapons.

The security dilemma is certainly emphasized with the advent of these systems, because resources are perceived as threats, especially if they are particularly advanced, but being a product born from research, universities and technological companies, it once again emphasizes its dual-use nature, being effectively a product born from the civilian sector,

²⁸ Unoda.org. (2026). *Convention on Certain Conventional Weapons -Group of Governmental Experts on Lethal Autonomous Weapons Systems (2026)* | United Nations. [online] Available at: <https://meetings.unoda.org/ccw-convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2026>.

²⁹ Human Rights Watch (2018). *Heed the Call: A Moral and Legal Imperative to Ban Killer Robots*. [online] Available at: <https://www.hrw.org/report/2018/08/21/heed-call/moral-and-legal-imperative-ban-killer-robots>; see also the Campaign to Stop Killer Robots, Available at: <https://www.stopkillerrobots.org/>.

making it increasingly complicated to separate technological and military progress, making scientific skills the subject of international competition.

AWSs represent the transformation of the security system that creates strategic competition and creates new challenges within the international context.

AI and Intelligence

The integration of these new systems and AI, creates innovation in today's security, intelligence agencies, base their research and processing findings on a wide range of information derived from heterogeneous sources, capable of supporting both political and military decision-making; But in any case, making society highly digitized requires access to a growing database, which is why there is a need to introduce automated tools to provide analysis more quickly.

AI is an excellent solution to this issue, because it uses machine learning, computer vision and natural language processing (NLP) algorithms that could process massive amounts of data in an exceedingly small portion of time.

The combined analytical power of satellite imagery, electronic communications, social media, open-source data, various sensors, and surveillance operations can identify trends and anomalies that can signal threats that would be overlooked if analysed by just one person (Allen & Chan, 2017).

It is not enough to say that the deployment and integration of artificial intelligence (AI) into intelligence helps automate existing processes. It changes the very essence of how intelligence is produced. For example, algorithms can collect and query data quickly and help the analyst generate a thoughtful and strategic assessment. In this regard, AI is a decision support system; it increases the ability of operators to understand complex issues, while still requiring human judgment (RAND Corporation, Artificial Intelligence for Intelligence Analysis).

An important component is also represented by the automated analysis of satellite images; since there is a visual recognition that AI uses to find movement of vehicles, military installations, or any infrastructure used for military and strategic purposes, becoming an important aid to discover terrorist networks, precisely because predictive models are a great resource, useful for finding estimates and probabilities.

The application of artificial intelligence technologies has led to the emergence of predictive technologies, by which predictive models are built to predict the likelihood of future events. By combining the analysis of historical data with real-time data, the algorithms can identify signals that could precede political, economic, or even military instabilities, as well as cyberattacks. This provides policymakers with an additional tool for preventive action. Algorithms cannot accurately predict the behaviour of global players, but they improve the understanding of the situation and the speed of decision-making.

The operational benefits of using AI in intelligence are numerous, but there are also significant challenges, analysts depend on the data provided to them, and the outcome is influenced by the quality of that data. The use of inadequate, incorrect, or poor-quality data can cause biased results and exacerbate existing biases in information systems. In addition, overconfidence in AI's predictive ability can encourage decision-makers to delegate too much to algorithms and, as a result, reduce the value of human judgment. It is therefore not surprising that AI is considered an extension of the intelligence analyst, but not a replacement. This is due to the importance of the intelligence analyst in reading information within the political, cultural, and strategic framework.

From a geopolitical point of view, the use of AI represents a growing competitive advantage of one world power over the others. In an information age, the ability to acquire, process and use data more effectively and quickly than an adversary has significant value, the integration of AI into intelligence, is crucial in understanding how owning information is important and part of international power, since if a system is equipped with good strategic competition, and to process as much data as possible, represents an advantage, comparable to the economic or military one.

The transformations described demonstrate how the control of Artificial Intelligence is now intricately connected to national security and the distribution of international power. In this context, there is growing competition between states that invest in the development of AI.

1.3 The Global AI Competition: The United States and China

AI has quickly become a key asset that states are acquiring for use in modern geopolitical clashes. As already mentioned, of its ability to influence security, and the speed of technological and economic factors, the control of technologies that encompass AI has become

fundamental to the power of a state. As a result, the scope of international rivalry has expanded beyond the military capabilities of a state, now also including the ability to develop advanced algorithms, attract and cultivate quality human resources, control digital networks and infrastructure, and have a continuous flow of access to strategic technologies.

The United States and China are the dominant players in the international AI race, and both share the goal of dominating the technology, but adopt different means to achieve that goal. The United States relies on a model focused on collaboration between the public sector, academia, and private enterprises, while China has a state-led and state-coordinated development model, focused on technological and industrial security.

When we look at different systems, we begin to understand why AI is one of the most important tools for competing in a geopolitical strategy in the 21st century. The competition between the United States and China is not only about technology, but also about a broader competition for dominance in the economic, military, and geopolitical spheres, which will determine the future of the international order. This will affect the European Union and other entities.

The United States: Innovation and Technological Leadership

The United States currently represents the global leader in the development of Artificial Intelligence, thanks to an ecosystem that combines scientific research, public investment, technological innovation, and private entrepreneurship. This ecosystem has enabled the country to maintain a leading position in AI research, innovation, and commercialization, making Artificial Intelligence a key strategic asset for economic competitiveness and national security.³⁰

In fact, the United States possesses about 74% of the capacity of high-end AI supercomputers (Haag, 2025), with an expenditure of about \$109.1 billion, used for major innovations led by companies such as OpenAI, Google DeepMind, Microsoft, Meta, Amazon and NVIDIA, becoming real essential economic players, and acting as strategic and technological resources for the United States.

³⁰ Haag, A. (2025). *The State of AI Competition in Advanced Economies*. [online] Federalreserve.gov. Available at: <https://www.federalreserve.gov/econres/notes/feds-notes/the-state-of-ai-competition-in-advanced-economies-20251006.html>.

But the United States does not enjoy solid leadership only thanks to the role of big tech, but on the contrary, the public sector remains the fundamental basis on which innovation itself revolves.

Taking DARPA (Defence Advanced Research Projects Agency) as a reference,³¹ it is clear that the agency has led AI research from 1960 to today (Darpa.mil, 2018), investing in and financing projects dedicated to technological development in both the military and civilian fields.

At the same time, the Department of Defence (DoD) is also committed and present in financing projects concerning AI ³²with an aggressive policy in which we see a modernization characterized by "AI-first", in which spending becomes increasingly massive, even if the total is not clear, since the army is also investing heavily in the development of autonomous weapons, where the Pentagon has requested \$13.4 billion for 2026 alone. (Amos & Emile, 2026).

Since AI is such an important and present entity in American security affairs, the US government introduced the National Security Commission on Artificial Intelligence (NSCAI), an independent body created by Congress that published a final report in 2021 in which it was made clear that AI would be able to profoundly change the American economy, national security and welfare, therefore destined to change forever the political, military and technological balances of the twenty-first century, for this reason the US government decided to invest deeply in research and human capital.

In the same document, this concept is emphasized several times: "The United States is not in a competition with China. It is in a technology competition."³³

Marking how investments are more than simple money connections but that they are the result of systemic competition that also involves China and identified as the major competitor of the US.

In this context, it is also appropriate to talk about the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act, a federal law introduced in 22, in which the goal

³¹ Darpa.mil. (2018). *AI Next*. [online] Available at: <https://www.darpa.mil/research/programs/ai-next>.

³² (2026). *The Military's Use of AI, Explained*. [online] Brennan Center for Justice. Available at: <https://www.brennancenter.org/our-work/research-reports/militarys-use-ai-explained>.

³³ Final Report National Security Commission on Artificial Intelligence. (n.d.). Available at: <https://www.dwt.com/-/media/files/blogs/artificial-intelligence-law-advisor/2021/03/nscai-final-report--2021.pdf>.

was to strengthen the national production of semiconductors through large funding, which was also raised to improve scientific research, thus increasing the industrial policy of the United States.³⁴

CHIPS was important in attracting microchip production to the US (Cfr.org, 2024) by ensuring that 40% of the world's semiconductor supply was produced, becoming an essential element of the national security strategy, while also trying to decrease dependence on other global supply chains, so as to be able to function as an "obstacle" for other rival powers.

As mentioned above, the United States has also progressed in the field of research, investing heavily in universities and research centres, in fact, Massachusetts Institute of Technology (MIT), Stanford University, Carnegie Mellon University and the University of California, Berkeley, are the historical and innovation core for the research and development of artificial intelligence, even worldwide.³⁵

The U.S. funds universities through competitive federal grants, which are issued by government agencies, and are strategic investments led by the National Science Foundation (NSF), the Department of Energy (DoE), and the National Institute of Health (NIH). Through the design of new resources, the collaboration between governments, companies and universities, security takes a new shape with the application of AI, growing the sectors that will soon be shaped by AI.³⁶

This ecosystem allows the United States to foster knowledge in the technology sector and to attract professionals and researchers, from all over the world, to allow it to remain in a leadership position in scientific production and everything related to AI innovation.

Overall, what makes the United States a country with leadership is scientific research through public investments that make the United States a decidedly competitive system in which artificial intelligence has been transformed into a tool for security, economic growth and strong technological superiority that becomes a strategic advantage in the international context. But such leadership is not the real end because it is highlighted that the United States is not alone, but rather is in competition with China., and this emerges from the National Security

³⁴ Cfr.org. (2024). *What Is the CHIPS Act?* | *Council on Foreign Relations*. [online] Available at: <https://www.cfr.org/articles/what-chips-act>.

³⁵ QS World University Rankings by Subject 2026: Data Science and Artificial Intelligence. [online] Available at: <https://www.topuniversities.com/university-subject-rankings/data-science-artificial-intelligence>.

³⁶ NSF - U.S. National Science Foundation. (2025). *National AI Research Institutes*. [online] Available at: <https://www.nsf.gov/focus-areas/ai/institutes>.

Commission's Final Report Intelligence Artifice (2021), a document that shows the critical elements of AI as a political asset, and highlights that this leadership cannot be taken for granted as China is changing the international balance.

China: State-led Development and Technological Sovereignty

China's rise in the technology and AI sector represents an extremely significant scenario in the geopolitical landscape, in recent years, China has tried to narrow the technological gap with the US, also becoming one of the largest international players in AI development. The gap in private investment remains wide: in 2025 the United States attracted \$285.9 billion in private AI investment against China's \$12.4 billion, roughly a 23-to-1 ratio, but China continues to lead in AI patents and research publications, and the performance gap between the two countries' best AI models narrowed to about 2.7% in 2025, showing that the gap is closing on some dimensions even as it widens on others.³⁷

Unlike the American model, which is composed of a strong and predominant component of the private sector, China has a diametrically opposed structure, since it is characterized by state planning, which sees the government as a central actor in defining technological priorities, especially with regard to research funding, and coordination between institutions, universities and companies.

An important point is represented by the publication of the New Generation Artificial Intelligence Development Plan in 2017, a document in which the state council declared the existence of a national strategy in order to make the country the main world leader in AI by 2030, a plan characterized by three phases and targets, the goal of 2020 was to align with other world leaders in the AI field, The first step to introduce the first significant progress, in 2025 the goal was to make AI the engine of Chinese society and economic transformation, together with the introduction of legislation, and by 2030, clearly make China the world's first centre of AI innovation.³⁸

The plan is created to modernize industry and national security, but within this theory, the concept of technological sovereignty is intrinsic, i.e. the ability to independently develop one's own technologies and national security, with the aim of reducing dependence on other

³⁷ Stanford Institute for Human-Centered AI (2026). *The 2026 AI Index Report*. [online] Available at: <https://hai.stanford.edu/ai-index/2026-ai-index-report/economy>.

³⁸ Eto.tech. (2017). *New Generation Artificial Intelligence Development Plan – ETO AGORA*. [online] Available at: <https://agora.eto.tech/instrument/1065>.

countries, decreasing strategic vulnerabilities, especially in critical sectors such as semiconductors and AI.

Unlike the United States, technological innovation in China is largely coordinated by the State. Through national programmes such as Made in China 2025 and the Military-Civil Fusion strategy, the Chinese government promotes close cooperation between research institutions, industry and the defence sector, accelerating the transfer of technological innovation into strategic and military applications. This approach reflects the central role of the State in directing technological development and integrating Artificial Intelligence into China's broader industrial and national security strategy.³⁹

The Chinese private sector also plays a key role, companies such as Baidu, Alibaba, Tencent, Huawei and SenseTime are essential players in the development of AI, contributing in areas related to machine learning, computer vision, speech recognition and generative AI systems.

These companies are under the regulations imposed by the central government, defining a strategic framework prepared for the achievement of national objectives.

Although China adopts a different way of operating than the West, the sector still has critical issues related to the dependence on foreign companies, due to semiconductors that are mostly produced abroad, and together with the export restrictions introduced by the US, accentuate how the control of technologies is actually one of the most influential tools of contemporary geopolitical competition, which, like a chain reaction, leads China to increasingly want to increase investment in domestic chip production and to invest in strategic technologies.

In sum, the Chinese model shows the deep connection between Artificial Intelligence and national development, industrial policy and security objectives. Whereas innovation in the United States is primarily market-driven, China relies on a state-led model where AI is a strategic instrument of national power.

The Militarization of Artificial Intelligence and the Global Semiconductor Race

The competition between the US and China in the field of artificial intelligence is comparable to a technological cold war, as Chris Miller documents in detail in his history of the global

³⁹ Allen, G.C. (2019). *Understanding China's AI Strategy*. [online] Cnas.org. Available at: <https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy>.

semiconductor industry⁴⁰, but it does not depend only on economic or industrial factors, but on the contrary, it has a strategic and political character. In fact, AI is perceived by both states as a technological resource that influences the way in which politics and military actions are undertaken, acting as a very useful resource especially in collecting data, analysing them, undertaking decision-making processes, cybersecurity actions and strong control capabilities.

For this reason, the militarization of AI becomes the fulcrum of today's technological competition, linking scientific innovation directly to national security and the way in which international power is distributed.

In the US, this role is attributed to the Department of Defence and the National Security Commission of Artificial Intelligence. Mentioning again the NSCAI's final report of 2021, he highlights how AI will certainly be an important influence factor, especially for the future of the American economy and militarization, in which investments in the public sector will be increasingly evident, which will also collaborate more with the private and defence sectors, implementing AI in national security systems.

AI, therefore, is of fundamental importance to maintain supremacy and strategic superiority for both giants.

China perceives this importance in the same way as its rivals, its strategy is expressed through the strategy of Military-Civil Fusion, in which the aim is to eliminate the barriers between the commercial and academic sector and technology and the People's Liberation Army (PLA), trying to dominate the war sector by integrating AI and dual-use technology, research and civil innovations in military and weapon systems.⁴¹

However, the militarization of AI is heavily dependent on the access of advanced semiconductors; AI systems need sophisticated systems given their large computing capacity that are made possible by extremely sophisticated and innovative chips and GPUs. Without this component, autonomous and military systems risk being heavily hampered, not allowing the development of complex AIs. For this reason, we cannot simply speak of competition on

⁴⁰ Miller, C. (2022). *Chip War: The Fight for the World's Most Critical Technology*. New York: Scribner.

⁴¹ Cesi-italia.org. (2020). *China Pushes Military Modernization Accelerator* | Ce.S.I. Center for International Studies. [online] Available at: <https://www.cesi-italia.org/it/articoli/la-cina-spinge-lacceleratore-della-modernizzazione-militare>.

AI, but mostly competition on global semiconductor chains, which also becomes a powerful indicator of power in the geopolitical landscape.⁴²

And this is where the "Chip-War" is at stake, the fulcrum of a fierce competition for the United States and China, placed at the centre of the global economy and defence.

The United States, through the CHIPS and Science Act, seeks to strengthen itself and above all to limit Chinese access to the most sophisticated technologies, imposing restrictions on the import of chips and resources around the production of software and semiconductors, and this is in fact a very strong political and commercial strategy.

China, in turn, perceives restrictions as a kind of strategic vulnerability and in response has intensified investments in the sector, so as not to have to be dependent on the acquisition of semiconductors; in any case, technological self-sufficiency is not yet feasible, since the global supply chain of this technological material involves other global players such as Taiwan, South Korea, Japan, the Netherlands and the United States. Companies such as TSMC, NVIDIA and ASML occupy central positions within this chain.⁴³

Advanced AI systems is therefore confirmed as a system deeply linked to international technological dependencies, and the race for semiconductors underlines how technological power is dependent on software, hardware but also human capital and supply chain, involving multiple fields, including economic, commercial, geopolitical and security.

From this review of realist and adoption-capacity perspectives, the following analytical framework emerges, which will guide the analysis of the EU's role in Chapters II and III: Waltz and Mearsheimer explain why states treat AI as a matter of survival and relative power, Gilpin explains why the uneven pace of technological and economic change is what actually redistributes that power over time, and Horowitz's Adoption Capacity Theory explains the concrete financial and organizational conditions under which a state can turn AI into usable capability rather than just potential. Put together, these perspectives suggest that AI's

⁴² Center for Strategic and International Studies, (2023). "China's New Strategy for Waging the Microchip Tech War" [online] Available at: <https://www.csis.org/analysis/chinas-new-strategy-waging-microchip-tech-war>.

⁴³ Center for Strategic and International Studies, (2025). "The Limits of Chip Export Controls in Meeting the China Challenge" [online] Available at: <https://www.csis.org/analysis/limits-chip-export-controls-meeting-china-challenge>; Center for Strategic and International Studies, (2025). "Countering China's Challenge to American AI Leadership" [online] Available at: <https://www.csis.org/analysis/countering-chinas-challenge-american-ai-leadership>; Stockholm International Peace Research Institute, (2026). "AI in Chinese, Indian and US Nuclear Postures, Norms and Risk Reduction" [online] Available at: https://www.sipri.org/sites/default/files/2026-02/2602_ai_integration.pdf.

geopolitical effects depend less on the technology itself and more on which states and blocs are structurally best placed to adopt it quickly and at scale, and it is against this framework that the European Union's regulatory strategy, examined in the following chapters, has to be assessed.

The European Union is trying to find its own strategic role against the backdrop of growing international polarization. The EU has adopted a different stance from that of the United States and China, primarily using regulation and governance as instruments to shape the global development of Artificial Intelligence. The analysis of this strategy is given in the next chapter.

Chapter II - The European Union's AI Strategy: From Regulation to Geopolitical Influence

The central role of artificial intelligence in international competition has radically altered global dynamics, and as analysed in the first chapter, AI is now perceived as a strategic resource that can profoundly affect national security, the distribution of power, and commercial and economic competitiveness. The rivalry between the US and China has become the defining feature of contemporary technological development, giving rise to a full-blown race for control over technology and global supply chains.

However, this analysis does not aim to focus solely on this dual dimension; rather, it seeks to examine more closely other actors capable of exerting a similar influence, albeit using systems and tools that differ from military and technological superiority.

The European Union, in fact, occupies a unique position: although it does not possess the same industrial, military and financial resources, the EU has implemented a strategy based on regulation, the setting of common standards and governance policies regarding emerging technologies, with the aim of guiding its own values and strategies.

It is worth noting at the outset, however, that the financial resources the Union has been able to mobilise for artificial intelligence remain very limited when compared with those of its competitors, and this asymmetry conditions everything that follows. In February 2025 the Commission launched the InvestAI initiative, presented as a plan ‘to mobilise €200 billion for investment in artificial intelligence’, including a new European fund of €20 billion for AI gigafactories⁴⁴. The headline figure is nevertheless misleading, since most of it is expected to come from private and national sources: the European Court of Auditors has observed that only about one tenth of the announced amount is direct EU funding, and that the Union cannot clearly track who will actually invest the rest⁴⁵. The genuinely European instruments are considerably smaller: the AI Continent Action Plan relies on around €10 billion committed

⁴⁴ European Commission, (2025). “*EU launches InvestAI initiative to mobilise €200 billion of investment in artificial intelligence*”, Shaping Europe’s Digital Future [online] Available at: <https://digital-strategy.ec.europa.eu/en/news/eu-launches-investai-initiative-mobilise-eu200-billion-investment-artificial-intelligence>.

⁴⁵ European Court of Auditors, (2025). “*The EU promises €200 billion for AI but cannot clearly track who will invest the money*”, reported in *2eu.brussels* [online] Available at: <https://2eu.brussels/en/news/european-court-of-auditors-warns-the-eu-promises-eur200-billion-for-ai-but-cannot-clearly-track-who-will-invest-the-money>.

between 2021 and 2027 for the network of thirteen AI Factories⁴⁶, while the Apply AI Strategy of October 2025 mobilises about €1 billion⁴⁷. The comparison with the United States is stark: private investment in artificial intelligence reached \$109.1 billion in the United States in 2024 and \$285.9 billion in 2025, against \$12.4 billion in China, while the four largest American technology firms alone are expected to spend in the order of \$700 billion in capital expenditure in 2026⁴⁸. Bruegel researchers have drawn the obvious conclusion, namely that the Union has to decide whether it can realistically catch up with the technological frontier or whether it should concentrate on diffusing and applying technologies developed elsewhere⁴⁹. The regulatory ambition examined in this chapter therefore develops against a background of comparatively modest public resources, and this is precisely why regulation, rather than industrial capacity, became the Union's main instrument of influence.

The European approach is not merely intended to limit risk management, but to create a broader vision of the EU within the international system. Proposed legislation such as the AI Act, together with a strong focus on technological sovereignty and related issues, is intended as a means for the EU to exert influence beyond its borders by helping to define regulations for the development and deployment of artificial intelligence at a global level.

This chapter therefore aims to analyse the European strategy in the AI sector, seeking to examine in depth the approach and policies implemented in recent years. The way in which regulations will be implemented as a geopolitical tool will form a fundamental part of the research, highlighting how the EU will assert its presence on the international stage through regulations rather than through the possession of more advanced technologies.

2.1 The Evolution of the European Union as a Regulatory Power

⁴⁶ European Commission, (2025). “*Communication on the AI Continent Action Plan*”, COM(2025) 165 final, p. 4 [online] Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:8707360e-15f6-11f0-b1a3-01aa75ed71a1.0001.02/DOC_1&format=PDF.

⁴⁷ European Commission, (2025). “*Questions and answers on the Apply AI Strategy*”, QANDA/25/2300 [online] Available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_25_2300/QANDA_25_2300_EN.pdf.

⁴⁸ Stanford Institute for Human-Centered Artificial Intelligence, (2026). “*AI Index Report 2026, Chapter 4: Economy*” [online] Available at: https://hai.stanford.edu/assets/files/ai_index_report_2026_chapter_4_economy.pdf; CNBC, (2026). “*Google, Microsoft, Meta and Amazon AI spending*” [online] Available at: <https://www.cnbc.com/2026/02/06/google-microsoft-meta-amazon-ai-cash.html>.

⁴⁹ Bruegel, García-Herrero, A. & Martens, B., (2025). “*Catch us if you can: prospering below the technological frontier and the EU's artificial intelligence strategy*”, Policy Brief [online] Available at: <https://www.bruegel.org/policy-brief/catch-us-or-prosper-below-tech-frontier-eu-artificial-intelligence-strategy>.

Any discussion of the European Union as a regulatory power has to start from Giandomenico Majone, who first described the emergence of what he called the regulatory state in Europe. Writing in 1994, Majone argued that ‘the growth of regulation is one of the most significant political developments of the last two decades’ and explained the shift by noting that, as direct state intervention through public ownership and public spending became increasingly constrained, rule-making became the instrument through which public objectives could still be pursued⁵⁰. The Community, in his reading, was the clearest illustration of this logic, because it had almost no budgetary or taxation powers of its own and could therefore expand its influence mainly by regulating⁵¹. This insight is the necessary starting point for the whole chapter: the Union did not choose regulation over industrial policy because it considered rules intrinsically superior, but because rule-making was the resource actually available to it. Everything that follows, from normative power to market power to the Brussels Effect, can be read as a further specification of Majone’s original observation, and the difficulties the Union now encounters in the field of artificial intelligence are, in the same way, the difficulties of a polity that is institutionally equipped to regulate a technology it does not produce.

The role of the European Union as a regulatory power is a much-debated topic in contemporary literature on international relations. Over time, many scholars have felt it necessary to explain how the EU manages to exert such international influence through the use of normative, regulatory and economic instruments, giving rise to an analysis based on the interpretation of European power; this is the aspect on which my analysis will focus most closely, in order to understand how the EU utilises its resources and how it exercises its regulatory power.⁵²

Ian Manners (2004) conducted studies on the role of the EU, and in describing its international role, he explains how 'civilian power' and 'military power' are two categories which, on their own, are not sufficient to convey the true nature of the EU's influence. The author emphasises that the distinctive feature of the EU does not lie solely in its economic and military capabilities; rather, the EU's true strength lies in 'the ability to shape conceptions of normal' (Manners, 2004); European normative power lies in the ability to influence what is perceived as normal

⁵⁰ Majone, G., (1994). “*The rise of the regulatory state in Europe*”, *West European Politics*, 17(3), pp. 77-101, at pp. 85-87 [online] Available at: <https://betterregulation.lumsa.it/sites/default/files/betterregulation/Majone%201994.pdf>.

⁵¹ Ibid., at p. 98.

⁵² Kennis, A. and Liu, X. (2024). *The European Union's Regulatory Power: Refining and Illustrating the Concept With the Case of the Transfer of EU Geographical Indication Rules to Japan*. *Journal of common market studies*. doi:10.1111/jcms.13579.

and legitimate, and thus in disseminating values, rather than imposing its will through coercive measures.

According to Manners, this normative value stems from three essential elements: the post-war European historical context; the political structure, identified as hybrid, capable of transcending the purely Westphalian conception; and its legal framework, which is based on shared values, positioning the EU as an institution distinct from other traditional state powers; furthermore, the EU promotes peaceful, democratic values, with full respect for the rule of law and human rights, thereby shaping the nature of the EU.⁵³

Ian Manners' work represented a more fundamental milestone for scholars seeking to identify the European Union's position within the world order. However, with the market becoming increasingly interconnected, there has been a growing academic impulse to regard the European Union as an emerging form of power. Indeed, building on Manners' approach to Europe's normative power, most scholars recognise the European Union's ability to project its policies within global value chains. However, Manners' approach does not address how the Union reshapes global economic and social structures.

In particular, Damro introduces the concept of Market Power Europe. In contrast to Ian Manners' value-based approach, Damro focuses on the economic aspect of the European integration project and argues that the Union's main source of influence lies in the structure of the Single Market and its ability to utilise the Union's international influence by regulating market access.

Building on the debate initiated by Manners, David Damro (2012) proposes an alternative framework for conceptualising the European Union's international position, introducing the concept of 'Market Power Europe' (MPE).

Damro suggests that the EU's main source of influence is *not* the export of values and principles, but rather the scale of the European single market. Damro refers to this as 'Market Power Europe' as a way of understanding the Union's power as the power to regulate markets and argues that the ability to influence the actions of international actors stems from a combination of three main elements: the size of the single market, the Union's capacity to create and enforce a legal framework, and the capacity and willingness of EU institutions, Member

⁵³ Manners, I. (2002). Normative Power Europe: a Contradiction in Terms? *JCMS: Journal of Common Market Studies*, 40(2), pp.235-258. doi:10.1111/1468-5965.00353.

States and interest groups to engage in ongoing dialogue to shape Union policies. Within this framework, the European single market is not merely an integrated economic market, but a means of projecting Europe's power and has the potential to influence the actions of businesses and states beyond the EU's borders. Rather than resorting to traditional coercive methods, the EU uses the appeal of its market to exert influence, as access to the EU's nearly 450 million consumers act as an incentive for businesses to comply with EU regulations and standards. This translates into a perspective of indirect EU policies.

Damro's thinking helps us to understand the natural progression of the 'Brussels Effect', through which European standards become a benchmark with global reach.⁵⁴

Damro's model is fundamental to understanding key EU phenomena, because whilst the MPE reflects how the EU exercises its influence through its market, the 'Brussels Effect' developed by Anu Bradford reflects how such influence can actually translate into the global dissemination of European standards, positioning regulation as the EU's primary instrument of projection.

The Brussels Effect: From Market Power to Global Standards

According to Anu Bradford (2020), the EU is perceived as a holder of regulatory power because it is a skillful actor in incorporating standards and reintroducing them into the global market through the well-known 'Brussels Effect', the effect whereby European laws are able to shape international dynamics and the global market can be described as 'unilateral regulatory globalisation', becoming the EU's strength that enables it to compete with major powers. Although European standards are intended for member states, they consequently also influence other international actors and their commercial practices; however, this does not occur through coercive means but rather through the economic choices of international firms; and so, as the EU is a large market that international firms cannot afford to ignore, they might modify their products and sell a new version, but the costs would outweigh the benefits; for this reason, many firms end up adopting European standards, thereby transforming European regulation into global standards.

⁵⁴ Damro, C. (2012). Market power Europe. *Journal of European Public Policy*, [online] 19(5), pp.682-699. Available at: https://www.pure.ed.ac.uk/ws/portalfiles/portal/10091990/DAMRO_2012_Market_power_Europe.pdf.

Bradford describes five key conditions for the Brussels effect to occur. The first three are that there must be a substantial market capable of attracting foreign economic agents, that the EU must be able to create and implement its own standards, and that the EU tends to adopt stricter standards. The last two are objectives set primarily within the EU: namely, the consumer market and the indivisibility of production, that is, the technical or economic impracticality of maintaining different production standards in different markets. These conditions mean that European standards are capable of dominating at a global level.

This analysis can be linked to the positions of the US and China, since China does not have regulatory institutions that are sufficiently mature to exert influence on a par with the EU, whilst the United States, despite having strong institutional capacity, does not share the same inclination to adopt such rigorous regulatory standards. For this reason, the EU continues to be the leading player as a global regulator across a range of economic sectors.

The 'Brussels effect' demonstrates that the EU is adept at influencing policies and regulations not through the use of coercion or military might, but rather through its ability to use the single market as a lever to steer corporate behaviour, thereby spreading its regulatory standards and becoming the EU's most significant tool for influencing the entire international system.⁵⁵

However, the gradual intensification of technological competition between the US and China highlights how regulatory power alone is not sufficient to ensure competitiveness in strategic sectors; for this reason, it is necessary to introduce the concepts of digital sovereignty and strategic autonomy, concepts which, in recent years, have formed a cornerstone of the European strategy in the field of artificial intelligence.

Digital Sovereignty and Strategic Autonomy

Although the EU is highly adept at regulation, it struggles to achieve technological autonomy, making digital sovereignty a crucial challenge, as it finds itself in a position of dependence on foreign actors.

There are persistent technological dependencies of the European Union on external actors, making it urgent to resolve this issue. The EU has played (and will continue to play) an important role in setting global regulatory standards. However, a large proportion of the world's

⁵⁵ Bradford, A. (2020). *The Brussels effect: how the European Union rules the world*. New York, NY: Oxford University Press.

digital infrastructure, advanced cloud systems, advanced semiconductors and most large-scale artificial intelligence models are developed and controlled by US or Chinese companies. This imbalance highlights what many authors refer to as the 'European paradox'.

In other words, the EU is a key player in the global export of rules and standards, but it relies heavily on other actors for the development of the technologies that incorporate these rules and standards. The EU's digital sovereignty is defensive in nature, aimed at addressing its vulnerabilities, but the EU also seeks to balance this position with the well-known principles of solidarity and intra-Community cooperation.

The pursuit of greater technological sovereignty must be viewed within the framework of European strategic autonomy. The concept of strategic autonomy does not imply withdrawal, total self-sufficiency or the end of European integration, but rather the European Union's ability to act autonomously, whilst maintaining cooperation with allies and partners. This is set out in the 2022 Strategic Compass for Security and Defence. The document aims to make the EU better able to protect its citizens, its interests and its values, whilst at the same time strengthening its strategic autonomy to act alongside other international actors. The document structures European action around four pillars: acting, protecting, investing and collaborating, and links operational capabilities with protection against hybrid and cyber threats, investment in technological and industrial capabilities, and international cooperation.

The concept has also been subjected to careful conceptual scrutiny. Daniel Fiott distinguishes what he calls three images of European strategic autonomy, showing that the term is used simultaneously to describe the Union's capacity to act, its degree of dependence on others, and its ambition to shape the international environment, and that these three meanings do not always point in the same policy direction⁵⁶. In more recent work he and Renaud Bellais examine security of supply and industrial interdependence, arguing that autonomy in practice depends less on declaratory objectives than on the resilience of supply chains and on the Union's ability to convert threat assessments into common action⁵⁷. This distinction is useful for the argument of this thesis, because in the field of artificial intelligence the Union clearly

⁵⁶ Fiott, D., (2025). "*The three images of EU strategic autonomy*", *Journal of European Integration* [online] Available at: <https://www.tandfonline.com/doi/full/10.1080/07036337.2025.2537369>.

⁵⁷ Bellais, R. & Fiott, D., (2026). "*Security of Supply and Interdependence*", ARES Policy Paper No. 131, IRIS, June 2026 [online] Available at: https://www.iris-france.org/wp-content/uploads/2026/06/ARES_2026_06_131_Security_Supply_Interdependence_PolicyPaper.pdf; Fiott, D., (2026). "*The Strategy Trap? European Threat Assessments and the Problem of Common Action*", CSDS Policy Brief 17/2026 [online] Available at: <https://csds.vub.be/publication/the-strategy-trap-european-threat-assessments-and-the-problem-of-common-action/>.

possesses the third form of autonomy, the ability to shape the rules others follow, while lacking the first two, the capacity to act independently and freedom from external dependence. Strategic autonomy in the digital domain is therefore not a single objective but a set of partly incompatible ones, and the AI Act should be read as an attempt to secure the form of autonomy that was actually within reach.

In a digital context, strategic autonomy is both an economic and a security issue. The Strategic Compass identifies the need to improve Europe's resilience to cyber and hybrid threats, to protect critical infrastructure, and to reduce structural technological and industrial dependencies. The tools include enhancing the capabilities of security and defence structures, an advanced Cyber Diplomacy Toolbox, greater preparedness for cyber-attacks, and joint investment in advanced technologies. The underlying rationale is that autonomy is not achievable solely through the establishment of a common set of rules, but rather through the combination of physical, industrial and operational resources that give the Union the capacity to protect its digital space.

The 2023 European Economic Security Strategy offers a more nuanced interpretation of this formulation. The document notes that economic interdependence is both a source of growth and a potential source of vulnerability, which can be exploited for geopolitical pressure. To address this reality, the strategy proposes a risk-mitigation framework, which prescribes an approach distinct from economic decoupling. Under this framework, the strategy does not aim to completely cease trade and technological relations with third countries, but rather to identify and mitigate the risk of dependency as the least desirable outcome.

This framework focuses on vulnerabilities in supply chains by minimising the EU's economic exposure to coercive actions, disruptions to production and trade, and inappropriate transfers of sensitive technologies. The instruments and measures implemented should adhere to the principles of proportionality and precision and cover only those sectors and technologies exposed to the greatest strategic risks.

The strategy identifies four categories of risk to Europe's economic security. The first concerns the resilience of supply chains, with the potential unavailability of critical goods and services. The second concerns the physical and cyber security of communications, energy and data infrastructure, and the security of technologies. The third concerns the security of technologies and the risk of losing advanced technologies, skills and knowledge. The fourth and final risk concerns the potential exploitation of economic dependence by third countries to influence the

political decisions of the Union or its Member States. These risks can be addressed at any point in the value chain, from basic research through to commercialisation and full-scale production.

This framework applies to Artificial Intelligence. The Commission deliberately identifies AI, alongside cutting-edge semiconductors, advanced quantum technologies and others, as dual-use technologies. Their proliferation may strengthen the military or intelligence capabilities of potentially hostile actors. For technological security, therefore, the ability to develop innovations is important, but so too is the ability to safeguard the outcomes of those innovations and to control the transfer of sensitive information. The strategy incorporates the need for continuous risk assessments, analysis of the potential exploitation of dependencies for geopolitical purposes and, in the most sensitive cases, of other transformative technologies and civil-military dual-use technologies, as well as potential technologies that undermine security and fundamental rights.

The European Economic Security Strategy organises the Union's response into three interconnected lines of action: promoting, protecting and collaborating. The first of these involves improving Europe's competitiveness, research and industrial base; the second aims to protect the Union through specifically targeted instruments that address economic and technological risks; the third pillar involves partnerships with reliable states to diversify supply chains and support an open international economic system. From this perspective, the single market is the EU's key asset, but it is also a means of securing supplies, channelling investment and strengthening Europe's capacity to develop strategic technologies, as well as promoting the adoption of standards (as seen in the 'Brussels Effect'). The strategy refers to the European Chips Act, industrial alliances and other instruments.

Concepts such as 'digital sovereignty' and 'strategic autonomy' highlight how the EU is seeking to balance its dual nature through its traditional regulatory capacity alongside a strategy aimed at strengthening its technological and industrial resilience.

Whilst the Brussels Effect demonstrates the EU's ability to export standards, competition in the AI sector has highlighted that regulation alone is not sufficient to guarantee competitiveness and security. In this context, it is worth mentioning the AI Act, through which the EU is seeking to establish a genuine governance model for AI.

The most recent phase of this debate has moved in the opposite direction, and it is here that the work of Alberto Alemanno is most useful. Alemanno reads the simplification agenda pursued

by the Commission from 2025 onwards as a deregulatory turn rather than a technical exercise, arguing in *The Dark Side of EU Deregulation* that the Union risks dismantling the very regulatory model that gave it international standing⁵⁸. Together with other legal scholars he has gone further, maintaining that parts of the omnibus programme are difficult to reconcile with the Union's own constitutional and better-regulation commitments⁵⁹. Read alongside Majone, Alemanno's intervention makes the trajectory of this chapter clear. The Union built its external influence on regulation because it had little else to build it on, and it is now being asked, mainly by industry and by the United States, to loosen the one instrument through which it exercises global influence. The AI Act, examined in the next section, sits precisely at this point of tension.

2.2 The AI Act: Structure and Political Logic

The AI Act, formally Regulation (EU) 2024/1689,⁶⁰ is a pioneering piece of legislation adopted by the European Parliament together with the Council, which entered into force on 1 August 2024, to regulate artificial intelligence across the member states. It represents a milestone in AI regulation, intended to create a safe environment consistent with the Union's values,⁶¹ for technological development within the member states.

The distinctive feature of this regulation lies in the fact that it is the first legal framework on AI in the world, and its peculiarity also lies in the fact that its approach is not merely normative, because it is not a regulation solely dedicated to AI, but follows a proportionate, risk-based approach: the greater the risk of causing harm to society, the stricter the rules.⁶²

It is a system in which obligations apply to multiple types of algorithms and sectors, all in line with safeguarding health, safety and fundamental rights; behind this regulatory instrument lies the logic pursued by the EU, namely to calibrate intervention in proportion to potential harm,

⁵⁸ Alemanno, A., (2025). "*The Dark Side of EU Deregulation*", *Project Syndicate*, February 2025 [online] Available at: <https://albertoalemanno.com/europe/the-dark-side-of-eu-deregulation/>.

⁵⁹ Alemanno, A., (2025). "*Is the Digital Omnibus Lawful?*", HEC Paris Research Paper No. 1588 [online] Available at: <https://ideas.repec.org/p/ebg/heccah/1588.html>; see also *EUobserver*, (2025). "*Deregulation plans break EU law, legal scholars warn*", 10 November 2025 [online] Available at: <https://euobserver.com/51992/deregulation-plans-break-eu-law-legal-scholars-warn/>.

⁶⁰ European Commission (2025). *AI Act*. [online] European Commission. Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

⁶¹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, OJ L, 12.7.2024.

⁶² Consilium. (2024). *Regolamento sull'intelligenza artificiale (IA): il Consiglio dà il via libera definitivo alle prime regole per l'IA al mondo*. [online] Available at: <https://www.consilium.europa.eu/it/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/>.

without having to govern innovation from above, just as the EU had already done in the past with the GDPR, of which the AI Act is the heir.

Before examining the structure of the Regulation in detail, it is worth noting that the AI Act has generated an unusually wide scholarly debate, and that this debate has been divided from the outset. On the supportive side, Luciano Floridi concluded in an early philosophical assessment that ‘the underlying philosophy is commendable, despite some limitations’ and that the text is ‘a good starting point to ensure that the development of AI in the EU is ethically sound, legally acceptable, socially equitable, and environmentally sustainable’⁶³. Gabriele Mazzini, who led the legal drafting of the proposal within the Commission, has defended it as ‘a horizontal legal instrument that aims to regulate, according to a tailored risk-based approach, the development and use of AI systems across a plurality of sectors’⁶⁴, and Nathalie Smuha has argued that regulation can itself be a competitive asset, since ‘besides minimising risks, such regulation could facilitate AI’s uptake, boost legal certainty, and hence also contribute to advancing countries’ position in the race’⁶⁵. Anu Bradford has made the same point in more general terms, showing that ‘lenient tech regulation is not necessary for the development of a thriving tech sector’ and that the supposed trade-off between regulation and innovation is a false choice⁶⁶. On the critical side, Michael Veale and Frederik Zuiderveen Borgesius accept that ‘different rules for different risk-levels of AI, make sense’ but warn that ‘some provisions of the Draft AI Act have surprising legal implications, whilst others may be largely ineffective at achieving their stated goals’, and observe that ‘standardisation is arguably where the real rule-making in the Draft AI Act will occur’⁶⁷. Nathalie Smuha and her co-authors, while welcoming the initiative in principle, concluded that ‘as currently drafted, the Proposal does not provide adequate fundamental rights protection, nor does it provide sufficient protection to

⁶³ Floridi, L., (2021). “*The European Legislation on AI: a Brief Analysis of its Philosophical Approach*”, *Philosophy & Technology*, 34(2), pp. 215-222 [online] Available at: <https://pmc.ncbi.nlm.nih.gov/articles/PMC8174763/>.

⁶⁴ Mazzini, G. & Bagni, F., (2023). “*Considerations on the regulation of AI systems in the financial sector by the AI Act*”, *Frontiers in Artificial Intelligence*, 6, art. 1277544 [online] Available at: <https://pmc.ncbi.nlm.nih.gov/articles/PMC10676199/>.

⁶⁵ Smuha, N. A., (2021). “*From a ‘race to AI’ to a ‘race to AI regulation’: regulatory competition for artificial intelligence*”, *Law, Innovation and Technology*, 13(1), pp. 57-84 [online] Available at: <https://www.tandfonline.com/doi/full/10.1080/17579961.2021.1898300>.

⁶⁶ Bradford, A., (2024). “*The False Choice Between Digital Regulation and Innovation*”, *Northwestern University Law Review*, 119(2), p. 377, at p. 382 [online] Available at: <https://scholarlycommons.law.northwestern.edu/nulr/vol119/iss2/3/>.

⁶⁷ Veale, M. & Zuiderveen Borgesius, F., (2021). “*Demystifying the Draft EU Artificial Intelligence Act*”, *Computer Law Review International*, 22(4), pp. 97-112 [online] Available at: <https://arxiv.org/abs/2107.03721>.

maintain the rule of law and democracy, and thus fails to secure Legally Trustworthy AI’⁶⁸. Marco Almada and Nicolas Petit describe the Regulation as ‘a legal medley’ that combines product safety and fundamental rights protection and identify ‘a mismatch between means and ends in the AI Act’, since ‘the Act aims to achieve a fundamental rights protection end by recourse to product safety means’⁶⁹. Johann Laux, Sandra Wachter and Brent Mittelstadt add a conceptual objection, arguing that ‘the EU adopted a simplistic conceptualization of trust and is overselling its regulatory ambition’ and that the Act ‘suggests an unfounded bright-line distinction between acceptable and unacceptable risks’⁷⁰, while Francesca Palmiotto shows that the trilogue produced ‘a deeply uncertain formulation of Article 6 and a worrisome delegation of powers to providers’, together with different standards ‘in the fields of law enforcement and migration’⁷¹. This division matters for the present analysis, because the two sides are not really disagreeing about the same thing: the supportive literature evaluates the Act as a normative and reputational achievement, whereas the critical literature evaluates it as an enforcement mechanism. The reading proposed here follows the second question while accepting the first, and the sections that follow examine the Regulation’s architecture with this distinction in mind.

⁶⁸ Smuha, N. A., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R. & Yeung, K., (2021). “*How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission’s Proposal for an Artificial Intelligence Act*”, LEADS Lab, University of Birmingham, 5 August 2021 [online] Available at: https://strathprints.strath.ac.uk/85567/1/Smuha_etal_SSRN_2021_How_the_EU_can_achieve_legally_trustworthy_AI.pdf.

⁶⁹ Almada, M. & Petit, N., (2023). “*The EU AI Act: A Medley of Product Safety and Fundamental Rights?*”, RSC Working Paper 2023/59, European University Institute, pp. 1-3 [online] Available at: https://cadmus.eui.eu/bitstream/handle/1814/75982/RSC_WP_2023_59.pdf; published as Almada, M. & Petit, N., (2025). “*The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights*”, *Common Market Law Review*, 62, pp. 85-120.

⁷⁰ Laux, J., Wachter, S. & Mittelstadt, B., (2024). “*Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk*”, *Regulation & Governance*, 18(1) [online] Available at: <https://onlinelibrary.wiley.com/doi/10.1111/rego.12512>.

⁷¹ Palmiotto, F., (2025). “*The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation*”, *European Journal of Risk Regulation*, 16, pp. 770-793 [online] Available at: <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/ai-act-roller-coaster-the-evolution-of-fundamental-rights-protection-in-the-legislative-process-and-the-future-of-the-regulation/5B512DDF859B55D549A7F5D21792AD73>.

The AI Act defines four levels of risk for AI systems:

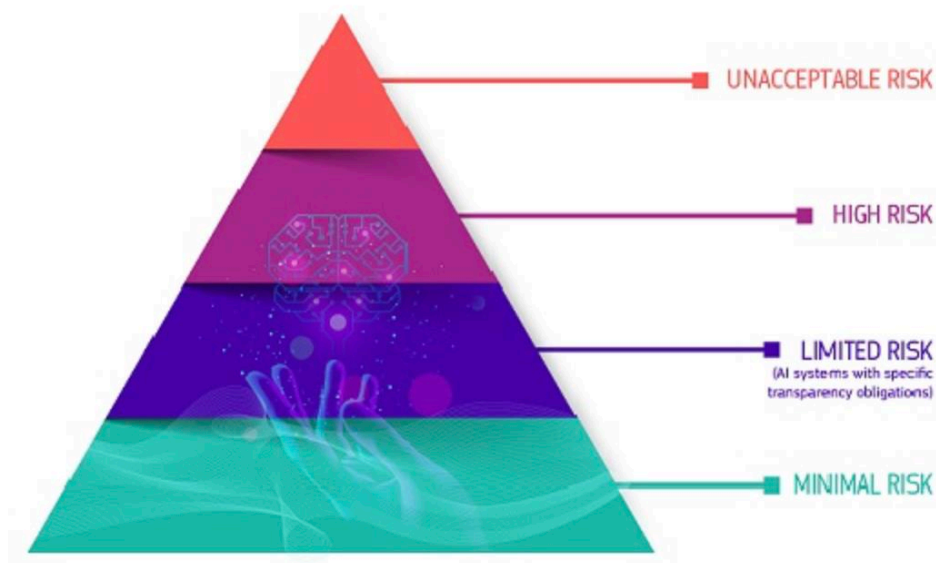


Figure 1 - The four risk levels for AI systems under Regulation (EU) 2024/1689. Source: European Commission, 'AI Act', Shaping Europe's Digital Future, available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

Unacceptable risk⁷²

All AI systems considered a clear threat to the safety, livelihoods and rights of people are banned. The AI Act prohibits eight practices, namely:

1. harmful AI-based manipulation and deception
2. harmful AI-based exploitation of vulnerabilities
3. social scoring
4. individual criminal offence risk assessment or prediction
5. untargeted scraping of the internet or CCTV material to create or expand facial recognition databases
6. emotion recognition in workplaces and education institutions

⁷² Shaping Europe's digital future. (2025). *AI Act*. [online] Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai#1720699867912-0>.

7. biometric categorisation to deduce certain protected characteristics

8. real-time remote biometric identification for law enforcement purposes in publicly accessible spaces

These systems are classified as unacceptable because they directly undermine the Union's values, and there is a thin but essential line that must clearly delineate the protection of fundamental rights from innovation. These prohibitions became applicable from 2 February 2025, marking the EU's determination both internally and externally, wishing to make clear that certain uses of AI cannot be negotiable, regardless of the benefits they might generate.

High-risk systems

Article 6 establishes high-risk systems, namely AI systems that could cause significant harm in the event of malfunction; these are permitted systems but subject to stringent obligations, such as conformity assessments or tests and the obligation to adopt safety measures.

The Act divides these into Annex I, which covers AI embedded in products already regulated by EU safety legislation (such as vehicles, medical devices and machinery), and Annex III, which identifies eight domains: biometric identification, management of critical infrastructure, vocational training, workforce and employment management, access to essential public and private services (including credit assessment and insurance), law enforcement, migration and border control, and judicial and administrative systems. These systems require thorough risk management, high-quality and well-documented training data, automatic logging and human oversight, as well as a market conformity assessment and registration in a public EU database for most Annex III systems.

In this context, the AI Act does *not block* the use of AI, but imposes extremely strict requirements on risk management, data quality, documentation, human oversight, transparency and compliance. It is worth quoting these requirements in the words of the Regulation itself, because their wording determines how demanding they actually are. Article 9(1) provides that ‘a risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems’, and Article 9(2) specifies that this system ‘shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating’, beginning with ‘the identification and analysis of the known and the reasonably foreseeable risks that the high-risk

AI system can pose to health, safety or fundamental rights’⁷³. On data quality, Article 10(3) requires that ‘training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose’⁷⁴. On transparency towards professional users, Article 13(1) provides that high-risk systems ‘shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system’s output and use it appropriately’⁷⁵. On human oversight, Article 14(1) requires that such systems be designed ‘including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use’, and Article 14(4) specifies that the persons assigned to oversight must be enabled ‘to remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (automation bias)’ and ‘to decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output’⁷⁶. Finally, Article 15(1) requires that high-risk systems ‘achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle’⁷⁷. Read together, these provisions confirm that the EU has a right to innovation but chooses to steer that innovation in line with its own principles. Two features of the drafting are worth noting. First, the obligations are procedural rather than substantive: the Regulation does not say which level of residual risk is acceptable, but requires that risk be identified, documented and managed, so that the decisive judgements are left to providers and to the harmonised standards that will operationalise these articles. Second, the language of ‘appropriate’ and ‘to the best extent possible’ builds flexibility into requirements that are often described as absolute. It is precisely this balancing act, between protecting fundamental rights and preserving the conditions for technological development, that runs through the rest of the Regulation’s

⁷³ Regulation (EU) 2024/1689, Article 9(1) and 9(2), official consolidated text reproduced in *artificialintelligenceact.eu*, “Article 9(1) and 9(2)” [online] Available at: <https://artificialintelligenceact.eu/article/9/>.

⁷⁴ Regulation (EU) 2024/1689, Article 10(3), official consolidated text reproduced in *artificialintelligenceact.eu*, “Article 10(3)” [online] Available at: <https://artificialintelligenceact.eu/article/10/>.

⁷⁵ Regulation (EU) 2024/1689, Article 13(1), official consolidated text reproduced in *artificialintelligenceact.eu*, “Article 13(1)” [online] Available at: <https://artificialintelligenceact.eu/article/13/>.

⁷⁶ Regulation (EU) 2024/1689, Article 14(1) and 14(4), official consolidated text reproduced in *artificialintelligenceact.eu*, “Article 14(1) and 14(4)” [online] Available at: <https://artificialintelligenceact.eu/article/14/>.

⁷⁷ Regulation (EU) 2024/1689, Article 15(1), official consolidated text reproduced in *artificialintelligenceact.eu*, “Article 15(1)” [online] Available at: <https://artificialintelligenceact.eu/article/15/>.

architecture, and that becomes even clearer once the lighter-touch obligations applying to limited-risk and minimal-risk systems are taken into account.

Besides the prohibitions and obligations already discussed, the AI Act completes its risk-based structure with two further, lighter tiers that still matter for understanding the Regulation's political logic: the limited-risk category, which is subject to specific transparency obligations, and the minimal-risk category, which is left essentially to voluntary self-regulation. These two lower tiers are not there by accident. They show that the EU legislator did not want to adopt the same precautionary approach for every kind of artificial intelligence; instead, it chose to concentrate its regulatory effort where the risk of harm to people and to democratic processes is highest, while leaving most everyday AI applications largely free from obligations. This choice is, in a way, also a political statement, since it signals that Brussels wants to be seen as supporting innovation and not simply restricting it, even while using the same instrument to spread a normative model of 'trustworthy AI' beyond its own borders.

Article 50 of the Regulation is the core of this limited-risk regime, and it sets out a series of transparency duties for providers and deployers of specific categories of systems. The first obligation concerns AI systems that are designed to interact directly with people: providers have to make sure these systems are built so that the people involved are told they are interacting with an artificial agent, 'unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect'⁷⁸. This is basically the chatbot-disclosure obligation, and the way it is drafted says something interesting: the legislator did not impose an absolute duty to disclose, but built in an exception based on how perceptive an ordinary user would reasonably be, which balances user protection against the practical cost of labelling literally everything.

A second, closely related obligation, set out in Article 50(2), requires providers of AI systems, including general-purpose AI systems, that generate synthetic audio, image, video or text content to make sure such outputs are marked in a machine-readable format and can be detected as artificially generated or manipulated⁷⁹. There is an exemption for systems that only perform an assistive function for standard editing, which shows that the legislator wanted to distinguish between AI used as a proper creative or generative tool and AI used simply as a support within

⁷⁸ Regulation (EU) 2024/1689, Article 50, summarized in (n.d.). *artificialintelligenceact.eu*, "Article 50: Transparency Obligations for Providers and Deployers of Certain AI Systems." [online] Available at: <https://artificialintelligenceact.eu/article/50/>.

⁷⁹ Ibid., Article 50(2).

an otherwise human-made production process. This provision seems to anticipate how difficult it is becoming to tell authentic from synthetic content in the public sphere, and it places the EU's regulatory intervention right inside the wider contest over information integrity that increasingly characterises geopolitical competition in the digital domain.

Article 50(3) covers a narrower but more sensitive category: deployers of emotion-recognition or biometric-categorisation systems have to inform the people exposed to such systems that they are operating, while processing any personal data in line with the General Data Protection Regulation, the equivalent regulation that applies to the EU institutions, and the Law Enforcement Directive⁸⁰. The last, and probably most politically sensitive, transparency duty concerns deepfakes: Article 50(4) requires deployers who generate or manipulate image, audio or video content amounting to a deepfake to disclose that the content has been artificially generated or manipulated, although works that are 'evidently artistic, creative, satirical, fictional or analogous' only need to mention the existence of such content in a way that does not get in the way of its display or enjoyment⁸¹. A similar duty, under the second subparagraph of Article 50(4), applies to text published to inform the public on matters of public interest, which must be disclosed as AI-generated unless it has gone through human review and a natural or legal person takes editorial responsibility for its publication⁸². Put together, these rules on deepfakes and AI-generated text place the AI Act right at the intersection between technology regulation and the protection of democratic debate, which matters directly for the EU's claim to project not just economic but also normative power internationally.

How these duties actually work in practice depends mostly on timing and on co-regulatory instruments. The Regulation itself fixes the moment at which the information has to reach the person concerned, since Article 50(5) requires that it be provided 'in a clear and distinguishable manner at the latest at the time of the first interaction or exposure'⁸³. This is a precise obligation as to when, but a very open one as to how, and it therefore leaves providers a considerable margin of interpretation. The same article then hands much of the technical detail to soft law: under Article 50(7) the AI Office is to encourage and facilitate the drawing up of codes of practice at Union level to support the obligations on detection and labelling of artificially generated content, while the Commission retains the power to approve those codes by

⁸⁰ Ibid., Article 50(3).

⁸¹ Ibid., Article 50(4).

⁸² Ibid., Article 50(4), second subparagraph.

⁸³ Ibid., Article 50(5).

implementing act⁸⁴. That is exactly what has happened. On 8 May 2026 the Commission published three studies on the technical solutions available to mark and detect AI-generated content, and on 9 July 2026 it issued its opinion assessing the Code of Practice on Transparency of AI-generated content⁸⁵. The order of these steps is telling: first the technical studies, then the code, then the formal assessment. In other words, a broadly worded legal duty is being turned into workable technical practice only gradually, and by instruments that are not themselves legislative. For the argument of this thesis this matters, because it shows that the effectiveness of the transparency regime does not depend on the strength of the text adopted in 2024 but on administrative work carried out years later, and this is the same gap between ambition and capacity that the next sections examine in the case of national authorities.

Below the limited-risk tier there is the residual category of minimal-risk AI, which the Regulation treats as the default classification for any system that does not fit the criteria of the three higher tiers. This category carries no mandatory requirements at all, and the Regulation addresses it only through voluntary instruments: Article 95(1) provides that ‘the AI Office and the Member States shall encourage and facilitate the drawing up of codes of conduct, including related governance mechanisms, intended to foster the voluntary application to AI systems, other than high-risk AI systems, of some or all of the requirements set out in Chapter III, Section 2’⁸⁶. Article 95(2) adds that such codes may cover objectives such as ‘assessing and minimising the impact of AI systems on environmental sustainability’, ‘promoting AI literacy’ and ‘assessing and preventing the negative impact of AI systems on vulnerable persons or groups of vulnerable persons’⁸⁷. The Commission, for its part, states plainly that ‘the vast majority of AI systems currently used in the EU fall into this category’ of minimal or no risk, listing applications such as spam filters and recommender systems⁸⁸. This shows something important: even though the AI Act has a reputation as a very strict, maximalist piece of regulation, in practice it reserves binding legal force for a fairly narrow set of applications and leaves most of the AI economy free of statutory constraints. This asymmetry supports the idea that the Regulation should not be read as a blanket form of control, but rather as a way of intervening selectively and in proportion to risk, protecting specific public goods such as safety,

⁸⁴ Ibid., Article 50(7).

⁸⁵ European Commission, (2026). “*AI Act*”, Shaping Europe’s Digital Future [online] Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

⁸⁶ Regulation (EU) 2024/1689, Article 95(1), official consolidated text reproduced in *artificialintelligenceact.eu*, “Article 95(1)” [online] Available at: <https://artificialintelligenceact.eu/article/95/>.

⁸⁷ Ibid., Article 95(2).

⁸⁸ European Commission, (2026). “*AI Act*”, Shaping Europe’s Digital Future [online] Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

non-discrimination and fundamental rights, without imposing a general licensing regime on the technology as a whole.

General-Purpose AI: A Late but Decisive Addition

The AI Act's treatment of general-purpose AI (GPAI) models, set out in Chapter V (Articles 51-56), is one of the most important and most debated additions made during the legislative process. The original Commission proposal, drafted before the rapid spread of large foundation models, did not anticipate systems whose capabilities could not be neatly assigned to a single risk tier defined by intended use; the arrival of models such as GPT-4 and its successors forced the co-legislators to design, in a relatively short time, a dedicated regulatory track for AI systems whose defining feature is precisely their generality⁸⁹. This late but decisive addition is itself a sign of the AI Act's hybrid nature: a legislative process that started out to regulate discrete, purpose-bound applications was forced, halfway through, to deal with a class of technologies whose risks are diffuse, cumulative and often only visible once the model is embedded in a downstream application.

The obligations on GPAI providers became applicable on 2 August 2025, twelve months after the Regulation's entry into force and therefore earlier than the deadline set for high-risk systems, while providers of models already placed on the market before that date have until 2 August 2027 to comply⁹⁰. The baseline duties are set out in Article 53(1), which requires providers to 'draw up and keep up-to-date the technical documentation of the model, including its training and testing process and the results of its evaluation', to 'put in place a policy to comply with Union law on copyright and related rights' and to 'draw up and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office'⁹¹. Article 53(2) then exempts models 'released under a free and open-source licence' from the documentation duties, while making clear that 'this exception shall not apply to general-purpose AI models with systemic risks'⁹². The threshold for that category is quantitative: under Article 51(2) a model

⁸⁹ European Commission, (2026). "*General-Purpose AI Models in the AI Act*", Shaping Europe's Digital Future [online] Available at: <https://digital-strategy.ec.europa.eu/en/policies/ai-act-general-purpose-ai>.

⁹⁰ Regulation (EU) 2024/1689, Article 111(3) and Article 113 [online] Available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>; see also European Commission, (2026). "*General-Purpose AI Models in the AI Act*" [online] Available at: <https://digital-strategy.ec.europa.eu/en/policies/ai-act-general-purpose-ai>.

⁹¹ Regulation (EU) 2024/1689, Article 53(1), official consolidated text reproduced in *artificialintelligenceact.eu*, "Article 53(1)" [online] Available at: <https://artificialintelligenceact.eu/article/53/>.

⁹² *Ibid.*, Article 53(2).

‘shall be presumed to have high impact capabilities’ when ‘the cumulative amount of computation used for its training measured in floating point operations is greater than 10^{25} ’⁹³. Choosing a computational-power threshold, rather than a qualitative or sector-based criterion, is worth noting: it makes the systemic-risk category more legally predictable and less open to case-by-case negotiation, but it also ties the scope of EU regulatory reach to a metric, training compute, over which the Union currently has very limited industrial control, a tension explored further in Chapter III.

For models that cross that threshold, Article 55(1) imposes four additional duties, and here too the wording repays attention. Providers must ‘perform model evaluation in accordance with standardised protocols and tools reflecting the state of the art, including conducting and documenting adversarial testing of the model with a view to identifying and mitigating systemic risks’, ‘assess and mitigate possible systemic risks at Union level’, ‘keep track of, document, and report, without undue delay, to the AI Office and, as appropriate, to national competent authorities, relevant information about serious incidents and possible corrective measures to address them’, and ‘ensure an adequate level of cybersecurity protection for the general-purpose AI model with systemic risk and the physical infrastructure of the model’⁹⁴. Supervision of these duties is centralised in the AI Office within the Commission, and Article 101(1) allows the Commission to impose fines on GPAI providers ‘not exceeding 3 % of their annual total worldwide turnover in the preceding financial year or EUR 15 000 000, whichever is higher’⁹⁵. Centralising GPAI enforcement in a single Union-level body, rather than in the twenty-seven national competent authorities responsible for most other aspects of the Act, is a deliberate institutional choice: it recognises that foundation models are usually developed and deployed across borders by a small number of firms, and that fragmented national oversight would risk both regulatory arbitrage and duplicated compliance burdens.

A large part of the practical detail governing GPAI compliance has, in fact, been left to a co-regulatory instrument rather than to binding statutory text, and the Regulation says so openly: under Article 55(2) providers ‘may rely on codes of practice within the meaning of Article 56 to demonstrate compliance with the obligations set out in paragraph 1 of this Article, until a

⁹³ Regulation (EU) 2024/1689, Article 51(2), official consolidated text reproduced in *artificialintelligenceact.eu*, “Article 51(2)” [online] Available at: <https://artificialintelligenceact.eu/article/51/>.

⁹⁴ Regulation (EU) 2024/1689, Article 55(1), official consolidated text reproduced in *artificialintelligenceact.eu*, “Article 55(1)” [online] Available at: <https://artificialintelligenceact.eu/article/55/>.

⁹⁵ Regulation (EU) 2024/1689, Article 101(1) [online] Available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.

harmonised standard is published’, and those who do not adhere to an approved code ‘shall demonstrate alternative adequate means of compliance for assessment by the Commission’⁹⁶. The instrument in question is the General-Purpose AI Code of Practice, published on 10 July 2025. The Commission describes it as ‘a voluntary tool, prepared by independent experts in a multi-stakeholder process, designed to help industry comply with the AI Act’s obligations for providers of general-purpose AI models’, and states that ‘the Commission and the AI Board have confirmed that the code is an adequate voluntary tool for providers of GPAI models to demonstrate compliance with the AI Act’⁹⁷. The Code ‘consist[s] of three separately authored chapters: Transparency, Copyright, and Safety and Security’. According to the Commission, ‘the Chapters on Transparency and Copyright offer all providers of general-purpose AI models a way to demonstrate compliance with their obligations under Article 53 AI Act’, the Transparency chapter doing so through ‘a user-friendly Model Documentation Form’, while the Copyright chapter ‘offers providers practical solutions to meet the AI Act’s obligation to put in place a policy to comply with EU copyright law’⁹⁸. The third chapter is deliberately narrow in scope: it ‘is only relevant to the small number of providers of the most advanced models, those that are subject to the AI Act’s obligations for providers of general-purpose AI models with systemic risk under Article 55 AI Act’, and it ‘outlines concrete state-of-the-art practices for managing systemic risks’⁹⁹. The incentive to sign is stated equally openly, since adherence ‘will reduce their administrative burden and give them more legal certainty and trust than if they proved compliance through other methods’¹⁰⁰. This reliance on a voluntary code to put a statutory obligation into practice is a good example of a recurring feature of the AI Act’s governance model: binding legislative text sets the outer boundaries of the obligation, while the actual content of compliance is negotiated, in real time, between regulators and industry through soft-law instruments. This gives flexibility, but it also brings a certain risk of regulatory capture, something critics of the Act’s implementation have not failed to note.

Governance: Ambition Meets Administrative Capacity

⁹⁶ Regulation (EU) 2024/1689, Article 55(2), official consolidated text reproduced in *artificialintelligenceact.eu*, “Article 55(2)” [online] Available at: <https://artificialintelligenceact.eu/article/55/>.

⁹⁷ European Commission, (2026). “*The General-Purpose AI Code of Practice*”, Shaping Europe’s Digital Future [online] Available at: <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>.

⁹⁸ Ibid.

⁹⁹ Ibid.

¹⁰⁰ Ibid.

The AI Act's institutional architecture is formally distributed across the European AI Office and the authorities of the Member States, which are responsible for implementing, supervising and enforcing the Regulation, while the AI Board, the Scientific Panel and the Advisory Forum steer and advise the Act's broader governance¹⁰¹. Once an AI system enters the market, this multi-level structure allocates distinct functions to distinct actors: market surveillance authorities conduct market surveillance, deployers ensure human oversight and monitoring, providers maintain post-market monitoring systems, and providers and deployers alike bear responsibility for reporting serious incidents and malfunctions¹⁰². Under the amendments introduced through the AI omnibus simplification package, the Commission has further proposed to reinforce the AI Office's powers and to centralise oversight of AI systems built on general-purpose AI models, explicitly in order to reduce governance fragmentation¹⁰³.

This carefully layered institutional design, however, has run into a persistent and well-documented implementation gap at national level. The obligation is clear enough in the Regulation: 'Member States were required to designate their competent authorities and single points of contact by 2 August 2025', and the AI Act 'obliges Member States to designate two types of authority - at least one notifying authority and a market surveillance authority', the latter also acting as 'the single point of contact at national level'¹⁰⁴. Compliance with that obligation has been very uneven. Independent tracking of national implementation shows that nine Member States have designated both a market surveillance authority and a notifying authority, twelve offer only partial clarity, and six remain unclear¹⁰⁵. The European Parliament's own research service confirms the picture from the institutional side, noting that the Commission maintains a list of national single points of contact and that, 'as of March 2026, the list comprised eight single contact points, out of 27'¹⁰⁶. The consequence is drawn in the same document, which observes that 'researchers note that the decentralised pattern remains dominant in the AI Act, potentially leading to challenges around uneven enforcement

¹⁰¹ European Commission, (2026). "*AI Act*", Shaping Europe's Digital Future [online] Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

¹⁰² Ibid.

¹⁰³ Ibid.

¹⁰⁴ European Parliamentary Research Service, Marcelin, T., (2026). "*Enforcement of the AI Act*", PE 785.670, March 2026 [online] Available at: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/785670/EPRS_ATA\(2026\)785670_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/785670/EPRS_ATA(2026)785670_EN.pdf).

¹⁰⁵ (2026). "*Overview of all AI Act National Implementation Plans*", *artificialintelligenceact.eu* [online] Available at: <https://artificialintelligenceact.eu/national-implementation-plans/>.

¹⁰⁶ European Parliamentary Research Service, Marcelin, T., (2026). "*Enforcement of the AI Act*", PE 785.670, March 2026 [online] Available at: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/785670/EPRS_ATA\(2026\)785670_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/785670/EPRS_ATA(2026)785670_EN.pdf).

in the EU'¹⁰⁷. The Commission's own consultations on the digital omnibus reached a similar conclusion, highlighting 'critical bottlenecks, including delays in designating national competent authorities and conformity assessment bodies, and the absence of harmonised standards, guidance and compliance tools for high-risk AI requirements'¹⁰⁸.

It is worth explaining what this implementation gap actually consists of, because the expression is often used loosely. The gap is not that Member States disagree with the Regulation, nor that they have refused to apply it. It is that the AI Act, like most instruments of EU product legislation, is written on the assumption that each Member State already possesses, or can rapidly create, an administrative body with the technical competence to assess artificial intelligence systems, and that assumption has turned out to be optimistic. Designating a market surveillance authority on paper is a legal act; equipping it with engineers able to audit a risk management system, evaluate training data or test a model for robustness is a budgetary and labour-market problem, and it is at this second stage that most Member States have stalled. The result is a Regulation that is formally in force everywhere and effectively enforced almost nowhere, with the further consequence that the substantive content of compliance is settled by harmonised standards and codes of practice rather than by public authorities applying the text. This is why the delay matters analytically and not only administratively.

These figures are not just administrative details; they support a broader claim that runs through the rest of this thesis. The AI Act was conceived, and is often presented in EU discourse, as an instrument of geopolitical ambition, a regulatory template capable of shaping global standards for artificial intelligence. Yet the very Member States responsible for enforcing it have, in most cases, been unable to complete even the preliminary institutional steps set out in the Regulation's own timetable. This is a capacity gap that really matters: a regulatory instrument whose credibility abroad depends, to a large extent, on evidence of effective enforcement at home cannot keep a reputation for stringency indefinitely if implementation keeps lagging behind legislative ambition. The tension between the EU's wish to project regulatory power internationally and its demonstrated difficulty in mobilising the administrative resources of twenty-seven Member States at once is, in this sense, a microcosm of the broader argument developed in Chapter III: that the EU's capacity to turn normative ambition into geopolitical

¹⁰⁷ Ibid.

¹⁰⁸ European Parliamentary Research Service, Niestadt, M., (2026). "*Digital Omnibus on AI*", PE 782.651, June 2026 [online] Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/782651/EPRS_BRI\(2026\)782651_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/782651/EPRS_BRI(2026)782651_EN.pdf).

weight is structurally limited by implementation and enforcement capacity, not just by how the rules are designed.

The governance framework is not limited to compliance monitoring; it also extends into the EU's wider security posture. The European Union Agency for Cybersecurity (ENISA), together with the Commission, is tasked with creating a blueprint to secure access to advanced AI systems for cybersecurity purposes, as part of the July 2026 EU Action Plan on Cybersecurity and Artificial Intelligence¹⁰⁹, an initiative that signals the Commission's intention to fold AI governance into its broader cybersecurity strategy rather than treating the two domains separately, a link that is examined further in section 2.3 below.

Implementation Timeline: A Staggered and Politically Contested Calendar

The AI Act's entry into force did not trigger the simultaneous application of all its provisions; rather, the Regulation establishes a staggered timeline that phases obligations in according to their perceived urgency and complexity. The Regulation entered into force on 1 August 2024¹¹⁰; prohibited AI practices and AI-literacy obligations became applicable on 2 February 2025¹¹¹; governance rules and GPAI model obligations became applicable on 2 August 2025¹¹²; and the Regulation was originally scheduled to become fully applicable, including transparency rules and high-risk system obligations, on 2 August 2026, two years after entry into force¹¹³. A further set of rules, applicable from 2 December 2027, governs AI systems used in specific high-risk areas such as biometrics, critical infrastructure, education, employment, migration, asylum and border control¹¹⁴, while rules for high-risk AI systems embedded in regulated products such as lifts and toys, originally due on 2 August 2026, were extended to 2 August 2028 following the AI omnibus political agreement¹¹⁵. The Commission has additionally announced plans to launch a 2026 call to increase the EU's evaluation capacity for AI models prior to market placement, expected to become operational by 2027¹¹⁶.

¹⁰⁹ European Commission, (2026). "AI Act", Shaping Europe's Digital Future [online] Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

¹¹⁰ Ibid.

¹¹¹ Ibid.

¹¹² Ibid.

¹¹³ Ibid.

¹¹⁴ Ibid.

¹¹⁵ Ibid.

¹¹⁶ Ibid.

The most consequential recent modification to this calendar arrived through the Digital Omnibus package, adopted by the Commission on 19 November 2025, which included an ‘AI omnibus’ legislative proposal described officially as introducing ‘targeted simplification measures to ensure timely, smooth, and proportionate implementation of certain of the AI Act’s provisions’¹¹⁷. The Commission’s own communications framed the package as business-friendly: companies would only have to apply the rules for high-risk AI systems once the necessary support tools and standards were in place, granting them up to sixteen months of additional time to comply, alongside simpler rules, opportunities for real-world testing, and centralised oversight¹¹⁸. A political agreement on the AI omnibus was subsequently reached on 7 May 2026, establishing a clear implementation timeline for high-risk AI rules, including the extension of the transition period for high-risk systems embedded in regulated products to 2 August 2028¹¹⁹. Substantively, the omnibus introduces a new prohibition on AI systems generating non-consensual sexually explicit or intimate content, including so-called ‘nudification’ applications and material amounting to child sexual abuse material, reinforces the AI Office’s powers and centralises oversight of GPAI-based systems, extends simplified SME-style documentation requirements to small mid-cap companies, broadens access to regulatory sandboxes including a new EU-level sandbox, and clarifies the interplay between the AI Act and EU product-safety law, notably the Machinery Regulation, to avoid duplication¹²⁰. Parliament adopted the agreed text in its June 2026 plenary session, and the final compromise set ‘fixed deadlines for the delayed application of high-risk AI rules: 2 December 2027 for stand-alone high-risk AI systems, and 2 August 2028 for high-risk AI systems embedded in products’¹²¹.

This simplification drive has not gone uncontested. On 13 November 2025, 133 civil society organisations and trade unions signed a joint statement urging the Commission to ‘immediately halt any attempts to reopen the GDPR, ePrivacy framework, AI Act or other core digital rights protections’, describing the leaked Digital Omnibus proposals as ‘the biggest rollback of digital

¹¹⁷ European Commission, (2025). “*Digital Omnibus on AI Regulation Proposal*” [online] Available at: <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal>.

¹¹⁸ European Commission, (2025). “*Simpler digital rules to help EU businesses grow*” [online] Available at: https://commission.europa.eu/news-and-media/news/simpler-digital-rules-help-eu-businesses-grow-2025-11-19_en.

¹¹⁹ European Commission, (2026). “*AI Act*”, Shaping Europe’s Digital Future [online] Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

¹²⁰ Ibid.

¹²¹ European Parliamentary Research Service, Niestadt, M., (2026). “*Digital Omnibus on AI: Adoption in plenary*”, PE 789.329, June 2026 [online] Available at: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/789329/EPRS_ATA\(2026\)789329_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/789329/EPRS_ATA(2026)789329_EN.pdf).

fundamental rights in EU history’¹²². This civil-society critique echoes an earlier warning issued by Carnegie Endowment analyst Raluca Csernaton, who documented a broader deregulatory turn already under way by May 2025: ‘Enforcement of the Digital Services Act (DSA) is in limbo, the liability directive has been shelved, and new AI codes of practice focus more on help and support than on firm restraints’, a shift she warned ‘might erode the Brussels effect’¹²³.

Beyond civil-society advocacy, the AI Act has also attracted more structural scholarly critique of its underlying regulatory design. Bruegel’s policy brief argues that the Act, as an ex-ante product-safety regulation, does not really fit the nature of contemporary AI systems, which ‘operate in unknown environments and take actions that were unforeseen at the time of coding’, meaning that ‘an ex-ante regime cannot effectively safeguard against unforeseeable harm’; the brief concludes that the Act ‘is unlikely to protect against AI harm while minimising market distortion’ and notes that it remains ‘not complemented by an ad-hoc AI liability framework’¹²⁴. University of Turin legal scholar Ugo Pagallo offers a similar institutional critique, describing how the Act welds product-safety audits, fundamental-rights tests and voluntary codes into a single statute, producing a ‘patchwork effect’ that makes the law complex even for EU lawyers, let alone for foreign regulators trying to copy it¹²⁵. Both critiques come down to the same underlying point: the Act’s internal complexity and its uncertain fit with the genuinely adaptive, emergent nature of AI systems are not just technical drafting concerns, but factors that affect the Regulation’s external credibility and, by extension, its capacity to function as a genuine instrument of geopolitical projection, a question taken up more systematically in section 3.1.

The AI Act has not only been contested inside the Union. Since 2025 it has become an object of open hostility on the part of the United States, and this external pressure is now one of the main variables shaping the Regulation’s future. The direction was set at the Paris AI Action Summit of February 2025, where Vice-President JD Vance told his European hosts that

¹²² European Digital Rights (EDRi), (2025). “*Forthcoming Digital Omnibus would mark point of no return*” [online] Available at: <https://edri.org/our-work/forthcoming-digital-omnibus-would-mark-point-of-no-return/>.

¹²³ Carnegie Endowment for International Peace, Raluca Csernaton, (2025). “*The EU’s AI Power Play: Between Deregulation and Innovation*” [online] Available at: <https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation>.

¹²⁴ Bruegel, (2026). “*How to fix European Union artificial intelligence regulation*” [online] Available at: <https://www.bruegel.org/policy-brief/right-balance-how-fix-european-union-artificial-intelligence-regulation>.

¹²⁵ Ugo Pagallo, cited in CEPA, Anda Bologa, (2025). “*Burying the Brussels Effect? AI Act Inspires Few Copycats*” [online] Available at: <https://cepa.org/article/burying-the-brussels-effect-ai-act-inspires-few-copycats/>.

‘excessive regulation of the AI sector could kill a transformative industry just as it’s taking off’ and warned that the United States would not accept rules that discriminate against American firms¹²⁶. A few days earlier the White House had already issued a presidential memorandum on ‘Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties’, which treats foreign digital regulation as a form of extraction from American firms and directs the administration to respond¹²⁷. That response has taken concrete form. The President has repeatedly threatened additional tariffs against countries that impose digital taxes or digital rules on American technology companies¹²⁸, the administration has weighed sanctions and visa restrictions against officials involved in enforcing EU digital legislation¹²⁹, and the Office of the United States Trade Representative has listed the AI Act itself among the foreign trade barriers affecting American exporters in its 2026 National Trade Estimate Report¹³⁰. Analysts have started to describe this as a coherent strategy rather than a series of episodes: a Center for Strategic and International Studies assessment speaks of a new containment doctrine through which the United States uses trade instruments to stop digital regulation abroad¹³¹. The Union has so far defended its right to legislate, with Commissioner Henna Virkkunen and other officials repeating before the European Parliament that European digital rules are not negotiable in trade discussions¹³². This transatlantic conflict is directly relevant to the argument of this thesis. The AI Act was designed as an instrument of influence

¹²⁶ Reuters, (2025). “*Europe looks to embrace AI at Paris summit’s 2nd day while global consensus unclear*”, 11 February 2025 [online] Available at: <https://www.reuters.com/technology/artificial-intelligence/europe-looks-embrace-ai-paris-summits-2nd-day-while-global-consensus-unclear-2025-02-11/>; TechCrunch, (2025). “*In Paris, JD Vance skewers EU AI rules, lauds US tech supremacy*” [online] Available at: <https://techcrunch.com/2025/02/11/in-paris-jd-vance-skewers-eu-ai-rules-lauds-us-tech-supremacy/>.

¹²⁷ The White House, (2025). “*Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties*”, Presidential Memorandum, 21 February 2025 [online] Available at: <https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/>.

¹²⁸ Reuters, (2025). “*Trump threatens more tariffs on countries with digital taxes*”, 26 August 2025 [online] Available at: <https://www.reuters.com/world/us/trump-threatens-more-tariffs-countries-with-digital-taxes-2025-08-26/>; *The Guardian*, (2026). “*Trump threatens tariff on EU countries that impose digital tax*”, 27 June 2026 [online] Available at: <https://www.theguardian.com/us-news/2026/jun/27/trump-threatens-tariff-eu-countries-impose-digital-tax>.

¹²⁹ Reuters, (2025). “*Trump administration weighs sanctions on officials implementing EU tech law*”, 26 August 2025 [online] Available at: <https://www.reuters.com/world/us/trump-administration-weighs-sanctions-officials-implementing-eu-tech-law-sources-2025-08-26/>.

¹³⁰ Office of the United States Trade Representative, (2026). “*2026 National Trade Estimate Report on Foreign Trade Barriers*” [online] Available at: <https://ustr.gov/sites/default/files/files/Press/Releases/2026/National%20Trade%20Estimate%20Report%202026.pdf>.

¹³¹ Center for Strategic and International Studies, (2026). “*A New Containment Doctrine: How the United States Is Using Trade to Stop Digital Regulation*”, 6 May 2026 [online] Available at: <https://www.csis.org/analysis/new-containment-doctrine-how-united-states-using-trade-stop-digital-regulation>.

¹³² European Parliament, (2025). “*Verbatim report of proceedings*”, plenary sitting of 8 October 2025 [online] Available at: https://www.europarl.europa.eu/doceo/document/CRE-10-2025-10-08-ITM-011_EN.html.

that works through the size of the internal market rather than through coercion, and it is precisely that mechanism which the United States is now attacking with coercive instruments of its own. Regulatory power, in other words, is not costless: it invites retaliation from those whose firms bear the cost of compliance, and the simplification agenda examined above cannot be understood in isolation from this pressure.

Putting all this together, the transparency regime of Article 50, the residual minimal-risk category, the elaborate GPAI framework, the persistently uneven governance rollout, and the contested trajectory of the AI omnibus show the AI Act working on two distinct registers at once. On the technical register, the Regulation is a sophisticated exercise in risk classification, trying to calibrate legal obligation to the probability and severity of harm across an extraordinarily varied population of AI applications. On the political register, however, the Act cannot be separated from the EU's broader project of shaping global technology governance in its own image, of asserting regulatory leadership in the absence of comparable industrial or military weight, and of using legislative stringency as a substitute for capabilities the Union does not otherwise have. These two registers do not always sit comfortably together. The tension between innovation and protection, visible in the deliberate narrowing of binding obligations to the higher risk tiers, is mirrored by a second, arguably more consequential tension between regulatory ambition and enforcement capacity, made evident by the national implementation delays documented above and by the deregulatory pressures embodied in the Digital Omnibus. Both tensions point ahead to the analysis that follows: section 2.3 examines the specific strategic domains in which the EU tries to convert its regulatory apparatus into political leverage, while Chapter III asks directly whether an instrument so weighed down by internal contradiction can still generate durable geopolitical power.

2.3 Fields in Which the EU Uses AI as a Political Asset

While section 2.2 looked at the AI Act as a piece of legislative architecture, this section looks instead at the uses to which that architecture, and the broader apparatus of EU digital policy, are being put across different strategic domains. The claim made here is that artificial intelligence has stopped being, for the European Union, a purely sectoral policy concern confined to consumer protection or market regulation; it has instead become a cross-cutting instrument used across industrial policy, cybersecurity, defence, fundamental-rights protection, and external action. Each of these domains shows a different facet of the same underlying

strategy: turning regulatory and institutional capacity into a substitute, however imperfect, for the industrial and military capabilities the Union structurally lacks.

Industrial Policy

The EU's AI industrial policy is most visibly expressed through the AI Continent Action Plan and its associated investment architecture, an initiative that treats the accumulation of computational infrastructure as inseparable from the pursuit of regulatory sovereignty. The Commission's decision to pair the AI Act's legal framework with a parallel programme of public investment, built around the InvestAI initiative and the ambition to expand European data-centre and 'AI gigafactory' capacity, signals an implicit recognition that regulation alone cannot secure the EU's position in the global AI economy¹³³. This pairing looks deliberate: industrial policy is used not just to close a competitiveness gap for its own sake, but to give substance to the EU's regulatory claims, since a regulator with no domestic industry to speak of risks being dismissed internationally as a rule-taker rather than a rule-maker in the very sector it claims to govern.

The political character of this industrial policy is reinforced by its explicit framing in terms of external dependence. In October 2025, the Commission unveiled a further €1 billion 'Apply AI' funding package, sourced from the Horizon Europe and Digital Europe programmes and targeting sectors including healthcare, energy, mobility, pharmaceuticals, construction, agri-food, defence, communications and culture, explicitly described as aimed at 'enhancing the deployment of artificial intelligence across essential sectors' in order to 'reduce the European Union's dependence on technologies from the United States and China'¹³⁴. Explicitly invoking a 'sovereignty drive' for a sectoral funding instrument shows that, for the Commission, industrial support for AI adoption is not framed in purely economic terms but is presented as part of a broader geopolitical strategy of reducing exposure to non-European technology providers, which is exactly the kind of use of ostensibly technical policy that this thesis takes as its central object of analysis.

Cybersecurity

¹³³ European Commission, (2026). "*AI continent*" [online] Available at: https://commission.europa.eu/topics/competitiveness/ai-continent_en.

¹³⁴ Reuters, (2025). "*EU rolls out \$1.1 billion plan to ramp up AI in key industries amid sovereignty drive*" [online] Available at: <https://www.reuters.com/world/china/eu-rolls-out-11-billion-plan-ramp-up-ai-key-industries-amid-sovereignty-drive-2025-10-08/>.

The EU's cybersecurity strategy increasingly treats artificial intelligence as both a source of new vulnerabilities and a tool for defending against them, and this dual framing has begun to shape institutional design. The European Union Agency for Cybersecurity, working with the Commission, has been tasked with creating a blueprint to secure access to advanced AI systems for cybersecurity purposes, as part of the July 2026 EU Action Plan on Cybersecurity and Artificial Intelligence¹³⁵. Linking the AI Act's implementing machinery directly to a dedicated cybersecurity action plan shows how the Union increasingly treats AI governance and cyber-resilience as two faces of a single strategic problem, rather than as separate regulatory silos, reflecting an awareness that AI systems are at the same time targets of attack, vectors of attack, and instruments of defence.

The debate on artificial intelligence and cybersecurity is far broader than the AI Act itself, and the Regulation is only one element of a much denser legal and institutional landscape. Within the Act, the relevant provision is Article 15, which requires high-risk systems to 'achieve an appropriate level of accuracy, robustness, and cybersecurity' and to be 'resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities', adding that technical solutions 'shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning)'¹³⁶. This is one of the few places where the Regulation acknowledges that artificial intelligence systems have vulnerabilities of their own, distinct from those of ordinary software. Around this provision sits the wider cybersecurity acquis. The NIS2 Directive, formally Directive (EU) 2022/2555 'on measures for a high common level of cybersecurity across the Union', explicitly encourages Member States to promote 'the use of any innovative technology, including artificial intelligence, the use of which could improve the detection and prevention of cyberattacks', and invites essential and important entities to 'pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems'¹³⁷. The European Union Agency for Cybersecurity documents the other side of the same

¹³⁵ European Commission, (2026). "*AI Act*", Shaping Europe's Digital Future [online] Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

¹³⁶ Regulation (EU) 2024/1689, Article 15(1) and 15(5), official consolidated text reproduced in artificialintelligenceact.eu, "Article 15(1) and 15(5)" [online] Available at: <https://artificialintelligenceact.eu/article/15/>.

¹³⁷ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), *OJ L 333/80*, recitals 51 and 89 [online] Available at: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>.

phenomenon in its annual *ENISA Threat Landscape*, published most recently in October 2025, which tracks the use of artificial intelligence by attackers in phishing, social engineering and information manipulation¹³⁸. Taken together, these instruments show that the Union treats artificial intelligence in the cyber domain in three capacities at once, as a defensive tool, as an attack surface and as an offensive capability in the hands of others, and that its response is spread across at least three distinct legal instruments rather than concentrated in one. This fragmentation is itself part of the problem, because it means that no single authority holds a complete picture of AI-related cyber risk.

This securitisation of AI policy is reinforced by voices within the EU's foreign-policy analytical community who link cybersecurity directly to the Union's broader defence posture. ECFR analyst Ángel Melguizo has argued that, as Europe rearms, 'the real vulnerability is not on tanks or missiles but the software and networks behind them', adding pointedly that 'the union can import weapons. It cannot afford to outsource the digital systems that make modern military power possible'¹³⁹. This captures precisely why cybersecurity functions as a strategic domain in its own right within the EU's AI policy: unlike conventional armaments, which can be procured from allied suppliers without necessarily compromising strategic autonomy, the software and data infrastructures underlying AI-enabled defence and security systems cannot be externalised so easily without creating durable dependencies on non-European actors, a concern that connects cybersecurity policy directly to the defence dimension considered next.

Defence, Within the Limits of EU Competence

Defence is the strategic domain where the limits of the EU's legal competence are most clearly exposed, and understanding those limits matters for any realistic assessment of the Union's geopolitical use of AI. The exclusion is set out in Article 2(3) of the AI Act, which provides that the Regulation 'does not apply to areas outside the scope of Union law, and shall not, in any event, affect the competences of the Member States concerning national security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences', and that it 'does not apply to AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out

¹³⁸ European Union Agency for Cybersecurity (ENISA), (2025). "*ENISA Threat Landscape 2025*", October 2025 [online] Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>.

¹³⁹ European Council on Foreign Relations, Ángel Melguizo, (2025). "*Deep pockets, DeepSeek, and the EU's digital drift*" [online] Available at: <https://ecfr.eu/article/deep-pockets-deepseek-and-the-eus-digital-drift/>.

those activities’¹⁴⁰. The safety, transparency and human-oversight requirements examined above therefore do not apply to military AI, which remains governed by separate national and EU defence rules. A related exclusion in Article 2(6) provides that the Regulation ‘does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development’¹⁴¹, although systems subsequently placed on the market or put into service for other purposes fall back within the scope of the Act.

The military exemption is not a marginal drafting choice; it is structural, and it follows directly from the Union’s own constitutional architecture. As Plixavra Vogiatzoglou observes, the provision ‘further clarifies that it shall not affect national competences in that field, as also stipulated in Article 4(2) of the Treaty on European Union’, which means that the carve-out reproduces a Treaty limit rather than a political preference¹⁴². The same analysis warns about the consequences for the internal market, noting that ‘by excluding national security from these regulations, the market becomes further fragmented, increasing legal uncertainty and undermining the trustworthiness and innovation of AI technologies at large’¹⁴³. The point is confirmed in the specialist literature on military AI governance: Javadi, Onderco and Vanhoonacker note that ‘despite the EU’s ambitions, military uses of AI were explicitly excluded from the Act’, and explain that this exclusion reflects ‘the EU’s lack of competence in national defence and security matters’, with the result that Member States pursue military AI governance in other forums¹⁴⁴. The European Parliament’s own research service puts it in the plainest terms, stating that the Act ‘focuses solely on commercial AI, explicitly excluding military applications and national security services’, and recording that ‘during the negotiations some Member States, notably France, pushed for exemptions to preserve Europe’s strategic autonomy’¹⁴⁵. This last detail is important, because it shows that the exemption was not merely a passive consequence of the Treaties but was actively defended by Member States in the name

¹⁴⁰ Regulation (EU) 2024/1689, Article 2(3), official consolidated text reproduced in *artificialintelligenceact.eu*, “Article 2(3)” [online] Available at: <https://artificialintelligenceact.eu/article/2/>.

¹⁴¹ Ibid., Article 2(6).

¹⁴² Vogiatzoglou, P., (2024). “*The AI Act National Security Exception*”, *Verfassungsblog*, 9 December 2024 [online] Available at: <https://verfassungsblog.de/the-ai-act-national-security-exception/>.

¹⁴³ Ibid.

¹⁴⁴ Javadi, M., Onderco, M. & Vanhoonacker, S., (2025). “*The European Union’s missing voice: member states’ forum shopping in military AI governance*”, *European Security*, 23 October 2025 [online] Available at: <https://www.tandfonline.com/doi/full/10.1080/09662839.2025.2570806>.

¹⁴⁵ European Parliamentary Research Service, Clapp, S., (2025). “*Defence and artificial intelligence*”, PE 769.580, April 2025 [online] Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI\(2025\)769580_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf).

of the same strategic autonomy the Union invokes elsewhere. The result is a paradox at the centre of the Union's position: the EU has produced the most comprehensive framework for trustworthy AI in the world, and that framework stops precisely where the strategic stakes are highest. Its celebrated regulatory power does not reach, as a matter of competence, into the domain of armed force, and this is why the Union's influence over military AI has to be exercised through funding instruments, procurement and coordination rather than through regulation. The pattern is not unique to Europe: South Korea's AI Framework Act contains a comparable carve-out excluding AI systems developed and deployed exclusively for national defence or security purposes¹⁴⁶, which suggests that the rights-versus-security carve-out is an almost universal feature of comprehensive AI legislation rather than a quirk of European constitutional design.

Precisely because the AI Act itself cannot reach the military domain, the EU's geopolitical use of AI in defence works through adjacent instruments: investment coordination, industrial policy for dual-use technologies, and diplomatic engagement rather than binding regulation. Carnegie's Raluca Csernatonu argues that the Union must 'increase investments, develop its own digital infrastructure, and regulate dual-use AI applications' as part of a broader 'balancing act between competing priorities', explicitly naming 'civilian and military AI governance' as one of the central tensions the EU must navigate to secure genuine technological sovereignty¹⁴⁷. This is a useful point: it acknowledges that the AI Act's regulatory instruments, however sophisticated within their own domain, are simply the wrong tool for the defence dimension of AI geopolitics, and that the EU's credibility as a security actor in the AI era will depend on capabilities, such as investment, infrastructure and dual-use industrial policy, that mostly sit outside the AI Act's own legal perimeter. This constraint, and what it means for the EU's broader claim to geopolitical relevance, is examined in greater depth in section 3.2.

Protection of Fundamental Rights

The protection of fundamental rights is the domain where the EU's AI policy is most clearly continuous with its longer-standing normative identity, and it is here that using regulation as

¹⁴⁶ Future of Privacy Forum, (2025). "South Korea's New AI Framework Act: A Balancing Act Between Innovation and Regulation" [online] Available at: <https://fpf.org/blog/south-koreas-new-ai-framework-act-a-balancing-act-between-innovation-and-regulation/>.

¹⁴⁷ Carnegie Endowment for International Peace, Raluca Csernatonu, (2025). "The EU's AI Power Play: Between Deregulation and Innovation" [online] Available at: <https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation>.

strategic leverage is, paradoxically, least controversial and most consistently pursued. The prohibitions on unacceptable-risk practices discussed in section 2.2, together with the transparency obligations of Article 50 examined above, particularly the ones addressing emotion recognition, biometric categorisation and deepfakes, are all justified mainly, in the Regulation's own architecture, by reference to the protection of fundamental rights rather than to market efficiency or industrial competitiveness.

Yet even this apparently values-driven domain is not insulated from the deregulatory pressures documented in section 2.2. The joint statement signed by 133 civil society organisations and trade unions in November 2025 explicitly framed the leaked Digital Omnibus proposals as risking 'the biggest rollback of digital fundamental rights in EU history'¹⁴⁸, a warning that shows how fundamental-rights protection, even when nominally the AI Act's primary justification, remains open to renegotiation whenever it comes into perceived conflict with competitiveness objectives. The fact that this tension persists suggests that fundamental-rights protection functions, within the EU's broader AI strategy, both as a genuine normative commitment and as part of the Union's international self-presentation as a rules-based, rights-respecting alternative to less constrained models of AI governance elsewhere, a self-presentation that keeps its strategic value regardless of how closely enforcement in practice actually keeps pace with legislative rhetoric.

External Action and Global Standard-Setting

The last domain in which AI functions as a political asset for the EU is external action, understood broadly as the Union's attempt to project its regulatory model beyond its own borders and so shape the global governance of artificial intelligence. This is the domain where the logic of the previous four sections comes together most clearly with geopolitics in the classical sense, since it concerns the EU's capacity to influence the behaviour of other states and firms without resorting to military or coercive instruments.

The conceptual foundation for this external dimension is the phenomenon that Anu Bradford has termed the 'Brussels Effect', and in her more recent work she extends this framework explicitly to artificial intelligence, writing that 'artificial intelligence may well be the next frontier of the Brussels Effect' and that the EU AI Act 'has the potential to shape the

¹⁴⁸ European Digital Rights (EDRi), (2025). "*Forthcoming Digital Omnibus would mark point of no return*" [online] Available at: <https://edri.org/our-work/forthcoming-digital-omnibus-would-mark-point-of-no-return/>.

development of AI globally’¹⁴⁹. This thesis will not develop that theory in full at this stage; the concept, its five underlying conditions, and the substantial body of critical commentary questioning whether the AI Act can actually replicate the GDPR’s global diffusion are left for systematic treatment in section 3.1, where the balance of evidence for and against a genuine ‘AI Brussels Effect’ is assessed directly. For now, it is enough to note that the aspiration to standard-setting is not a peripheral or rhetorical add-on to the EU’s AI strategy but one of its constitutive goals: the Union’s regulatory activity in the AI domain is explicitly conceived, by its own architects and by outside observers alike, as a vehicle for external influence, not just as an instrument of internal market governance.

Putting these five domains together, this section shows that the EU’s use of artificial intelligence policy cannot be reduced to a single register. In industrial policy and cybersecurity, regulation is explicitly paired with investment and institutional capacity-building in pursuit of reduced external dependence. In defence, the Union’s regulatory instruments are structurally inapplicable, which forces it to rely on adjacent tools of industrial and diplomatic leverage instead. In fundamental-rights protection, regulation stays closest to its original normative justification, even though it too is exposed to competitiveness-driven renegotiation. In external action, finally, regulation is explicitly used as a tool of global influence, positioning the AI Act as a template the EU actively wants to see copied abroad. So the guiding question of this section, whether the EU is using AI purely as regulation or also as strategic leverage, has a fairly clear answer: it is doing both, and the boundary between the two functions is becoming progressively harder to draw. Regulation was never simply a defensive or technocratic exercise for the Union; it has become, more and more explicitly across each of the domains surveyed here, an instrument consciously used in pursuit of strategic advantage. Whether that regulation-as-leverage can actually deliver durable geopolitical power is the question the rest of this thesis now turns to.

¹⁴⁹ Anu Bradford, (2023). *Digital Empires: The Global Battle to Regulate Technology*, p. 348, quoted in Alexander von Humboldt Institute for Internet and Society, “Brussels effect or experimentalism? The EU AI Act and its extraterritorial application” [online] Available at: <https://policyreview.info/articles/analysis/brussels-effect-or-experimentalism>.

Chapter III - Regulation as an Instrument of Geopolitical Power: Limits and Potential of the EU

The previous chapter showed that the European Union does not treat artificial intelligence only as an object to be regulated, but as a lever it uses across industrial policy, cybersecurity, defence, the protection of fundamental rights and external action, and that regulation itself is increasingly used as a form of strategic leverage.

This chapter now takes up the analytical question that discussion left open: can regulation, in the specific case of AI, really translate into geopolitical power, understood as the capacity to shape outcomes beyond one's own borders and to hold a durable position in an international system that is more and more organised around technological capability?

The chapter proceeds in three steps. Section 3.1 looks at the Brussels Effect, which is the theoretical mechanism through which EU regulation is supposed to become global influence, and submits Anu Bradford's framework to a critical reading. Section 3.2 moves from the diffusion of rules to the capabilities that lie underneath them, asking whether the Union actually has the industrial, military and technological base that would make its normative model credible and self-sustaining. Section 3.3 brings the two lines of analysis together into three possible future trajectories for the EU's technological geopolitics, and then gives a direct answer to the central research question of this thesis.

3.1 The Brussels Effect in the Technological Domain

The theoretical starting point for any assessment of whether EU regulation can generate geopolitical power is the concept of the 'Brussels Effect', first set out by the Columbia Law School scholar Anu Bradford in a 2012 law-review article and then developed at length in her 2020 book, *The Brussels Effect: How the European Union Rules the World*, published by Oxford University Press and named one of the best books of 2020 by Foreign Affairs¹⁵⁰. Bradford's framework distinguishes two mechanisms that are related but analytically separate. The de facto Brussels Effect describes the process by which multinational companies, in order to keep access to the large internal market of the EU, voluntarily extend European standards to

¹⁵⁰ Anu Bradford, (2020). *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020); see also Cato Institute, "The Brussels Effect" [online] Available at: <https://www.cato.org/regulation/summer-2020/brussels-effect>

their global operations, without any government action being needed. This is what happened when Apple, Microsoft, Google and Meta adopted GDPR-style privacy architectures across their worldwide operations¹⁵¹. The de jure Brussels Effect, instead, happens when foreign governments formally adopt EU-style rules, usually because the multinationals that have already adapted to European requirements lobby their own governments to level the domestic playing field. Bradford describes the de jure effect as being 'largely a consequence of' the de facto effect, which creates an important sequence between the two mechanisms¹⁵².

Bradford identifies five conditions that must all be present for the Brussels Effect to work: a market large enough to attract foreign economic actors; regulatory capacity and stringency sufficient to set meaningful standards; 'inelastic targets', meaning that the regulation must fall on consumers and products, which cannot move, and not on capital, which can; non-divisibility of production, so that firms find it more efficient to apply one single global standard than to fragment compliance jurisdiction by jurisdiction; and, in general, the absence of coercion, because the mechanism depends on voluntary commercial adaptation and not on the exercise of formal international authority¹⁵³. In her later book, *Digital Empires: The Global Battle to Regulate Technology* (2023), Bradford extends this framework explicitly to artificial intelligence, writing that 'artificial intelligence may well be the next frontier of the Brussels Effect' and that the AI Act 'has the potential to shape the development of AI globally'¹⁵⁴. It is important to note that, when she discusses the AI Act specifically, Bradford treats both dimensions of diffusion as open empirical questions and not as foregone conclusions: whether companies will change their behaviour outside the EU because of AI Act obligations, and whether other jurisdictions will copy the European legislative approach at home, are, in her own words, matters still to be settled by evidence rather than assumed from the GDPR precedent¹⁵⁵. It is also worth noting that by December 2025 Bradford's own public commentary

¹⁵¹ Anu Bradford, (2020). *The Brussels Effect* (Oxford University Press, 2020), excerpted at Scribd [online] Available at: <https://www.scribd.com/document/512434092/Anu-Bradford-The-Brussels-Effect-How-the-European-Union-Rules-the-World-Oxford-University-Press-2020>

¹⁵² Anu Bradford, (2020). *The Brussels Effect* (2020), cited in EJLS book review, University of Luxembourg [online] Available at: <https://ejls.eui.eu/wp-content/uploads/sites/32/2021/06/16.-EJLS-131-Patrin.pdf>

¹⁵³ Anu Bradford, (2025). *The Brussels Effect* (2020), summarized in University of Luxembourg book review [online] Available at: <https://www.uni.lu/fdef-en/articles/a-book-review-of-anu-bradford-the-brussels-effect-how-the-european-union-rules-the-world/>

¹⁵⁴ Anu Bradford, (2023). *Digital Empires*, p. 348, quoted in Alexander von Humboldt Institute for Internet and Society, "Brussels effect or experimentalism? The EU AI Act and its extraterritorial application" [online] Available at: <https://policyreview.info/articles/analysis/brussels-effect-or-experimentalism>

¹⁵⁵ LinkedIn, Luiza Jarovsky, citing Anu Bradford, (2025). "AI and the Brussels Effect: Anu Bradford's Insights" [online] Available at: https://www.linkedin.com/posts/luizajarovsky_ai-aireregulation-airace-activity-7306990879234248704-O0cp

had become considerably more critical of how the AI Act has been carried out, discussing 'how the EU botched its attempt to regulate' AI, while still maintaining that the theoretical possibility of Brussels Effect diffusion remains open¹⁵⁶.

The empirical plausibility of an AI-specific Brussels Effect is best assessed against the precedent on which it is openly modelled, that is the global diffusion of the GDPR after 2018. Measured by that benchmark, the record is striking. By the end of 2024 an estimated 144 countries had put national data-privacy laws in place, covering roughly 6.64 billion people¹⁵⁷, while a 2025 SSRN survey counts as many as 172 countries with data-privacy laws in force and notes that many of the twelve new laws adopted in 2023/24 alone 'continue to show strong influence of the EU's GDPR'¹⁵⁸. Bradford's own account attributes this diffusion to the de facto Brussels Effect working through Big Tech in particular: once Apple, Google, Meta and Microsoft had adapted their global privacy architecture to the GDPR, they had a straightforward commercial incentive to apply one single global standard instead of fragmenting compliance country by country¹⁵⁹. At first sight, then, the GDPR precedent seems to confirm Bradford's general theory; the question this section has to answer is whether the AI Act has the same structural properties that made the diffusion of the GDPR possible.

Critical Counter-Arguments: Why AI May Not Replicate the GDPR Precedent

A substantial and growing body of scholarship suggests that the AI Act *does not* satisfy Bradford's own conditions as easily as the GDPR did, and that the analogy between the two regulations is less secure than European policymakers have assumed. A peer-reviewed analysis published in *Internet Policy Review* concludes that 'the external impact of the AI Act is more in line with experimentalist governance than with the theory of the Brussels effect', and argues in particular that AI applications 'are far from non-divisible', a condition the same analysis calls 'crucial' for the de facto Brussels effect, because providers can easily differentiate applications for different markets, especially where AI is embedded in specific devices such as cars or

¹⁵⁶ LinkedIn, Anu Bradford, (2025). "How to balance regulation and innovation in AI" [online] Available at: https://www.linkedin.com/posts/anu-bradford-5036309_how-the-eu-botched-its-attempt-to-regulate-activity-7397212465018707970-pW00

¹⁵⁷ IAPP, (2025). "Data protection and privacy laws now in effect in 144 countries" [online] Available at: <https://iapp.org/news/a/data-protection-and-privacy-laws-now-in-effect-in-144-countries>

¹⁵⁸ SSRN, (2025). "Global Data Privacy Laws 2025: 172 Countries, Twelve New in 2023/24" [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5275559

¹⁵⁹ Anu Bradford, (2025). *The Brussels Effect* (2020), discussed in Alexander von Humboldt Institute, "Brussels effect or experimentalism?" [online] Available at: <https://policyreview.info/articles/analysis/brussels-effect-or-experimentalism>

medical technology¹⁶⁰. This is a decisive difference from the GDPR: the architecture for processing personal data is genuinely difficult to fragment across jurisdictions once it has been built to a single global standard, while an AI system embedded in a vehicle or in a piece of medical equipment can in principle be configured differently for the European market and for other markets without prohibitive extra costs. The same analysis also observes that 'the de jure Brussels effect relies to a significant extent on the de facto effect, since if the EU's leverage over the regulated companies is more limited then it also becomes a less compelling example for other jurisdictions'¹⁶¹. This means that any weakness in the de facto mechanism passes directly into the de jure one, so that the diffusion potential of the AI Act is weakened on both dimensions at the same time.

The empirical evidence on actual legislative emulation reinforces this scepticism. The CEPA analyst Anda Bologa reports that, unlike the GDPR and the Digital Markets Act, 'so far Europe's ambitious AI rules are inspiring few others', and identifies only Peru, Canada and Brazil as showing real interest in reproducing the European risk-based blueprint, while the United Kingdom, Australia, New Zealand, Switzerland, Singapore and Japan have preferred lighter, pro-innovation, sector-specific approaches¹⁶². The legal scholars Marco Almada and Anca Radu, cited in the same analysis, add an institutional dimension to this scepticism, noting that 'Brussels sprinted ahead of multilateral tracks' such as the G-7 Hiroshima Process, the OECD's AI risk matrix and the Council of Europe treaty. In other words, the EU acted unilaterally instead of working through consensus-building bodies, and this choice may have reduced wider international support precisely because it bypassed the diplomatic channels that many states prefer to use when they coordinate on emerging technologies¹⁶³. A further structural obstacle to emulation lies in compliance costs: the AI Act 'front-loads hefty conformity-assessment costs', obliging start-ups 'to pay auditors and generate reams of technical documentation before launching a single line of code', which contrasts sharply with the iterative release-and-monitoring model preferred by the United Kingdom and Japan¹⁶⁴. This asymmetry in compliance costs plausibly discourages third countries from adopting the heavier

¹⁶⁰ Alexander von Humboldt Institute for Internet and Society, (2025). "*Brussels effect or experimentalism? The EU AI Act and its extraterritorial application*" [online] Available at: <https://policyreview.info/articles/analysis/brussels-effect-or-experimentalism>

¹⁶¹ Ibid.

¹⁶² CEPA, Anda Bologa, (2025). "*Burying the Brussels Effect? AI Act Inspires Few Copycats*" [online] Available at: <https://cepa.org/article/burying-the-brussels-effect-ai-act-inspires-few-copycats/>

¹⁶³ Marco Almada and Anca Radu, cited in CEPA, (2025). "*Burying the Brussels Effect?*" [online] Available at: <https://cepa.org/article/burying-the-brussels-effect-ai-act-inspires-few-copycats/>

¹⁶⁴ Ibid.

European template even when they share its underlying risk-based philosophy. On top of this, the decision of the Trump administration in 2025 to rescind the AI safety initiative of the Biden administration, instructing federal agencies to 'remove barriers' to AI development, 'darkens prospects for transatlantic cooperation on AI' and makes American regulatory convergence with the European model less likely¹⁶⁵. This removes what would otherwise be the single most important potential adopter of an EU-aligned model.

A further and more theoretically ambitious critique holds that, even where the Brussels Effect does happen in the AI domain, its consequences may be counterproductive from the point of view of the EU itself. An article in the *German Law Journal* coins the concept of a 'Brussels Side-Effect', arguing that even a successful diffusion of the AI Act as a global regulatory template 'might undermine many of the European values the EU AI strategy is meant to promote', because the abstract high-risk rules of the Act make providers 'de facto responsible for determining how the legal requirements are converted into software requirements'. This delegation of interpretive authority can produce a lower level of protection for those values that cannot easily be translated into product-safety requirements¹⁶⁶. This critique is genuinely double-edged for the EU, because it suggests that the Brussels Effect, even when it works as a mechanism of diffusion, may not reliably transmit the substantive values the Union associates with its own regulatory model, since the firms that implement abstract rules across different jurisdictions keep considerable discretion over how those rules are technically applied.

Two further contributions refine the analytical vocabulary needed to assess diffusion in the AI field. A 2024 SSRN working paper argues that the concept of the Brussels Effect has been applied too loosely to the AI Act and should be broken down into four distinct types of influence, that is extraterritorial application, de facto corporate adoption, legislative emulation by third countries, and adoption in international agreements and standards. The paper maintains that any credible assessment of the real influence of the EU in AI has to examine all four dimensions instead of treating the Brussels Effect as one single, unitary phenomenon¹⁶⁷. A related think-tank analysis notes that even Bradford herself, while she appreciates the diffusion

¹⁶⁵ CEPA, (2025). "Burying the Brussels Effect?" [online] Available at: <https://cepa.org/article/burying-the-brussels-effect-ai-act-inspires-few-copycats>

¹⁶⁶ Cambridge Core, (2024). "The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy" [online] Available at: <https://www.cambridge.org/core/journals/german-law-journal/article/brussels-sideeffect-how-the-ai-act-can-reduce-the-global-reach-of-eu-policy/032C72AEC537EBB6AE96C0FD90387E3E>

¹⁶⁷ SSRN, (2024). "EU AI Act: Brussels Effect(s) or a Race to the Bottom?" [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4975172

potential of the AI Act, has acknowledged that the EU 'could no longer...trust that AI development elsewhere would follow EU imperatives', which points to a real and growing de facto regulatory divergence at global level¹⁶⁸. Finally, a commentary of December 2024 titled 'Doubting a "Brussels Effect 2.0"' observes that 'despite the large-scale formal acceptance of the AI Act, domestic implementations greatly vary, based on each country's capacity to do so', with many countries facing a 'lack of funding, lack of trained personnel, and lack of national consensus'¹⁶⁹. This criticism closely parallels the implementation gaps already documented inside the EU in section 2.2, and it suggests that capacity constraints on AI governance are not specific to the Union but reappear wherever its regulatory template is adopted.

Concrete Evidence of Emulation: A Mixed and Partial Picture

Despite this weight of critical commentary, the empirical record is not uniformly negative, and a balanced assessment has to register the genuine cases of diffusion alongside the scepticism documented above. It is worth recalling, before this record is examined, that emulation is not only a category of regulatory studies but also a long-standing concept in the organisational literature on innovation, where Thomas G. Mahnken and James R. FitzSimonds have shown that the adoption of a foreign model depends far less on the intrinsic merits of that model than on the attitudes, incentives and absorptive capacity of the organisations expected to adopt it, so that imitation is normally selective and partial rather than wholesale¹⁷⁰. Read through that lens, the uneven and largely vocabulary-level diffusion documented below is the expected pattern rather than an anomaly. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, also known as the Vilnius Convention, was adopted by the Committee of Ministers on 17 May 2024 and opened for signature on 5 September 2024, becoming the first internationally binding treaty on AI. On that date it was signed, among others, by the European Union, Andorra, Georgia, Iceland, Israel, Moldova, Norway, San Marino, Ukraine, the United Kingdom and the United States¹⁷¹. The

¹⁶⁸ Hoch and Mugge, (2025). "EU Influence in Global AI Governance and its Limits" [online] Available at: <https://regulaite.eu/images/pdf/HochMugge2025.pdf>

¹⁶⁹ Modern Diplomacy, (2024). "Doubting a "Brussels Effect 2.0": Can the European Union's AI Act Foster Legitimacy?" [online] Available at: <https://moderndiplomacy.eu/2024/12/24/doubting-a-brussels-effect-2-0-can-the-european-unions-ai-act-foster-legitimacy/>

¹⁷⁰ Mahnken, T.G. and FitzSimonds, J.R., (2003). *The Limits of Transformation: Officer Attitudes toward the Revolution in Military Affairs*, Newport Paper 17, Newport, RI: Naval War College Press; see also Mahnken, T.G. and FitzSimonds, J.R., (2003). "Revolutionary Ambivalence: Understanding Officer Attitudes toward Transformation", *International Security*, 28(2), pp. 112-148.

¹⁷¹ Council of Europe, cited in eucrim.eu, (2024). "Council of Europe Convention on Artificial Intelligence" [online] Available at: <https://eucrim.eu/news/council-of-europe-convention-on-artificial-intelligence/>

European Commission's own account of the Convention describes it as 'fully compatible with Union law in general, and the EU AI Act in particular', and the Convention was signed on behalf of the EU by Commission Vice-President Věra Jourová¹⁷², while by May 2026 it counted 46 signatories, including all EU member states together with the United Kingdom, the United States, Japan, Canada, Israel and Switzerland¹⁷³. This multilateral result is a genuine, if partial, confirmation of the standard-setting ambition of the EU, even though the binding force of the Convention and its degree of substantive alignment with the risk-based architecture of the AI Act remain much looser than a strict Brussels Effect would require.

More direct evidence of legislative emulation can be found in specific national initiatives. Brazil's PL 2338/2023, the 'Marco Legal da Inteligência Artificial', was approved by the Federal Senate on 10 December 2024 and 'draws directly from the European AI Act', adopting a four-tier risk classification modelled explicitly on the European framework, with fines of up to R\$50 million per infraction for individuals or 2% of Brazilian revenue for legal entities, and provisions on regulatory sandboxes that echo the enforcement design of the EU¹⁷⁴. South Korea's AI Framework Act, passed by the National Assembly on 26 December 2024 and in force since 22 January 2026, made Korea 'the second jurisdiction in the world, after the European Union, to implement a comprehensive statutory framework governing artificial intelligence'¹⁷⁵. The substance of this emulation is telling precisely because it is partial: the Korean Act 'borrows the EU's talk of "risk" and "transparency," but skips the EU's heavy pre-launch inspection requirements', since it only requires a risk-review filing for high-impact systems, with no mandatory third-party audit, and caps fines at around €21,000, a level far below the AI Act's fines of up to 7% of global turnover¹⁷⁶. This is emulation of the conceptual vocabulary of the EU, with its risk tiers and transparency duties, but not of its enforcement

¹⁷² European Commission, (2024). "Commission signed the Council of Europe Framework Convention on Artificial Intelligence and Human Rights" [online] Available at: <https://digital-strategy.ec.europa.eu/en/news/commission-signed-council-europe-framework-convention-artificial-intelligence-and-human-rights>

¹⁷³ Center for AI and Digital Policy, (2026). "International AI Treaty" [online] Available at: <https://www.caidp.org/resources/coe-ai-treaty/>

¹⁷⁴ Douglas Vilar Sociedade de Advogados, (2026). "Marco Legal da IA no Brasil" [online] Available at: https://douglasvilar.com.br/artigos/posts/2026-06-13_marco-legal-ia-pl-2338-regulacao-brasil

¹⁷⁵ Future of Privacy Forum, (2025). "South Korea's New AI Framework Act: A Balancing Act Between Innovation and Regulation" [online] Available at: <https://fpf.org/blog/south-koreas-new-ai-framework-act-a-balancing-act-between-innovation-and-regulation/>

¹⁷⁶ CEPA, (2025). "Burying the Brussels Effect?" [online] Available at: <https://cepa.org/article/burying-the-brussels-effect-ai-act-inspires-few-copycats/>

intensity, which is exactly the kind of selective adoption that the compliance-cost critique discussed above would predict.

Canada, by contrast, offers an example of failed emulation. The Artificial Intelligence and Data Act, introduced in 2022 as part of Bill C-27 and initially described as mirroring 'Europe's push' towards a risk framework centred on high-impact systems, was left in legislative limbo when Parliament was prorogued, so that as of April 2026 Canada still has no dedicated federal AI law¹⁷⁷. California's Transparency in Frontier Artificial Intelligence Act, adopted on 29 September 2025, is instead an entirely independent regulatory model at American state level, which has developed in parallel with the European framework rather than being derived from it¹⁷⁸. Among the EFTA states the picture is again mixed: Switzerland is integrating the Council of Europe AI Convention 'through fine-tuned updates to existing laws' rather than reproducing the heavier structure of the AI Act, while Norway is 'incorporating the EU AI Act in its domestic legislation' directly¹⁷⁹. Even among the states that are geographically and economically closest to the EU, therefore, the depth of regulatory alignment varies considerably.

Weighing all this evidence together, the balance tilts, on the present record, against a robust AI-specific Brussels Effect on the GDPR model, although it does not justify dismissing European influence altogether.

The theoretical case for scepticism is considerably more developed and better supported empirically than the case for optimism. It rests on the divisibility of AI applications, on front-loaded compliance costs, on the unilateral departure of the EU from multilateral standard-setting tracks, and on the risk that diffusion, where it does occur, transmits vocabulary rather than substance. The case for optimism, by contrast, currently rests on a comparatively thin set of examples: a small number of partial legislative adopters, a multilateral treaty with a looser binding force than the AI Act itself, and Bradford's own extension of a framework she originally built for a completely different regulatory instrument. This suggests an answer to the question this section set out to resolve: regulation can translate into geopolitical power, but *only conditionally*, and it is the structural features of the AI Act itself, and not only the

¹⁷⁷ Ibid.

¹⁷⁸ A&O Shearman, (2025). "California adopts landmark AI law" [online] Available at: <https://www.aoshearman.com/en/insights/ao-shearman-on-tech/california-adopts-landmark-ai-law>

¹⁷⁹ CEPA, (2025). "Burying the Brussels Effect?" [online] Available at: <https://cepa.org/article/burying-the-brussels-effect-ai-act-inspires-few-copycats>

resistance of external competitors, that limit how far that translation is taking place. The regulatory activity of the EU in the field of AI generates real international influence, but that influence is partial and unevenly distributed, and it is not yet the kind of almost automatic diffusion that characterised the GDPR. Whether this partial regulatory influence is enough to compensate for the more fundamental capability constraints of the Union is the question addressed in the section that follows.

3.2 The EU as a Geopolitical Technology Actor

If section 3.1 assessed whether European rules spread internationally, this section addresses a more basic and arguably more important question: does the European Union have the industrial, military and technological capabilities that would make its normative model credible as a foundation for geopolitical power, independently of how far its regulations travel? The evidence collected below suggests a largely negative answer, and shows structural weaknesses across defence, digital infrastructure and industrial competitiveness that qualify, without cancelling, the regulatory achievements documented in Chapter II.

Defence Fragmentation

Total EU defence expenditure reached €381 billion in 2025, and yet the increase in spending has clearly not produced a matching growth in joint acquisition: only 18% of defence investment took place collaboratively in the most recent coordinated annual review, far below the European Defence Agency's own benchmark of 35% collaborative procurement, which was set as long ago as 2007¹⁸⁰. In response the Union has expanded its financial instruments, EDIRPA, EDIP and SAFE, which offer grants and loans to encourage joint procurement, and a defence readiness roadmap sets a target of 40% joint procurement by 2027¹⁸¹. Even so, the EU institutions themselves continue to point to 'duplication issues, capability gaps and over-reliance on non-EU suppliers', and they attribute these persistent constraints to 'differing threat perceptions by national governments' and to 'industrial competition that often runs counter to consolidation'¹⁸². These aggregate figures also rest on incomplete reporting, since only twelve of the twenty-seven member states supplied the European Defence Agency with data on their

¹⁸⁰ European Parliament Research Service, (2026). “*EU joint defence procurement*” [online] Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/785665/EPRS_BRI\(2026\)785665_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/785665/EPRS_BRI(2026)785665_EN.pdf)

¹⁸¹ Ibid.

¹⁸² Ibid.

EU collaborative equipment procurement, which makes a comprehensive assessment of collaborative spending impossible at present¹⁸³. Independent datasets confirm that the problem lies in coordination rather than in volume: SIPRI records European military expenditure rising by 14% in 2025 to USD 864 billion, the steepest increase among European NATO members since 1953, while the IISS Military Balance 2026 places Europe at more than 21% of global defence spending, against 17% in 2022¹⁸⁴. This fragmentation persists despite substantial aggregate resources, since the European members of NATO together with Canada spent more than USD 482 billion on defence in 2024, and yet capability gaps remain and are, in the assessment of one analysis, 'documented in European sources and growing more expensive to close with each year of structural delay'¹⁸⁵. This is an important qualification of the military exemption in Article 2(3) of the AI Act discussed in section 2.3. The Treaty-based limits on EU competence in defence would matter much less if the member states compensated for them through effective intergovernmental coordination, but the persistence of fragmented and largely national procurement suggests that the absence of European regulatory reach into the military domain is made worse, rather than offset, by the absence of collective capability in the same domain.

The Absence of an EU 'Big Tech' and the Compute-and-Cloud Dependency

The most consequential structural weakness identified in the diagnostic literature concerns the dependence of the EU on non-European digital infrastructure. The Draghi Report, presented to the European Commission on 9 September 2024, finds that only three American 'hyperscalers' account for more than 65% of the global as well as the European cloud market, and that around 70% of foundational AI models have been developed in the United States since 2017¹⁸⁶. The report states plainly that 'the largest European cloud operator accounts for just 2%' of the EU

¹⁸³ European Defence Agency, (2025). *Defence Data 2024-2025*, Brussels: EDA [online] Available at: https://eda.europa.eu/docs/default-source/brochures/2025-eda_defencedata_web.pdf.

¹⁸⁴ Stockholm International Peace Research Institute, Liang, X., Tian, N., Lopes da Silva, D., Scarazzato, L., Karim, Z. and Guiberteau Ricard, J., (2026). *Trends in World Military Expenditure, 2025*, SIPRI Fact Sheet, April 2026 [online] Available at: https://www.sipri.org/sites/default/files/2026-04/2604_milex_2025.pdf; International Institute for Strategic Studies, (2026). *The Military Balance 2026*, "Global defence spending" [online] Available at: <https://www.iiss.org/publications/the-military-balance/2026/the-military-balance-2026/global-defence-spending/>.

¹⁸⁵ Friends of Europe, (2026). "*Europe's defence gap: increased spending, limited power*" [online] Available at: <https://www.friendsofeurope.org/insights/critical-thinking-europes-defence-gap-increased-spending-limited-power/>

¹⁸⁶ Mario Draghi, (2024). *The Future of European Competitiveness*, presented to the European Commission 9 September 2024, cited in Euronews, "With AI, EU has opportunity to capitalise on digital, says Draghi" [online] Available at: <https://www.euronews.com/next/2024/09/09/with-ai-eu-has-opportunity-to-capitalise-on-digital-says-draghi>

market, and that of the world's top ten investors in quantum computing five are based in the United States and four in China, with none in the EU¹⁸⁷. Draghi's warning is unambiguous: 'For Europe, there is a risk of being completely dependent on AI models designed and developed abroad', a risk he extends beyond general-purpose applications to vertical applications in the 'automotive, banking, telecommunications, healthcare, mobility and retail' sectors¹⁸⁸.

These structural weaknesses can be measured across several metrics. On global financing for AI start-ups, the Draghi Report finds that 61% went to American companies, 17% to Chinese companies and only 6% to companies based in the EU, and it identifies Aleph Alpha and Mistral as Europe's leading developers of generative-AI models, both of which need 'large investments to become competitive alternatives to their US counterparts', investment that the report says is 'currently not being met by the EU's capital markets'¹⁸⁹. Only four of the world's top fifty technology companies are European, according to the presentation text of the Draghi Report¹⁹⁰, and EU companies spent around €270 billion less on research and development than their American counterparts in 2021, while the report estimates that closing the competitiveness gap with the United States and China would require between €750 and €800 billion of additional investment every year, a figure that has been independently confirmed by the European Central Bank¹⁹¹. More recent market data confirm that this dependency has deepened rather than eased: AWS, Microsoft Azure and Google Cloud together held approximately 70-72% of the European cloud market in 2025, while the collective share of European providers fell from 29% in 2017 to around 15% by 2025¹⁹².

Even the most credible European challenger illustrates the size of the gap rather than closing it. Bruegel describes Mistral AI as 'the European Union's most serious attempt at a competitive AI presence', while it notes that the firm nonetheless 'operates at a scale that barely registers against frontier US or Chinese labs'¹⁹³. The same analysis attributes part of this weakness to

¹⁸⁷ Ibid.

¹⁸⁸ Draghi Report, cited in Heise Online, (2024). "*Draghi competition report: gloomy tech outlook, only niches remain for the EU*" [online] Available at: <https://www.heise.de/en/news/Draghi-competition-report-gloomy-tech-outlook-only-niches-remain-for-the-EU-9864084.html>

¹⁸⁹ Ibid.

¹⁹⁰ Mario Draghi, (2024). "*Address by Mr. Draghi – Presentation of the report on the Future of European competitiveness*", European Commission [online] Available at: https://commission.europa.eu/document/download/fcbc7ada-213b-4679-83f7-69a4c2127a25_en

¹⁹¹ Ibid.

¹⁹² Synergy Research Group, cited in SRG Research, (2025). "*European Cloud Providers' Local Market Share Now Holds Steady at 15%*" [online] Available at: <https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>

¹⁹³ Bruegel, (2026). "*Europe needs a strategy to close the artificial intelligence compute gap*" [online] Available at: <https://www.bruegel.org/analysis/europe-needs-strategy-close-artificial-intelligence-compute-gap>

fragmentation on the demand side, rather than to a lack of talent or ambition, observing that 'EU demand is fragmented across twenty-seven member states, each acting largely alone', unlike the coordinated public procurement of China, and concluding bluntly that 'there is no realistic prospect for Europe to switch to its own AI chip production in the short to medium term'¹⁹⁴. This diagnosis is consistent with the aggregate production figures: an analysis of June 2026 reports that 'the US produced 40 large foundation models last year, China 15 and the EU just 3', and that AI adoption among European SMEs ranges only between 13% and 21%¹⁹⁵. Progress in implementing even the recommendations of the Draghi Report has been slow, since an analysis by Deutsche Bank found that, one year after the report was published, only 11.2% of its 383 recommendations had been fully implemented, with 'limited progress in closing the innovation gap with the US'¹⁹⁶.

The policy response of the Union to this diagnosis has been substantial in scale, even if its adequacy remains contested. The AI Continent Action Plan, formally COM(2025)165 and published on 9 April 2025, is built around the InvestAI initiative, which mobilises €200 billion for AI investment across the EU, including a dedicated €20 billion InvestAI facility intended to attract private investment into 'AI gigafactories'¹⁹⁷. The plan foresees at least nineteen 'AI factories' across Europe, built on the existing supercomputing network, plus up to five 'AI gigafactories' meant to secure European leadership in frontier AI, and it is complemented by a Cloud and AI Development Act which aims to at least triple the data-centre capacity of the EU within five to seven years¹⁹⁸. More recently, on 3 June 2026, the Commission presented a further 'sweeping plan' on technological sovereignty covering semiconductors, AI and cloud, explicitly aimed at achieving 'greater independence from the US and Asia', with possible consequences for eligibility for subsidies and for whether firms such as Microsoft and Amazon may provide cloud services for sensitive government data¹⁹⁹. Bruegel's own policy recommendation is telling in this respect: instead of trying to achieve full self-sufficiency, the

¹⁹⁴ Ibid.

¹⁹⁵ European Commission, (2025). "*High Level Conference – One year after the Draghi report*", factsheet [online] Available at: https://commission.europa.eu/document/download/0951a4ff-cd1a-4ea3-bc1d-f603decc1ed9_en

¹⁹⁶ Deutsche Bank analysis, cited in AOL/Business Insider, (2025). "*Europe promised an innovation comeback against the US and China*" [online] Available at: <https://www.aol.com/articles/europe-promised-innovation-comeback-against-123729455.html>

¹⁹⁷ European Commission, (2026). "*AI continent*" [online] Available at: https://commission.europa.eu/topics/competitiveness/ai-continent_en

¹⁹⁸ Ibid.

¹⁹⁹ Bloomberg, (2026). "*Europe Unveils Sweeping Tech Sovereignty Plan to Boost Chips, AI*" [online] Available at: <https://www.bloomberg.com/news/articles/2026-06-03/europe-unveils-sweeping-tech-sovereignty-plan-to-boost-chips-ai>

EU should adopt a 'two-track strategy' inspired by China, that is continue to buy AI chips from NVIDIA and other American suppliers while at the same time investing in domestic production of advanced chips, together with coordinated EU-wide public procurement of AI compute for public administration, healthcare, defence and research, so as to create an aggregated demand base²⁰⁰. This recommendation is itself an implicit admission that the compute gap documented above cannot realistically be closed through import substitution alone, but only through a more modest strategy of selective capability-building combined with a continued and managed dependency, which is a much less ambitious position than the 'sovereignty' rhetoric surrounding these initiatives would suggest.

Analysis: The Normative Model's Advantages, Structural Limits, and the Rights-Security Tension

The evidence collected in this section supports a layered conclusion about the standing of the EU as a geopolitical technology actor.

The normative model built on regulation and standard-setting has genuine advantages: *it does not require* the Union to match American or Chinese compute capacity in order to exert influence, it fits the comparative institutional strength of the EU in law-making and market governance, and, as section 3.1 showed, it does produce a partial international diffusion even without fully repeating the GDPR precedent. These advantages, however, operate against a background of structural limits that are not accidental but constitutive of the current position of the Union: a defence fragmentation that persists after two decades of institutional effort to overcome it; a dependency on American hyperscalers for compute and cloud that is now approaching three quarters of the European market; the almost complete absence of European firms among global frontier AI developers; and a gap in research and development investment measured in hundreds of billions of euros a year.

These structural limits produce a tension that the drafting choices of the AI Act, examined in section 2.3, bring out very clearly. The exemption in Article 2(3) of military, defence and national-security applications from the scope of the AI Act reflects, on one level, simply the constitutional limits of EU competence. Seen from the perspective of strategic autonomy, however, the same exemption also reveals a deeper vulnerability, because it means that

²⁰⁰ Bruegel, (2026). “*Europe needs a strategy to close the artificial intelligence compute gap*” [online] Available at: <https://www.bruegel.org/analysis/europe-needs-strategy-close-artificial-intelligence-compute-gap>

precisely the AI applications that matter most for the hard-power position of the EU are governed by twenty-seven separate national regimes instead of a coordinated framework at Union level, a fragmentation that mirrors, and probably makes worse, the fragmentation in defence procurement described above. ECFR's Ángel Melguizo captures this connection when he warns that Europe 'can import weapons' but 'cannot afford to outsource the digital systems that make modern military power possible'²⁰¹, and yet the data on compute and cloud dependency reviewed above suggest that the EU has, to a significant extent, already outsourced exactly those digital systems, which makes his warning much harder to act on in practice than in principle. Carnegie's Csernatoní describes the resulting predicament as one that requires the EU to 'increase investments, develop its own digital infrastructure, and regulate dual-use AI applications' at the same time, as part of a real 'balancing act between competing priorities'²⁰². Read against the evidence in this section, that formulation means admitting that the regulatory achievements of the EU and its capability deficits have to be addressed jointly, because neither is enough on its own to secure the position of the Union as a credible technological power. The internal political fragmentation that runs through defence procurement, cloud demand and industrial policy is, in this sense, not a marginal administrative failing but the most consistent explanatory factor behind each of the structural weaknesses listed above, and this conclusion has direct implications for the future trajectories examined in the next section.

3.3 Future Scenarios

Building on the assessment of the Brussels Effect in section 3.1 and on the review of capabilities in section 3.2, this final section synthesises the scholarly and policy debate on the likely trajectory of the European Union, organising the positions defended in that literature into three analytically distinct scenarios: the EU as global regulatory leader, the EU marginalised between the United States and China, and the EU as a 'normative balancer' or third pole. These scenarios are not mutually exclusive in a strict sense, since elements of each can be seen in the contemporary evidence, but they do represent genuinely different equilibria towards which current trends could converge, and it is necessary to distinguish them clearly before this thesis can offer a defensible answer to its own central research question. The three scenarios set out

²⁰¹ European Council on Foreign Relations, Ángel Melguizo, (2025). “*Deep pockets, DeepSeek, and the EU’s digital drift*” [online] Available at: <https://ecfr.eu/article/deep-pockets-deepseek-and-the-eus-digital-drift/>

²⁰² Carnegie Endowment for International Peace, Raluca Csernatoní, (2025). “*The EU’s AI Power Play: Between Deregulation and Innovation*” [online] Available at: <https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation>

below are therefore reconstructions of arguments already advanced in the specialist literature, and each is attributed to the scholars and analysts who defend it, rather than an autonomous forecast offered by this thesis.

Scenario (a): EU as Global Regulatory Leader

The optimistic scenario holds that the comparative advantage of the EU in rule-making, rather than being a second-best substitute for the industrial capability it lacks, is in itself enough to secure lasting geopolitical relevance, especially if the Union takes the opportunity created by the absence of regulation elsewhere. Alberto Alemanno, whose critique of the deregulatory turn was discussed in section 2.1, belongs to this camp, since his objection to the simplification agenda rests precisely on the premise that regulation is the instrument through which the Union exercises global influence, so that weakening it would mean forfeiting the only leadership position the EU currently occupies²⁰³. The ECFR analyst Herman Quarles van Ufford puts this position directly: 'While the US administration dodges regulation in the name of innovation, the real problem is the lack of common rules. Europe has an opportunity to set the standard - if it's bold enough to take it'²⁰⁴. This framing is consistent with an older but still influential CSIS analysis, which argued that the EU and the United States needed to 'agree on a basic framework of topline, democratic, regulatory principles for AI that can be promoted with trading partners' in order to counter China's 'intrusive model of data governance', and which therefore presented the European regulatory template as a leadership tool for the wider democratic bloc and not only for the EU²⁰⁵. ECFR's own institutional framing reinforces this reading, describing the EU as 'often described as a "regulatory superpower" benefitting from the so-called "Brussels effect"', with the AI Act cited as its leading contemporary example²⁰⁶. Read against the findings of section 3.1, this scenario is not implausible, but it depends on a condition that the evidence gathered above shows to be far from automatic: it requires the EU to strengthen, and not merely

²⁰³ Alemanno, A., (2025). "*The Dark Side of EU Deregulation*", February 2025; see also Alemanno, A., (2020). "The European Response to COVID-19: From Regulatory Emulation to Regulatory Coordination?", *European Journal of Risk Regulation*, 11(2), pp. 307-316.

²⁰⁴ European Council on Foreign Relations, Herman Quarles van Ufford, "Regulate or stagnate: Why the EU must lead on AI," cited in (2025). ECFR, "*Technology and Information*" [online] Available at: <https://ecfr.eu/category/digital/>

²⁰⁵ Center for Strategic and International Studies, (2021). "*AI Regulation: Europe's Latest Proposal is a Wake-Up Call for the United States*" [online] Available at: <https://www.csis.org/analysis/ai-regulation-europes-latest-proposal-wake-call-united-states>

²⁰⁶ European Council on Foreign Relations, (2021). "*The geopolitics of technology*", podcast description [online] Available at: <https://ecfr.eu/podcasts/episode/geo-tech-politics-why-technology-shapes-european-power/>

defend, the diffusion mechanisms that critics have found wanting, and to do so precisely in the window opened by the deregulatory turn documented in Washington.

Scenario (b): EU Marginalised Between the United States and China

The pessimistic scenario holds, on the contrary, that the capability deficits documented in section 3.2 are decisive, and that regulatory activity, however sophisticated, cannot compensate for the absence of industrial and military weight in an international system that is increasingly organised around raw technological capacity. Carnegie's Csernatoní warns that, without structural reform, 'the union risks becoming little more than a footnote in a global market dominated by the United States and China'²⁰⁷, and ECFR's Ángel Melguizo makes a similar diagnosis when he describes the EU as 'a cautious spectator' while 'the US and China are racing to dominate artificial intelligence', with European firms 'absent from this technology race' altogether²⁰⁸. Euronews reporting from January 2026 backs up this diagnosis empirically, finding that 'the European Union is losing the global "AI race" on nearly every key metric except regulation' and citing policy fragmentation across twenty-seven member states, talent flight and shortfalls of capital²⁰⁹, while TRT World similarly observes that 'Europe is not absent from the AI race, but it is weaker than its political rhetoric suggests', because 'even if European companies develop strong models, the underlying training infrastructure, chips, and cloud capacity often remain under the control of non-European companies'²¹⁰. A speculative but rhetorically influential scenario paper, 'Europe 2031', illustrates this trajectory by imagining a Europe whose economy is 'in disarray due to its lack of a homegrown AI infrastructure', hit by 'rising populism, a faltering euro, and rampant cyber-attacks'. This is deliberately a cautionary illustration, used to argue for urgent European technological independence, and not a literal forecast²¹¹. The scenario is directly consistent with the review of capabilities in section 3.2: if compute dependency, defence fragmentation and the absence of European frontier-AI firms persist or become worse, the regulatory activity of the EU, however influential in narrow legal

²⁰⁷ Carnegie Endowment for International Peace, Raluca Csernatoní, (2025). "*The EU's AI Power Play: Between Deregulation and Innovation*" [online] Available at: <https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation>

²⁰⁸ European Council on Foreign Relations, Ángel Melguizo, (2025). "*Deep pockets, DeepSeek, and the EU's digital drift*" [online] Available at: <https://ecfr.eu/article/deep-pockets-deepseek-and-the-eus-digital-drift/>

²⁰⁹ Euronews, (2026). "*AI power play: Can Europe catch up with the US and China?*" [online] Available at: <https://www.euronews.com/my-europe/2026/01/27/the-ai-race-can-europe-catch-up-to-the-us-and-china>

²¹⁰ TRT World, (2026). "*The AI divide: US-China dominance and the rest of the world*" [online] Available at: <https://www.trtworld.com/article/c0ac3b3826d5>

²¹¹ Cited in The Guardian, (2026). "*As the US and China surge ahead, is Europe sleepwalking into AI disaster?*" [online] Available at: <https://www.theguardian.com/technology/2026/jun/20/europe-sleepwalking-ai-disaster-us-china>

terms, would increasingly look like governance over a domain that the Union itself does not control industrially.

Scenario (c): EU as 'Normative Balancer'

The third scenario takes an intermediate position, and treats the EU neither as an emerging regulatory superpower nor as an inevitable casualty of the competition between the United States and China, but as a different kind of actor whose influence comes precisely from its position between the two dominant poles. The ECFR paper of 2021 by Ulrike Franke and José Ignacio Torreblanca presents this position as the likely default outcome for the Union if it does not act decisively, warning that 'if the EU wants to be more than a mediator between the two real technological powers, the United States and China, it will need to change its mindset'²¹². Carnegie's Csernatoní offers the most developed contemporary version of this 'balancer' role for the specific case of AI, calling on the EU to pursue 'a dynamic third pathway' that balances 'innovation and regulation', 'strategic autonomy and democratic oversight' and 'civilian and military AI governance', on the basis that 'regulating AI models is fundamentally about regulating unchecked power'²¹³. Csernatoní is careful to specify that this balancer role is neither costless nor self-sustaining, since the 'regulatory credibility' of the EU 'depends on coupling effective governance with an ambitious industrial policy', which implies that the balancer position depends on investment and regulatory action together and is not available through regulation alone²¹⁴. A related ECFR-edited volume, 'Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry', frames the ambition of the EU directly as a transition from being a pure 'rulemaker' towards 'superpower' status while navigating between the United States and China, and this normative-balancer framing has become a recurring reference point in the wider ECFR programme on technology and geopolitics²¹⁵.

The most recent expert commentary, from late 2025 and the first half of 2026, converges on the view that none of these three scenarios is locked in at present, and that the trajectory of the

²¹² European Council on Foreign Relations, Ulrike Franke and José Ignacio Torreblanca, (2021). "*Geo-tech politics: Why technology shapes European power*" [online] Available at: <https://ecfr.eu/wp-content/uploads/Geo-tech-politics-Why-technology-shapes-European-power.pdf> [

²¹³ Carnegie Endowment for International Peace, Raluca Csernatoní, (2025). "*The EU's AI Power Play: Between Deregulation and Innovation*" [online] Available at: <https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation>

²¹⁴ Ibid.

²¹⁵ European Council on Foreign Relations, Carla Hobbs (ed.), "Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry," cited in (2021). *ECFR podcast, "The geopolitics of technology"* [online] Available at: <https://ecfr.eu/podcasts/episode/geo-tech-politics-why-technology-shapes-european-power/>

EU remains genuinely contested and dependent on policy. ECFR's Giorgos Verdi argues that the Union 'will need a more ambitious AI Continent Action Plan to catch up to its tech rivals', which implies that current policy, although moving in the right direction, is still insufficient to secure a leadership trajectory without a further increase in investment²¹⁶. ECFR's José Ignacio Torreblanca warns explicitly of 'techno-imperialism', arguing that 'US tech giants are preparing to test the EU's resolve, emboldened by support from the Trump administration', and that the Union 'will need to prepare itself for the inevitable clash to safeguard its democratic and technological future'²¹⁷. This framing implicitly rejects the assumption that European leadership, or even successful balancing, will come about automatically, and insists instead that the Union has to resist marginalisation actively. This warning has since been at least partly borne out, since the clash Torreblanca anticipated has in fact begun to take shape, both in the pressure exerted on European digital enforcement during 2025 and 2026 and in the decision of the Commission itself, through the Digital Omnibus discussed in section 2.2, to postpone and soften parts of the AI Act. A joint ECFR paper by Torreblanca and Verdi, 'Control-Alt-Deliver: A digital grand strategy for the European Union', states plainly that 'the EU is falling behind the US and China in the digital realm' and 'urgently needs a new agenda combining innovation, security, and influence for an age of geopoliticised technology'²¹⁸. As a sign of how live this debate still is, Bruegel convened a closed-door expert event, 'Europe's policy options for AI in the midst of US-China strategic competition', on 22 June 2026 in Brussels, which shows continuing think-tank engagement with exactly this question in the period when this thesis was written²¹⁹. The World Economic Forum, in May 2026, complicates all three scenarios further by arguing that 'the AI race is shifting to power', meaning that the competition is increasingly about energy and compute infrastructure and not only about regulation²²⁰. This last point applies with particular force to the pure 'regulatory leader' scenario, because it suggests that even a successful diffusion of rules may become progressively less relevant if the underlying

²¹⁶ European Council on Foreign Relations, Giorgos Verdi, "Back to the future: How the EU can upgrade its AI Continent Action Plan," cited in (2025). ECFR, "*Technology and Information*" [online] Available at: <https://ecfr.eu/category/digital/>

²¹⁷ European Council on Foreign Relations, José Ignacio Torreblanca, "Big tech, Donald Trump, and "techno-imperialism": How Europe can avoid becoming a digital colony," cited in (2025). ECFR, "*Technology and Information*" [online] Available at: <https://ecfr.eu/category/digital/>

²¹⁸ European Council on Foreign Relations, José Ignacio Torreblanca and Giorgos Verdi, "Control-Alt-Deliver: A digital grand strategy for the European Union," cited in (2025). ECFR, "*Technology and Information*" [online] Available at: <https://ecfr.eu/category/digital/>

²¹⁹ Bruegel, (2026). "*Europe's policy options for AI in the midst of US-China strategic competition*" [online] Available at: <https://www.bruegel.org/event/europes-policy-options-ai-midst-us-china-strategic-competition>

²²⁰ World Economic Forum, (2026). "*The AI race is shifting to power — and Europe faces a new test*" [online] Available at: <https://www.weforum.org/stories/2026/05/the-ai-race-is-becoming-a-race-to-power-and-europe-faces-new-test/>

contest moves onto a terrain, energy and compute, where the deficits of the EU documented in section 3.2 are most serious. A more optimistic analysis of October 2025 presents the opposite possibility, arguing that '2025 marks the start of Europe's strategic counteroffensive' and reading the AI Continent Action Plan and InvestAI as the attempt of the EU to move explicitly from 'dependency' to 'sovereignty'²²¹, which shows that the framing based on leadership and sovereignty still has active supporters even alongside the warnings about marginalisation reviewed above.

²²¹ European Economics, (2025). “*Europe’s AI journey: From dependency to sovereignty*” [online] Available at: <https://www.europeaneconomics.com/en/europe-s-ai-journey/>

Conclusion

The analysis developed across this chapter now allows a direct answer to the question that has structured Chapter III as a whole, and that is the analytical core of this thesis. Posed in its simplest form, whether the governance of artificial intelligence is sufficient to make the European Union a relevant geopolitical actor in the technological domain, the question largely answers itself, and it becomes analytically productive only once it is reformulated in conditional terms: through which mechanisms, under which conditions and within which limits can regulatory power be converted into geopolitical relevance, and what follows for the Union when those conditions are satisfied only in part? The answer defended here is a qualified one. AI governance on its own is not sufficient, but it is not irrelevant either, and the correct description of the position of the EU is closer to Csernatori's 'dynamic third pathway' than to either of the two polar scenarios examined above, provided that this pathway is understood as a precarious equilibrium and not as a stable resting point.

Three considerations support this conclusion. First, section 3.1 showed that the Brussels Effect, which is the main mechanism by which regulation is supposed to become influence, works only partially and conditionally in the AI domain: real diffusion exists, but it is selective, it is often limited to vocabulary rather than to substantive enforcement, and it is exposed to the divisibility of AI applications in a way that the GDPR was not. Regulatory power, in other words, is real but bounded, and that boundedness is not a temporary implementation problem but a structural feature of AI as an object of regulation. Second, section 3.2 showed that the underlying capability base of the EU, in defence, in compute and cloud infrastructure and in frontier AI development, remains critically dependent on the United States in particular, and that recent investment programmes are only beginning, slowly and unevenly, to address this dependency. A regulatory model without a matching capability base is inherently exposed to the risk that its normative claims will be seen, by allies and rivals alike, as not backed by material weight, which is precisely the danger that Melguizo and Csernatori identify from different angles. Third, and most importantly, these two considerations are not independent of each other: the credibility of European regulatory diffusion, discussed in section 3.1, depends significantly on the demonstrated capability and enforcement capacity of the Union, discussed in section 3.2, because third countries and firms calibrate their compliance with European rules partly on the basis of how seriously, and how consistently, the EU itself can enforce them. This link is made explicit by the finding that 'the de jure Brussels effect relies to a significant extent on the de facto effect'.

This interdependence between regulatory power and material power is the most important analytical conclusion of this thesis. The European Union has not failed to become a geopolitical actor in the technological domain; it has become a specific and historically distinctive kind of actor, whose power is real and is exercised mainly through law and standard-setting, but which remains dependent on capability investments that are still incomplete. Whether the EU moves towards the scenario of regulatory leadership or drifts towards marginalisation over the coming decade will therefore be decided less by the sophistication of its legislative drafting, which is already considerable, than by whether the AI Continent Action Plan, InvestAI, the Cloud and AI Development Act and the measures that follow them succeed in closing the gaps in compute, cloud and industrial capacity documented in this chapter. Regulation has bought the European Union a seat at the table of global AI governance, but it has not yet bought it a comparable seat at the table of AI production. Until that second seat is secured, the geopolitical relevance of the Union in the technological domain will remain real, consequential and thoroughly incomplete, that of a normative balancer as much by necessity as by design, whose final trajectory remains, as the evidence reviewed throughout this chapter makes clear, still to be written.