Executive Order 14110 Governing Artificial Intelligence: Technological Leadership and Regulatory Challenges in an Era of Exponential Growth

di Ciro Sbailò

Abstract: *L'Executive Order 14110 sulla regolazione dell'intelligenza artificiale: leadership tecnologica e sfide regolatorie in un'era di crescita esponenziale* –Joe Biden's Executive Order 14110 addresses Artificial Intelligence governance at a critical "technological inflection point," a term Biden uses to describe historical moments marked by rapid technological and geopolitical change. Building on Donald Trump's initial impetus with EO 13859 in 2019, which launched the American AI Initiative and promoted public-private cooperation to establish U.S. technological leadership, Biden's EO 14110 introduces further, more specific requirements for privacy, security, and civil rights. It lays out approximately 150 concrete actions across over 50 federal agencies, strengthening the United States' role as an ethical and technological leader on the global stage. This regulatory acceleration addresses the rapid advancement of AI, which has outpaced institutional capacity for adaptation, creating a growing gap between innovation and regulation. In this context, the concept of "super-cognition" – a synergy between human intelligence and machine learning – is essential, enhancing decision-making in defense and security sectors. While Europe adopts a prescriptive regulatory approach, the United States favors greater flexibility, aiming to foster responsible innovation without excessive limitations. Despite these differences, cooperation between the United States and Europe is crucial to creating shared AI governance and jointly addressing the challenges posed by AI, promoting a global, responsible approach to innovation and security.

Keywords: Artificial Intelligence, Technological Leadership, Regulatory Challenges, Global Governance.

1. Introduction: from Trump's initial impetus to Biden's vision of a technological inflection point

Executive orders (EOs) are essential instruments through which U.S. Presidents manage federal operations and direct the actions of government agencies, often addressing innovative and complex topics such as Artificial Intelligence (AI). These executive orders, signed and issued by the President, hold binding authority over federal agencies, although they do not constitute laws passed by Congress. In the context of AI regulation, EOs are particularly effective, as they allow for the rapid establishment of priorities and standards in this rapidly evolving field, often anticipating legislative processes. Among the most significant EOs in AI policy, three

DPCE online
ISSN: 2037-6677

orders outline a distinct and progressive trajectory. In 2019, Donald Trump issued EO 13859 *Maintaining American Leadership in Artificial Intelligence* – a foundational directive that established the American AI Initiative and set the groundwork for U.S. technological leadership.

This EO promoted AI growth, emphasizing research and innovation, workforce training, and the protection of advanced technologies, fostering an ecosystem in which public and private sectors collaborate flexibly to advance AI. In 2020, Trump further strengthened the framework with EO 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, focusing on promoting reliable AI use within the federal government. Finally, in 2023, Joe Biden signed EO 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, one of the most comprehensive orders to date, with approximately 150 concrete actions assigned to over 50 agencies.

This EO aims to protect privacy, ensure security, and promote the global competitiveness of the United States in AI. Biden followed Trump's flexible framework but added strict regulatory requirements and safety standards, positioning the United States as a secure and ethical leader on the international stage. Executive orders are particularly well-suited to addressing the challenges posed by technological advancement, as today, rapid response capability is an essential aspect of political decision-making. Indeed, it is widely recognized that we are at a historical moment defined by a paradigmatic crisis fueled by the relentless advance of Artificial Intelligence (AI).

This emerging technology is rapidly transforming our societies, impacting not only the economic sphere but also security, communication, and the dynamics of daily life. However, the primary challenge lies not so much in technological progress itself but in the capacity – or perhaps incapacity – of political and legal institutions to adapt and govern this change effectively. The pace at which AI evolves far exceeds the rate at which institutions can respond, creating what could be termed a crisis of transition, similar to the "period of crisis" described by Thomas Kuhn in his studies on paradigm shifts.[1]

This need for specific responses to global technological challenges finds explicit recognition in Executive Order 14110, which can best be understood by referring to the concept of a "technological inflection point." Frequently invoked by President Joe Biden in his speeches and strategic documents, this term highlights crucial moments of decision in global history, when challenges such as the crises in Ukraine, tensions with China and Russia, and the growing threats to democracy emerge. However, Biden's repeated invocation of the concept of an "inflection point" has faced criticism. Some[2] argue that, while he connects various global events under this

[1] T. S. Kuhn, *The Structure of Scientific Revolutions*, Chicago, 1962. For a recent critical overview, see: C. Bartocci and G. Giorello, Introduction to Kuhn's essays in *La tensione essenziale: tradizione e innovazione nella ricerca scientifica*, Torino, 2006.

[2] Among various critiques of Biden's rhetoric on 'inflection points', see, for example, M. Hirsh, *Biden's 'Inflection Points' Don't Add Up*, in *Foreign Policy*, October 20, 2023. Accessed at foreignpolicy.com. Among numerous articles examining President Biden's Executive Order 14110 on Artificial Intelligence, Brian Connor's piece, *Examining the New Artificial Intelligence Executive Order*, published by MITRE Corporation (2024),

framework, these links may appear contrived, potentially obscuring their practical implications.

This use of "inflection point" is seen by critics as more rhetorical than strategic, risking a lack of clarity in conveying cohesive policy guidance. Despite these and other criticisms, Biden's references to the concept of an "inflection point" reflect a growing awareness within American political circles of the gap between rapid technological advancements and the slower pace of institutional governance. This issue has found some of its more radical expressions in the theories of Ray Kurzweil, who posits that technological progress is accelerating exponentially, thereby widening the "exponential gap" between technology and governance. According to Kurzweil, this acceleration in technology creates a critical discrepancy, leaving political and social institutions struggling to adapt quickly enough. Unchecked, this gap could lead to systemic vulnerabilities across social, economic, and political structures. Although it is highly unlikely that Biden shares Kurzweil's radical vision — which has, moreover, sparked widespread debate and critique, especially regarding the concept of "technological singularity"[3] — he nonetheless acknowledges the real issue of the

provides an overview of the EO's key provisions. The order directs various federal departments, including the Department of Commerce and the Office of Management and Budget, to prioritize AI security, regulation, and civil rights. Connor highlights the EO's potential industry impact, noting Microsoft's supportive response alongside constructive criticism from groups like NetChoice. Similarly, Aram Gavoor, in *Structural Challenges Loom for Biden's Executive Order on Artificial Intelligence*, published by George Washington University's Regulatory Studies Center (November 8, 2023), addresses structural challenges in the EO's implementation, such as interagency coordination issues and the shortage of AI experts within the public sector, which may complicate the regulatory landscape for new entrants. Janet Egan and Diletta Milana, in *Action on AI: Unpacking the Executive Order's Security Implications and the Road Ahead*, published by the Belfer Center at Harvard Kennedy School (November 2023), explore the EO's approach to dual-use AI risks and its bolstering of U.S. technological leadership, particularly in terms of international cooperation and security. Another valuable resource is the Center for Security and Emerging Technology (CSET) report from Georgetown University, *The Executive Order on Safe, Secure, and Trustworthy AI: Decoding Biden's AI Policy Roadmap* (November 2023), which offers a detailed guide and a "tracker" to monitor federal agency progress on the EO's timelines, enhancing understanding of the evolving U.S. regulatory framework for AI.

[3] Ray Kurzweil's concept of "accelerating returns", as outlined in his influential book *The Singularity is Near: When Humans Transcend Biology* R. Kurzweil, New York, 2005, forecasts a transformative future where rapid advancements in fields such as AI, biotechnology, and computing lead to a "singularity." According to Kurzweil, this singularity will arrive when Artificial Intelligence surpasses human intelligence, fundamentally reshaping society and challenging existing structures. His ideas on exponential technological growth and the resulting gap between innovation and societal preparedness are now central to debates on governance and regulatory approaches in this fast-evolving age. Critiques of Kurzweil's theories highlight the limitations and potential risks of his technological optimism. Melanie Mitchell in M. Mitchell, *Artificial Intelligence: A Guide for Thinking Humans*, New York, 2019, critiques Kurzweil's projections, emphasizing the practical and ethical challenges that such exponential growth entails. Additional analyses, such as the one of D.J. Chalmers in D.J. Chalmers, *The Singularity: A Philosophical Analysis*, in 17 *Journal of Consciousness Studies* 7 (2010) and of N.K. Hayles, in N.K. Hayles, *Computing the Human*, in 22(1) *Theory, Culture and Society* 131 (2005), explore the philosophical and cultural impacts of

DPCE online
ISSN: 2037-6677

"governance gap", which arises whenever institutions struggle to effectively regulate new technologies. In this context, the Biden administration's efforts can be seen as part of a broader push—often advocated by top intelligence officials—for a holistic approach to these emerging threats. Put simply, this means an approach that can continuously regenerate itself in response to the evolving nature of these challenges, without being overly concerned with drawing sharp distinctions between military and civilian matters, foreign policy and defense, social security, or public order.

Evidently and inevitably, we are faced with a work in progress. On October 24, 2024, the Biden administration issued the *Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence*, a strategic document aimed at reinforcing the United States' global leadership in Artificial Intelligence (AI), particularly within national security.[4] This memorandum introduces several significant updates compared to the prior Executive Order 14110 issued in October 2023, with a focus on frontier AI models and detailed goals to accelerate American technological development. As Biden stated, "The United States must lead the world in the responsible application of AI to appropriate national security functions. Unlike the previous executive order, which primarily addressed traditional AI applications developed from 2012 to 2022, this memorandum emphasizes advanced frontier models like OpenAI's ChatGPT and Google's Gemini, which possess greater capacity and versatility across various applications.

The Biden administration highlights the strategic importance of maintaining leadership in these technologies to ensure national security and to establish global governance standards in collaboration with international allies. The *Memorandum* also introduces innovative measures to attract international talent in the AI sector, prioritizing visa facilitation as a matter of national security and proposing a significant infrastructure expansion to support the development and adoption of advanced technologies.

Additionally, it underscores the need to protect American intellectual property against external threats by intensifying counterintelligence efforts and positioning the AI sector as a key component of national security strategy. In summary, the memorandum outlines a strategy that not only leverages AI's potential for national security but also solidifies the United States' position as a global leader in developing ethical and secure standards for AI use, promoting democratic values and establishing a framework for international collaboration.

Kurzweil's vision, focusing on human identity and the complex societal adjustments required. These critiques provide a more nuanced perspective on Kurzweil's theories, balancing his future-oriented optimism with the practical and ethical considerations that his vision entails.

[4] For an initial assessment of the memorandum, see G. C. Allen and I. Goldston, *The Biden Administration's National Security Memorandum on AI Explained, Center for Strategic and International Studies* (CSIS), October 27, 2024, https://www.csis.org, and J. Woo, *National Security Memorandum: Biden Administration's New AI Guidance, Just Security*, October 25, 2024, https://www.justsecurity.org.

2. Legal framework and regulatory challenges

The Executive Order sets out a clear regulatory framework for AI governance, emphasizing transparency, accountability, and respect for civil rights. It mandates strict testing and monitoring of AI systems to ensure compliance with federal laws and requires agencies to publish periodic reports on the status of AI use. Transparency in AI applications across sectors is crucial for public trust, especially in areas like healthcare and law enforcement, where decisions directly affect people's lives.

Federal agencies are tasked with implementing AI in accordance with privacy laws and monitoring its impact on public services. Additionally, the order emphasizes investment in AI professionals' training and certification to ensure they adhere to legal and ethical standards, especially in critical sectors like healthcare, security, and justice. This focus on ethical compliance is vital, as the deployment of AI in high-risk areas without adequate safeguards could result in significant harm.

One of the major regulatory challenges involves keeping pace with the rapid development of AI technologies. Policymakers must constantly adapt to the evolving landscape of AI, where new applications and innovations emerge at an unprecedented rate. This requires an agile regulatory framework capable of responding to unforeseen developments, such as the rise of generative AI models that can produce human-like text or images, which present unique challenges in terms of misinformation, bias, and intellectual property rights.

3. Objectives and core principles of EO 14110

Executive Order 14110 outlines a comprehensive and structured approach to the management and implementation of Artificial Intelligence technologies in the United States, with a particular focus on governance, security, and socioeconomic impact. Among its key elements is the role of generative AI, which includes advanced tools such as large language models and generators of synthetic content (text, images, code).

The executive order also emphasizes the effective management of algorithmic bias and the need to ensure transparency and fairness through the creation of *AI Governance Councils* within federal agencies.

In parallel, it introduces the position of *Chief Artificial Intelligence Officer*, responsible for coordinating the safe and responsible use of AI.

Another crucial point is the integration of Privacy-Enhancing Technologies (PET), such as differential privacy, aimed at mitigating the risks associated with the mass collection and use of personal data, especially in government applications. Furthermore, the executive order highlights the central role of infrastructure and AI in transportation, managed by agencies like ARPA-I, underscoring the importance of improving autonomous mobility ecosystems.

Advanced communication networks, such as 6G and Open RAN, also benefit from AI to enhance spectrum efficiency and security.

The order also calls for the creation of an *AI toolkit for education*, aimed at ensuring the safe and non-discriminatory use of AI in schools.

DPCE online
ISSN: 2037-6677

In summary, EO 14110 adopts an integrated approach that balances the promotion of technological innovation with strict measures of security, transparency, and civil rights protection, while ensuring the development of a workforce capable of meeting the challenges posed by AI.

The fundamental objectives of EO draw an octagon.

- Security of AI Systems: Stringent security measures are essential to prevent misuse and safeguard against the dual-use nature of AI technologies. This includes ensuring that AI developed for civilian purposes does not serve military or malicious goals, especially in the realm of cyber warfare and national defense.
- Responsible Innovation: A collaborative ecosystem between government, the private sector, and academic institutions fosters sustainable, transparent innovation. This requires careful coordination and the establishment of ethical standards that prevent monopolization and promote fair competition.
- Worker Protection: The order emphasizes reskilling initiatives aimed at mitigating the impact of automation on jobs. In doing so, it seeks to open new opportunities in a digital economy, ensuring that AI-driven innovation does not result in mass unemployment or socioeconomic disparity. A just transition is critical for maintaining social stability in the face of technological disruption.
- Equity and Civil Rights: Ensuring that AI does not perpetuate biases is paramount. Inclusive algorithm development and robust controls to prevent discrimination are at the heart of EO 14110's principles. AI systems must be designed to promote fairness and avoid systemic inequalities in sectors like finance, healthcare, and criminal justice.
- Consumer Protection: Compliance with consumer protection regulations is non-negotiable, particularly in critical sectors such as healthcare and finance. This principle ensures that AI technologies are used responsibly to avoid fraud and protect sensitive personal data.
- Privacy: Advanced standards for handling personal data in accordance with existing privacy laws are a cornerstone of EO 14110. Protecting privacy in the age of AI is a multifaceted challenge, as AI systems increasingly rely on vast datasets that include sensitive personal information. Safeguarding this data while ensuring that AI models remain effective is one of the order's core concerns.
- Government Use of AI: Federal agencies must adopt AI ethically and transparently, ensuring security and civil rights protections while enhancing the efficiency and transparency of government processes. This involves creating clear guidelines for how AI is used within the public sector, ensuring that it benefits society without overstepping ethical boundaries.

The length of this octagon that seems to me more marked is *Global Leadership*: The U.S. must maintain its leadership in AI by shaping international standards for responsible technology use. By fostering international cooperation, the U.S. can ensure that AI is developed and deployed in a manner that respects human rights, promotes fair competition, and supports innovation across borders.

4. An integrated strategy for middle-class protection in the AI era

The impact of Artificial Intelligence extends well beyond security and hybrid warfare, reaching every dimension of modern society. The Biden administration has responded to these complex challenges with a holistic approach to safeguarding workers, consumers, and, especially, the middle class—the backbone of American society, as highlighted by Tocqueville. Recognizing this group's central role in maintaining social stability and economic prosperity, Biden's strategy addresses both the benefits and risks of AI with the middle class in mind.

The middle class is, however, under pressure. From 1970 to 2023, the percentage of Americans in the middle class fell from 61% to 51%, while income shares for high- and low-income households increased, reflecting a growing economic divide.[5] This trend has drawn significant attention, with political figures like Trump and Harris emphasizing the importance of protecting and revitalizing the middle class in their campaigns. Biden's approach echoes this focus, seeking to mitigate the disruptive effects of AI on this demographic, which is particularly vulnerable to automation, biased decision-making, and privacy violations.

The Executive Order's flexibility supports AI regulation that not only addresses technical issues but also adapts to broader societal needs, acknowledging the threats of disinformation, automated decision-making, and social and political manipulations. This integrated response is structured around three core objectives:

(a) *Worker Protection and Prevention of Discrimination*

Protecting workers from AI-driven automation is central to Biden's strategy. The federal government is tasked with tracking AI's impact on the labor market and implementing reskilling programs to help workers adapt to the digital economy. The middle class, particularly blue-collar and service sector workers, faces the highest risk of job displacement due to automation. By prioritizing worker protection, Biden's approach aims to prevent further erosion of economic security for middle-class workers, who already face increasing precarity. Additionally, the administration underscores the

[5] The Pew Research Center report, *The State of the American Middle Class* (2024), examines changes in the U.S. middle class from 1970 to 2023 using data from the U.S. Census Bureau. Over recent decades, the percentage of Americans in the middle class has decreased from 61% to 51%, while both low- and high-income groups have grown. The vulnerability of the middle class is particularly evident in the widening income gap compared to high-income groups. This economic polarization highlights slower income growth within the middle class and a declining share of total national income. See Pew Research Center, *The State of the American Middle Class: Who is in it and Key Trends from 1970 to 2023*, by R. Kochhar, Washington, D.C., May 31, 2024, www.pewresearch.org. In the United States, the issue is also the subject of attention in the military, especially by socially engaged ex-soldiers. See, for example, the work of Jack Gardner, a retired Lieutenant General in the United States Army and founder of the 21st Century Jobskills Project. Gardner argues that the fragility of the American middle class represents not only an economic challenge but also a threat to national security. According to Gardner, declining economic mobility and social stability reduce trust in institutions and destabilize the democratic fabric, necessitating coordinated and bipartisan intervention. See J. Gardner, *National Security and the Middle Class*, *HP3*, January 16, 2023, realcleardefense.com.

DPCE online
ISSN: 2037-6677

importance of ensuring fairness in crucial areas such as employment and finance.

(b) *Consumer and Privacy Protection*

AI's rise brings significant privacy concerns, particularly for middle-class Americans, who are more susceptible to breaches of personal data. Biden's strategy mandates strict privacy standards for federal agencies, ensuring that AI technologies comply with laws like the Privacy Act of 1974. In sensitive sectors such as healthcare and finance, these protections are essential for fostering public trust.

Rigorous testing and transparency in AI systems are essential to prevent misuse, offering protection for middle-class Americans.

(c) *Global Leadership and International Cooperation*

To position the U.S. at the forefront of global AI governance, Biden emphasizes international cooperation on ethical AI standards.

This leadership ensures that American workers, particularly in the middle class, are not left behind in the competitive global tech landscape. The administration's commitment to equitable sharing of AI benefits aims to secure American workers' interests in an interconnected world.

Together, these three elements—worker protection, consumer and privacy safeguards, and global leadership—form Biden's holistic approach, designed to manage AI's risks while fostering its benefits. Despite this ambitious plan, questions remain about whether this approach will sufficiently address AI's systemic challenges for the vulnerable middle class. The rapid pace of technological evolution and the complexity of hybrid threats make it difficult to predict whether this strategy will remain adaptable and sustainable. While Biden's approach is a proactive step, the real test will be whether the administration can keep pace with AI's developments and the uncertainties they bring.

5. Bridging the gap between technology and law: a comparative analysis of U.S and EU artificial intelligence regulation

To get a comprehensive view of AI regulation between the United States and the European Union, a synchronic and diachronic comparison could be useful. Since Trump's main executive orders have already been discussed, a focus on the regulatory developments promoted by the Biden administration is suggested here, which introduce, as mentioned above, additional and more specific requirements. This two-pronged approach allows you to examine the historical evolution and interactions between key regulatory documents: the GDPR of 2018, the European Union's AI Act of 2021, the Blueprint for an AI Bill of Rights of 2022, and EOs 14086 and 14110 of 2022 and 2023. These documents highlight the differences and similarities between the two legal systems, highlighting how shared governance can generate regulatory overlaps in a constantly and rapidly evolving field such as Artificial Intelligence.[6]

[6] For an initial overview, see M. Bassini, *The Global Race to Regulate AI: Biden's Executive Order Spillover Effects on the EU AI Act*, iep.unibocconi.eu, October 30, 2023. This article examines Executive Order 14110 as a U.S. tool for technological leadership, contrasting it with the EU's risk-based regulatory approach in the proposed AI Act and

The GDPR, while not specifically targeting AI, serves as a foundation for personal data protection in Europe. Its significance lies in its capacity to set high standards for data processing, extending its reach to external actors via the so-called "Brussels Effect." The increasing reliance of AI on personal data means that GDPR provisions directly affect the AI ecosystem, limiting illegal processing and ensuring respect for citizens' fundamental rights. This rigorous approach has influenced regulations in other jurisdictions, particularly those aiming to operate in the European market, posing a significant challenge for global tech companies.

Complementing this regulatory framework, the EU proposed the AI Act in 2021, which introduces specific regulation for AI systems.

This Act classifies AI applications according to their level of risk, imposing stringent requirements on those deemed high-risk. The European regulatory approach, consistent with the GDPR, aims to safeguard fundamental rights while fostering responsible innovation. Thus, it creates a regulatory framework that seeks to balance AI adoption with individual protection, reflecting a philosophy that views technology as a tool to be controlled to prevent social or economic harm.

In the U.S., the Blueprint for an AI Bill of Rights, published in 2022, outlines a similar theoretical approach, but with a crucial difference: it lacks the force of law. This document represents a set of guiding principles for future regulation, where the protection of individual rights is central to AI policy. However, the absence of concrete regulatory constraints reflects a more flexible approach compared to the European one, which favors stringent rules for high-risk applications from the outset.

Executive Order 14086, issued in 2022 in response to the Schrems II decision, fits within this framework with the goal of restoring trust in data transfer activities between the U.S. and Europe. The invalidation of the Privacy Shield highlighted gaps in U.S. personal data protection, emphasizing the need to strengthen safeguards for European citizens. This order introduces new protections for intelligence activities, focusing on personal data protection in transatlantic relations, contributing to a greater alignment between the two regulatory systems[7] in a domain of growing importance.

The final piece of this comparative analysis, Executive Order 14110 of 2023, represents a significant step toward AI regulation in the U.S. Unlike the European AI Act, which defines clear and detailed regulatory obligations, EO 14110 focuses more on general guidelines and flexible commitments, leaving more room for innovation. This highlights a fundamental philosophical divergence: while the European Union prefers a prescriptive and regulated approach, the U.S. leans toward a more fluid framework geared toward promoting technological innovation with fewer legal constraints.

---

discussing indirect political pressures on EU lawmakers regarding foundational AI models.

[7] For a detailed analysis of the convergences and divergences between EU and U.S. regulatory systems, and to understand the link between these issues and international security, see paragraph 3, *International Terrorism: Old Threat and New Patterns*, by A. Vedaschi, in A. Vedaschi, C. Graziani, *The American Presidency After Two Years of President Biden*, in *DPCE Online*, 2023, Special Issue 1, 209-234.

DPCE online
ISSN: 2037-6677

The interaction between these regulatory documents demonstrates that, despite significant differences in legal philosophies and regulatory goals, there are important points of convergence between the two systems. The protection of fundamental rights, on the one hand, and the promotion of innovation, on the other, represent two priorities that, if properly balanced, could lead to greater regulatory harmonization globally. In this sense, cooperation between the U.S. and the European Union will be crucial in addressing the common challenges posed by Artificial Intelligence. Dialogue between the two regulatory blocks could lead to the creation of a shared framework that not only safeguards individual rights but also promotes responsible and safe innovation in an era where emerging technologies continually redefine the boundaries of what is possible. The common theme across these documents, despite their different forms, is the shared intent to close the gap between technology and law within a democratic context. As Azeem Azhar points out,[8] the speed at which technologies like Artificial Intelligence are developing often outpaces the ability of regulatory systems to adapt. Both U.S. and EU regulations seek to address this gap, balancing technological innovation with the need to protect individual rights and ensure the ethical use of AI.

To conclude, while there are clear differences between the European and U.S. regulatory approaches, both respond to common challenges. The European Union adopts a more prescriptive and structured approach, while the United States favors strategic flexibility. Both systems, however, recognize the need for regulatory frameworks that accompany technological development, seeking to bridge the gap between the rapid pace of innovation and the capacity of legal systems to manage it. Differences in legal and structural nature underscore the importance of understanding how each system influences the governance and ethical use of AI technologies within its context.

[8] Azeem Azhar is a renowned technology analyst and author of the book *Exponential: How Accelerating Technology is Leaving Us Behind and What to Do About It* (New York, 2021). In Exponential, Azhar explores the concept of the "exponential age" — a period characterized by technologies advancing at exponential rates, leading to rapid and often disruptive changes in economies and societies. He delves into areas such as Artificial Intelligence, genomics, renewable energy, and other transformative technologies that, according to his analysis, are progressing far faster than society's ability to adapt. Azhar introduces the idea of the "exponential gap", which describes the widening discrepancy between the pace of technological progress and the slower adaptability of institutions, regulations, and infrastructures. This gap, he argues, represents one of the greatest challenges of our time. His insights draw on his extensive experience as a technology entrepreneur, investor, and innovation advisor, providing a uniquely informed perspective on the effects of exponential change. Azhar advocates for a proactive and collaborative approach to managing the impacts of technological growth, suggesting that governments, businesses, and citizens all have roles to play in bridging this gap. Sulla rilevanza di tale questione per il diritto pubblico comparato, cfr. C. Sbailò, *Perché l'Europa è condannata a vincere a vincere. Premessa allo studio delle ricadute del pensiero di Emanuele Severino nella dottrina giuspubblicistica*, in *DPCE Online*, 2020, 4, 4735-4780; C. Sbailò, *Europe's Call to Arms: Philosophical Roots and Public Law Profiles of the Confrontation With the Monster of the 21st Century: Westernization Without Democratization*, Baden-Baden, 2023, 15 ss.

6. Exponential development of artificial intelligence and hybrid warfare

In today's dynamic threat landscape, the pragmatic U.S. approach appears particularly well-suited to address new and unpredictable challenges. The flexibility of the Executive Order enables swift and adaptable responses, a crucial advantage in an era marked by rapid technological advancements and increasing geopolitical complexity.

The exponential growth of AI is transforming fields like healthcare and finance, as well as the nature of modern conflict.

AI now sits at the core of hybrid warfare, a sophisticated strategy that combines conventional military tactics with unconventional tools such as cyberattacks, disinformation, and economic sabotage. This type of warfare challenges traditional geopolitical concepts like sovereignty and jurisdiction, operating across physical, digital, and cultural dimensions.

A notable example is the 2007 cyberattack on Estonia, which paralyzed the nation's critical systems, illustrating the vulnerability of interconnected, advanced societies. The lesson learned is that even the most powerful democracies can be unprepared to confront the complexities of hybrid warfare. AI plays a dual role in this context: it is both a critical defense tool and a potential weapon. As AI advances, the attack surface—the interconnected devices and systems exposed to adversaries—continues to grow, offering new entry points for malicious actors. In his analysis, Azeem Azhar highlights the exponential pace of technological change, where each advancement accelerates further innovation. This rapid growth in AI technology amplifies both opportunities and risks, especially in hybrid warfare.

In the 2007 cyberattack on Estonia, coordinated digital strikes disabled the nation's critical infrastructure, a clear example of how AI-driven capabilities can exacerbate vulnerabilities. AI's predictive power in processing massive datasets enables more sophisticated military and intelligence operations. However, these same capabilities provide adversaries with new methods to destabilize societies without resorting to conventional warfare.

7. The role of AI in hybrid warfare: synergy and super-cognition

As hybrid warfare continues to reshape global security dynamics, the role of AI expands beyond conventional applications, merging into advanced strategies like super-cognition that amplify decision-making capabilities in real-time conflict scenarios.

This transition highlights the shift from the general impacts of AI to its specific, synergy-driven contributions in modern warfare. Since this change, AI's role in conflict has evolved into a synergy-based approach, known as "super-cognition," where human intelligence and machine learning converge to improve decision-making in complex scenarios.

"Super-cognition" refers to a combination of human intelligence and machine learning designed to optimize decisions in complex contexts.[9]

This combination has become an area of particular interest for intelligence communities, especially in the United States and Israel, as it allows them to address threats that traditional methods struggle to manage. Although EO 14110 does not explicitly address this issue, it is reasonable to assume that the drafters of the executive order were aware of its relevance.

Future efforts by the U.S. administration are likely to advance in this direction, as indicated by the previously mentioned *Memorandum*.

Through real-time data processing and hidden pattern detection, AI provides military and intelligence agencies with an unprecedented level of foresight. However, human oversight is essential to interpret AI-generated insights accurately, minimizing errors and ensuring that ethical and strategic goals are met. While AI is extraordinarily powerful in processing vast amounts of data rapidly, it is ultimately human judgment that guides decisions with responsibility and awareness.

This collaboration between human and artificial cognition represents a paradigm shift in the approach to conflicts, fostering an increasingly data-driven decision-making process. Nevertheless, the traditional reliance of Western democracies on conventional defense systems could pose significant risks. Without effectively integrating AI into national defense strategies, these systems may prove inadequate in responding to the emerging threats posed by hybrid warfare.

Consequently, there is a need for targeted political action to promote the integration of AI within defense strategies under democratic and political oversight. Only in this way can defense strategies effectively address the challenges of hybrid warfare while remaining aligned with democratic values and transparent public governance.

[9] See Brigadier General Y.S., *The Human Machine Team. How to Create Synergy Between Human & Artificial Intelligence That Will Revolutionize Our World*, eBookPro Publishing, 2021. The identity of the author, Yossi Sariel, an Israeli intelligence officer known as Brigadier General YS, was revealed on April 5, 2024 by *The Guardian*, which discovered his presence on public social media accounts and on a Jewish Wikipedia page, where he had shared his name and rank. The book explains how hybrid warfare represents one of the main threats related to the development of Artificial Intelligence (AI), which is rapidly changing the dynamics of international security and military operations. AI's ability to collect and process large amounts of data in a short time makes it possible to identify hidden threats and predict attacks, making the technology a crucial asset in hybrid warfare scenarios, where the distinction between war, terrorism and disinformation is becoming increasingly blurred. In the European context, these threats become more insidious due to political fragmentation and the lack of a unified response that makes it difficult to quickly coordinate and effectively protect against sophisticated attacks. As the text shows, hybrid warfare exploits the inherent vulnerabilities of interconnected systems, increased by the exponential growth of digital technologies and AI, creating an extensive and difficult to monitor "attack surface". The concept of super-cognition expresses the synergy between human and artificial capabilities, which makes it possible to enhance defense strategies and identify threat signals in advance, overcoming the limits of human judgment in complex situations. However, this synergy also amplifies the risks: every device, system or network adds a new vulnerable spot, exposing democratic societies to cyberattacks, disinformation campaigns and economic sabotage

8. Achievements and challenges of executive order 14110: first 270 days review

The 270-day milestone review was a pivotal element of Executive Order 14110, which tasked agencies, including the National Institute of Standards and Technology (NIST), with developing guidelines, conducting evaluations, and publishing reports to promote the safe and responsible advancement of AI. By this deadline, NIST and the Department of Commerce released essential documents, such as new guidance for generative AI risk management and tools to assess AI vulnerabilities to adversarial attacks. This milestone underscores the EO's phased implementation and transparency focus, positioning the 270-day mark as an early benchmark for public accountability and strategic adjustments.

This built-in review process facilitated timely adjustments based on initial feedback, creating a structured opportunity to address ongoing concerns around privacy and innovation. While the EO established crucial guidelines, some critics argue that stronger mechanisms are needed to protect data privacy without stifling innovation—a balance that may require additional refinement as future milestones approach.

Key Advancements

a) Risk Management

The National Institute of Standards and Technology (NIST) has published comprehensive guidelines addressing AI-related risks, especially in generative AI models. These guidelines offer organizations frameworks for managing risks effectively, ensuring that AI systems are safe and reliable.

b) Strengthening the AI Talent Pipeline

Through the AI Talent Surge initiative, hundreds of AI experts have joined federal service, enhancing the government's capacity to oversee and implement AI technologies. Additionally, the initiative has allocated funding for AI research and development, fostering innovation while ensuring robust oversight.

c) Promoting responsible innovation

The National AI Research Resource (NAIRR) has supported over 80 research teams tackling complex challenges, such as detecting deepfakes and advancing AI applications in medical diagnostics. These efforts emphasize a commitment to responsible AI use and the development of socially beneficial technologies.

d) Global Leadership in AI Governance

The U.S. has proactively shaped international AI standards, particularly in ethical AI applications for defense and human rights, positioning itself at the forefront of global AI governance.

Criticisms and Concerns

Despite these accomplishments, EO 14110 has faced criticism, primarily on privacy and innovation-related issues.

a) Privacy concerns

Privacy advocacy groups, such as the Electronic Privacy Information Center (EPIC), argue that the executive order does not adequately protect personal data. They believe that, despite emphasizing privacy, the EO lacks enforceable mechanisms to prevent data misuse in AI applications. EPIC and

DPCE online
ISSN: 2037-6677

similar organizations advocate for stronger data minimization policies and oversight to avoid AI-driven surveillance and unauthorized data collection. While the order marks a step toward addressing privacy, critics believe more rigorous measures are necessary to build public trust and protect civil liberties.

b) Innovation and Competitiveness

Some industry leaders and tech entrepreneurs have raised concerns that the regulatory approach in EO 14110 could hinder U.S. innovation. Critics warn that an overly restrictive regulatory framework may slow technological advancement, putting the U.S. at a competitive disadvantage, especially compared to China, which is progressing rapidly in AI. This is also highlighted by *The Wall Street Journal's* headline from March 27, 2024, "AI Is Moving Faster Than Attempts to Regulate It".

Balancing Progress and Oversight

The first 270 days of EO 14110 reflect significant efforts to position the U.S. as a leader in AI governance while promoting safe and ethical AI use. However, these criticisms underscore the challenges of balancing stringent oversight with the need for innovation and global competitiveness. Addressing these concerns through enhanced privacy safeguards and a more adaptable regulatory framework will be essential for EO 14110 to meet its ambitious goals while fostering an environment that supports responsible and competitive AI development.

9. Towards a unified European defense strategy and global AI governance

The rapid growth of artificial intelligence technologies and the rise of hybrid warfare necessitate a strategic rethinking of defense and security policies. Traditional military resources and isolated approaches are no longer sufficient to counter modern threats, which span civil, social, and geopolitical dimensions. U.S. Executive Order 14110 marks an initial step toward AI regulation that fosters innovation while also protecting civil rights and privacy. A coordinated European strategy that integrates AI, quantum cryptography, and cybersecurity could help reduce internal divisions and provide a unified, responsive defense.

Technological evolution also presents new challenges for legal experts, who must adapt legal frameworks to preserve democratic values and social cohesion in Europe, while managing the disruptive impacts of innovation. In this context, international cooperation is essential to develop shared ethical standards and policies that balance security needs with the promotion of innovation.

The alliance between the United States and Europe goes beyond individual administrations, as both are closely interconnected in facing common threats. As the saying goes, "a chain is only as strong as its weakest link"—even small vulnerabilities in this network require attention. A unified transatlantic framework would not only safeguard democratic principles and individual rights but also promote responsible innovation, allowing the United States and Europe to face future challenges and opportunities together.

While the integration of European defense and global AI governance is a desirable strategic goal, the complexity of harmonizing diverse regulatory approaches, such as those adopted by the United States and the European Union, represents a significant challenge. The EU favors a prescriptive and stringent approach aimed at protecting fundamental rights through detailed regulations, whereas the United States prefers greater flexibility to promote innovation without excessive constraints. This philosophical and regulatory divergence is a major obstacle to establishing a common framework. However, ongoing dialogue and cooperation on shared ethical standards and principles could facilitate convergence on key issues, promoting responsible AI governance on a global scale.

Ciro Sbailò
Dip.to di Scienze Umanistiche e Sociali Internazionali
Università degli studi internazionali di Roma
ciro.sbailò@unint.eu