Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Antoni Mestre Gascón
Researcher at the Instituto Universitario Valenciano de Investigación en Inteligencia Artificial and associate professor at the Universitat Oberta de Catalunya

Mail: anmesgas@vrain.upv.es

Javier García Rodríguez
Graduated in Police and Criminology Studies, and Deputy Inspector of the National Police Corps.

Mail: javideckard@hotmail.es

Artificial Intelligence as a Geopolitical Asset: Chinese Strategy and its Global Impact

Abstract

Technological development has become a determining factor in the geopolitical competition of the 21st century, with China consolidating its position as one of the most influential players in its application to the fields of security and defense. Through initiatives such as *DeepSeek* and an ambitious national plan for 2030, the Asian country seeks to lead a strategic sector with profound implications for the international order. This article examines the impact of such a strategy on three key fronts: its role in cybersecurity and hybrid warfare, the deployment of autonomous systems in military operations, and the regulatory and strategic challenges arising from its global expansion. It also analyzes the responses of actors such as the United States and the European Union, the role of these technologies in contemporary deterrence and unconventional conflicts, as well as the need to establish international regulatory frameworks to contain the risks derived from their

proliferation. Based on the study of recent sources and strategic analysis, this paper argues that China's technological rise not only reshapes the global balance of power, but also poses crucial challenges in terms of security, digital governance and international stability.

Keywords

Emerging Technologies, Geopolitics, Defense Technology, China.

Cite this article:

Mestre Gascón, A. (2025). Artificial Intelligence as a Geopolitical Asset: China's Strategy and its Global Impact. *Artificial Intelligence as a Geopolitical Asset: Chinese Strategy and its Global Impact*. 25, pp 521-544.

1 Introduction

Artificial intelligence has become one of the most disruptive technologies of the 21st century, with an impact that transcends the scientific and economic spheres to insert itself fully into the field of international security (Hunter *et al.*, 2023). Its accelerated development and its capacity to transform power structures have generated an unprecedented geopolitical competition, in which the main global players seek to consolidate their leadership in this sector. China, in particular, has emerged as one of the most ambitious countries in the race for artificial intelligence, challenging the technological supremacy of the United States and Europe (Khalid, 2025). Its strategic plan to dominate this field by 2030, along with recent advances in advanced models such as *DeepSeek* (DeepSeek-AI *et al.*, 2025) , have set off alarm bells in the West, not only for their economic impact, but also for their implications in the field of security and global stability (Kanellopoulos, 2024).

From a strategic perspective, artificial intelligence not only represents a technological breakthrough, but also constitutes a factor of power with the potential to redefine the balance of power between major powers. Its application in military, cybersecurity and hybrid operations offers considerable advantages in terms of information processing capabilities, decision automation and development of autonomous weaponry (Carlo, 2021). In this context, the Chinese government has demonstrated a remarkable ability to integrate artificial intelligence into its national security strategy, largely due to the close linkage between the private technology sector and the state. Companies such as *Baidu*, *Alibaba*, *Tencent* and, more recently, *DeepSeek*, have developed technologies that, directly or indirectly, strengthen the country's defensive and offensive capabilities, raising concerns about their use in intelligence, surveillance and social control operations.

1.1 Artificial intelligence in the context of international security

The development of artificial intelligence is not taking place in an isolated context, but in an environment characterized by deep geopolitical tensions, strategic uncertainty and growing competition between powers for technological dominance. The United States and China have positioned themselves as the main players in this race, not only with regard to artificial intelligence, but also in other key sectors such as quantum computing, 5G telecommunications and the semiconductor industry (Araya and King, 2022). However, artificial intelligence stands out for its cross-cutting impact on multiple dimensions of international security, as it offers disruptive capabilities that transform conflict scenarios, deterrence strategies and the dynamics of social control.

One of the areas where artificial intelligence has become more relevant is cyber warfare and hybrid operations. The automation of cyber attacks and the ability to manipulate information through advanced algorithms have changed the nature of

threats in cyberspace (Jahankhani *et al.,* 2020: 93-101). China has been identified as one of the most active countries in this field, with a documented history of cyber espionage and intellectual property theft that has affected governments, companies and research centers in the West (Kanellopoulos, 2024). The combination of artificial intelligence with disinformation techniques has allowed the creation of highly sophisticated campaigns that seek to influence public opinion and destabilize democratic systems through the mass dissemination of false or manipulated content on social networks. This type of strategy, which combines cyber-attacks with information warfare, has been classified by various analysts as a new form of hybrid conflict, in which artificial intelligence plays a fundamental role by enhancing the speed, scope and effectiveness of operations.

In the military field, artificial intelligence is driving a profound transformation in the strategic capabilities of major powers. The development of autonomous combat systems has reduced the need for human intervention in war scenarios, facilitating the creation of drones and unmanned vehicles capable of operating in reconnaissance, attack and surveillance missions with a high degree of autonomy (Hunter *et al.*, 2023). China has made significant progress in this field, with research programs aimed at integrating artificial intelligence into advanced military platforms. The combination of deep learning algorithms with intelligent weapon systems poses an unprecedented challenge to global security, as it opens the door to a potential arms race based on the automation of warfare. Although Western powers have promoted initiatives to regulate the development of autonomous weapons, the lack of international consensus and the accelerated investment in this sector have made it difficult to implement effective control mechanisms.

Another area in which artificial intelligence has acquired a central role is surveillance and internal control. In China, technology has become a key tool for the supervision of the population through advanced facial recognition systems, behavioral analysis and online activity monitoring. The implementation of the Social Credit System, which evaluates and classifies citizens' behavior through artificial intelligence algorithms, represents a paradigmatic example of the use of these technologies to consolidate a governance model based on digital control. These practices have generated concern at the international level, as they could serve as a reference for other regimes with authoritarian tendencies that seek to replicate similar systems to reinforce their power. The combination of artificial intelligence with mass surveillance mechanisms raises questions about the balance between security and fundamental rights, as well as about the ethical limits of its application in the field of domestic politics.

These developments have led to a rethinking of security strategies in the West, where the urgency of establishing regulatory frameworks for the use of artificial intelligence in defense and security clashes with the geopolitical interests of the main technological players. The absence of an international consensus on the limits and rules for the application of artificial intelligence has generated a regulatory vacuum that facilitates its development without clear restrictions, which could lead to a scenario of uncontrolled competition and strategic use of these technologies in

conflicts of different kinds. Faced with this reality, the international community faces the challenge of balancing innovation with global security, preventing the advance of artificial intelligence from leading to a new phase of geopolitical instability marked by the strategic use of automation and massive data processing in security and defense operations.

1.2 China and AI: towards a new architecture of technological power

The development of artificial intelligence in China cannot be analyzed in isolation, but within an ecosystem that combines scientific advances, state policies and a military-civilian integration strategy. The Chinese government has made a firm commitment to artificial intelligence as a fundamental pillar of its national security and global competitiveness, establishing clear objectives in its *Next Generation Artificial Intelligence Development Plan*, published in 2017 (Araya and King, 2022). In this document, the need to make China the world leader in artificial intelligence by 2030 is put forward, a goal supported by massive investment in technological infrastructure, the promotion of research in neural networks and the harnessing of large volumes of data for training advanced algorithms. The centralization of information and almost unlimited access to citizen data has given China a comparative advantage over other countries, allowing it to advance rapidly in areas such as facial recognition, predictive security systems and the automation of surveillance processes.

In the area of defense, the People's Liberation Army (PLA) has adopted an approach that combines civilian and military applications, facilitating technology transfer between the private sector and security institutions. This strategy, known as military-civilian fusion, has enabled China to accelerate the development of autonomous weapons, advanced detection systems and artificial intelligence platforms aimed at electronic warfare. In regions such as Xinjiang, the deployment of artificial intelligence-based surveillance technologies has been widely documented, evidencing the use of these tools for monitoring populations and strengthening social control (Khalid, 2025). This dynamic raises questions about the impact that artificial intelligence can have on authoritarian governance models and its possible export to other countries with similar regimes.

The recent *DeepSeek* breakthrough has intensified the perception that China is closing the technology gap with the West (Kanellopoulos, 2024). This artificial intelligence model has achieved performance levels comparable to *OpenAI* and *Google DeepMind* developments, but with less investment in computational infrastructure. Its emergence has generated an intense debate on the viability of artificial intelligence systems in China and on the risks associated with censorship, information manipulation and the strategic use of these models in disinformation campaigns. In a context where artificial intelligence is increasingly linked to global security, China's advancement in this field poses challenges both in terms of regulation and strategic stability.

1.3 Objective and focus of the study

This article analyzes the implications of China's development of artificial intelligence for international security, focusing on three key aspects. First, it examines the impact of artificial intelligence on Chinese military capabilities, including the development of autonomous systems and the integration of algorithms into intelligence operations and strategic deterrence. Second, it assesses technological competition with the West and its implications for the global governance of artificial intelligence, considering the responses adopted by the United States, the European Union, and other relevant actors. Finally, the ethical risks and challenges associated with the advancement of artificial intelligence are addressed, including the lack of clear regulations, the use of these technologies in hybrid conflicts and their implications for global stability.

Through the analysis of strategic documents, government reports and recent academic literature, this study seeks to provide a comprehensive view of China's role in artificial intelligence and its potential to redefine international security in the coming decades. As technology advances and new AI-based defense strategies take hold, it is essential to understand how these transformations are shaping a new world order in which artificial intelligence is not only a tool for innovation, but also a determining factor in the geopolitics of the future.

From a methodological perspective, this study adopts a qualitative approach of a descriptive-analytical nature, based on the documentary analysis of scientific literature, strategic reports and institutional sources from international organizations, *think tanks* and specialized publications (Bowen, 2009). The theoretical framework guiding this research is based on the postulates of offensive realism, which interprets technological development as a strategy for the accumulation of power by states in an anarchic international system (Mearsheimer, 2001: 154-170) ; on the theory of securitization, which allows us to understand how certain narratives –such as leadership in artificial intelligence– are constructed as existential threats that justify extraordinary responses in terms of defense and control (Buzan *et al.*, 1998: 25-57); and in algorithmic governance and technonationalism approaches, which analyze how states use advanced digital technologies to strengthen internal control, protect their strategic interests and project global influence (Zeng, 2022: 12-15, 45-48). This approach allows structuring the analysis around variables such as the degree of AI militarization, the capacity for geopolitical influence and international regulatory mechanisms, thus delimiting the limits and scope of the research.

2 China and AI: strategy and technological development

China has identified artificial intelligence as a key pillar for its economic development and geopolitical positioning (Zeng, 2022). Unlike other technological sectors in which the country has traditionally been dependent on foreign innovations, AI represents an area in which China aspires to become a global leader (Khan *et al.*, 2021) , not only in terms of scientific development, but also in its application in

security, defense and social control. This ambition has been embodied in a comprehensive state strategy that combines massive investment, government support and close collaboration between the public and private sectors.

2.1 China's national AI plan (2017-2030) and its impact on security 2.2

The turning point in China's AI strategy was the publication of the *Next Generation Artificial Intelligence Development Plan* in 2017 (Araya and King, 2022). This document sets out a framework for action to consolidate China as the world leader in AI by 2030, with a progressive approach that is divided into three stages: by 2020, to reach the level of the major powers in AI; by 2025, to lead in certain key application areas; and by 2030, to become the global reference in research, development and application of this technology.

The plan is not only limited to technological innovation objectives, but also stresses the importance of AI for national security. Artificial intelligence is seen as a strategic tool to strengthen the country's defensive and offensive capabilities, particularly in areas such as cybersecurity, mass surveillance and automation of military operations (Kanellopoulos, 2024). The ability to process large volumes of data and optimize decision making in real time represents a key advantage in conflict scenarios and hybrid threat management.

To support this strategy, China has implemented a funding model that combines state investment with private sector incentives (Hunter *et al.*, 2023). The central government, through programs such as the *National Guidance Fund for AI Industry Investment*, has channeled billions of dollars to research in machine learning, machine vision, and robotics. In addition, local governments have established technology parks and innovation centers in cities such as Beijing, Shanghai and Shenzhen, promoting a dynamic ecosystem that fosters collaboration between companies, universities and military institutions.

The development of technological infrastructures has been another key element in this strategy. China has built high-capacity data centers and supercomputers designed specifically for training advanced AI models. Companies such as *Huawei* have played a key role in the expansion of 5G networks, facilitating real-time data transmission and improving the efficiency of AI systems deployed in security and defense (Chu, 2024).

The growth of China's AI sector has also been driven by the leadership of key companies that have been designated as strategic players in the implementation of the national plan. Between 2017 and 2023, public and private investment in artificial intelligence in China exceeded $ 70 billion, placing the country among the top three global investors in the field (Stanford University, 2024). In 2022 alone, more than 20% of the world's total AI startups were founded in China, indicating a structural consolidation of its technology ecosystem. Companies such as *Baidu*, *Tencent* and *Alibaba* have invested heavily in artificial intelligence applied to data analytics,

facial recognition and natural language processing. *Huawei* has been a pillar in the development of technology infrastructures and cloud computing, while *DeepSeek* has recently emerged as a relevant player in the field of advanced language modeling. This convergence between private sector and government strategy has enabled China to accelerate its technological development and reduce dependence on foreign suppliers in key areas of AI.

2.2 DeepSeek and its impact on the geopolitics of AI

One of the most recent and significant developments within the Chinese AI ecosystem has been the emergence of *DeepSeek*, an advanced language model that has surprised the international community with its ability to compete with cutting-edge solutions from the West, such as *OpenAI*'s GPT or *Google DeepMind*'s *Gemini*. *DeepSeek* has proven to be able to operate at a high level of computational efficiency, achieving results comparable to those of its competitors with a fraction of the computational resources used by large Western technology companies.

The emergence of *DeepSeek* has generated debate around China's real ability to close the technology gap with the West in the field of AI. While the United States and Europe have historically led the way in the development of large-scale language models, *DeepSeek*'s efficiency suggests that China has found innovative ways to optimize the performance of these systems without relying on the massive computational infrastructure that characterizes its rivals. This breakthrough could have significant implications in terms of technological sovereignty, as it would allow China to reduce its reliance on key components manufactured by U.S. companies, such as the *NVIDIA* processors used in training AI models (Chu, 2024).

On a geopolitical level, the consolidation of *DeepSeek* as a competitive alternative to Western models poses a new scenario in the race for artificial intelligence. While *OpenAI* and *Google* have adopted a regulatory stance in their developments, with restrictions on access to their models based on government regulations and security concerns, *DeepSeek* represents an alternative that could be used by states and actors seeking to avoid oversight by the United States and its allies. This could facilitate the proliferation of artificial intelligence technologies in countries with authoritarian regimes or in contexts where information control and censorship are prioritized.

One of the aspects that most concerns the international community about *DeepSeek* is the possibility that the model incorporates censorship and information control mechanisms aligned with Chinese government policy. There are indications that certain sensitive issues for the Chinese Communist Party, such as the situation in Xinjiang, the conflict in Taiwan or the protests in Hong Kong, could be restricted within the *DeepSeek* model, limiting access to objective information on these issues. These types of restrictions not only have implications in terms of freedom of expression, but could also be used as a strategic tool in the realm of information warfare and manipulation of the global narrative.

The development of *DeepSeek* and its potential impact on international security reflect a broader trend in China's artificial intelligence strategy (Hunter *et al.*, 2023). Beyond technological competition with the West, AI has become a key instrument in the projection of power and the consolidation of a governance model based on information control. As advanced language models become an essential tool for knowledge management and decision making, China's ability to develop proprietary solutions without external constraints reinforces its strategic autonomy and amplifies its influence in global cyberspace.

In this context, the consolidation of China as a central player in artificial intelligence poses a significant challenge for the international community. The lack of agreements on ethical and strategic limits on the use of AI, coupled with the absence of effective global regulatory mechanisms, increases the risk of these technologies being used for purposes that compromise international stability and security. Competition in artificial intelligence is no longer just a question of technological innovation, but a determining factor in shaping the geopolitical order of the future.

3 AI and national security in China: applications in defense and cybersecurity

The development of artificial intelligence in China not only responds to economic and technological objectives, but has also acquired a central role in the country's national security and military strategy (Zeng, 2022: 29-33). In recent years, the PLA has increasingly adopted an approach based on automation, massive data collection, and artificial intelligence to improve its defense capabilities and strategic positioning on the international stage (Kania, 2022: 68-77) . This transformation has enabled China to advance the integration of autonomous weapons, enhance its surveillance systems, and strengthen its role in cyber warfare.

Unlike other powers that have debated ethical and regulatory limits on the use of artificial intelligence in warfare, China has promoted the development of these technologies with a pragmatic approach, prioritizing their implementation in the military and security domain (Taddeo *et al.*, 2024). Close collaboration between the government, the private sector and military institutions has enabled advances in artificial intelligence to be rapidly transferred to defense applications, accelerating the modernization of the PLA and consolidating China as a key player in the AI-based arms race.

3.1 Military applications of AI

The PLA has embraced artificial intelligence as a key element in the modernization of its military capabilities. One of the areas in which most progress has been made is the development of autonomous weapons and intelligent combat systems, including attack drones, unmanned ground vehicles, and machine learning-based defense

systems (Hunter *et al.*, 2023). These developments have led to increased operational efficiency and reduced the need for human intervention on the battlefield, representing a significant change in the way China conceives of modern warfare. According to estimates by the *Center for Security and Emerging Technology* (CSET), China has allocated between $ 1.6 billion and $ 2 billion annually to the development of military capabilities with artificial intelligence since 2019, including autonomous weapons systems, intelligence, surveillance, and reconnaissance (ISR) platforms, and tactical prediction algorithms (Konaev *et al.*,2023)

Autonomous drones have been one of the most prominent technologies in this field. Models such as the Wing Loong II and the GJ-11 have been designed for reconnaissance, attack and tactical support missions, with an increasing capacity to operate independently thanks to the incorporation of advanced artificial intelligence algorithms (Qiao-Franco and Bode, 2023). These systems not only enhance the PLA's response capability in conventional conflicts, but also represent a key instrument in its deterrence strategy against other actors in the Indo-Pacific region.

Another key aspect of China's military use of artificial intelligence is its application in ISR. Real-time data collection and analysis has enabled the PLA to improve its threat detection capabilities and optimize the planning of its operations. Through a combination of satellite imagery, facial recognition, and large-scale data processing, the PLA can accurately monitor strategic movements of rival actors and anticipate potential conflict scenarios (Araya and King, 2022).

Artificial intelligence has also been integrated into hybrid warfare and deterrence strategies, allowing China to deploy covert operations of influence and information manipulation. The automation of disinformation campaigns, the use of *deepfakes* in political propaganda and the manipulation of social networks have been tools used to generate confusion and destabilize adversaries without resorting to direct confrontation. These mechanisms, added to the PLA's ability to execute sophisticated cyberattacks, have turned artificial intelligence into a weapon of soft power with significant geopolitical effects.

3.2 AI and cybersecurity in the context of cyberwarfare

The use of artificial intelligence in cybersecurity has transformed China's role in cyberspace, consolidating it as a major player in cyberespionage and cyberattacks globally (Admass *et al.*, 2024). The ability to process and analyze large volumes of data in real time has enabled China to develop advanced techniques to infiltrate government, corporate and military networks of other countries, with the aim of obtaining strategic information and weakening the security of its adversaries.

Cyber espionage operations conducted by groups linked to the Chinese government have been widely documented (Cavelty and Wenger, 2022). According to the *Microsoft Digital Defense Report* (Microsoft, 2023) , 44% of cyberattacks attributed to state actors in 2022 originated in China, with targets primarily focused on strategic

sectors such as defense, energy, and telecommunications in the United States, Europe, and Southeast Asia.

These attacks have highlighted the high degree of sophistication of the tools used by Chinese actors to obtain sensitive information and compromise critical infrastructures. The incorporation of artificial intelligence in these operations has made it possible to automate the detection of vulnerabilities, coordinate large-scale attacks and optimize evasion techniques to circumvent the cyber defense systems of targeted countries. This technical evolution increases not only the frequency and precision of cyberattacks, but also their ability to destabilize essential networks with minimal human intervention, thus consolidating AI as a central resource in the Chinese state's digital power projection.

In addition to cyber espionage, China has resorted to artificial intelligence to develop strategies for manipulating and controlling data in cyberspace. The automation of disinformation campaigns has made it possible to influence political and electoral processes in different countries, using *botnets* and artificial intelligence algorithms to amplify narratives favorable to Chinese interests. These strategies have been especially visible on issues such as Taiwanese independence, the situation in Hong Kong and international perceptions of Chinese-driven infrastructure projects abroad.

The combination of artificial intelligence and cyber warfare has generated a response from the United States, the European Union and other powers seeking to contain Chinese influence in this area (Khalid, 2025). Washington has implemented technological restrictions and sanctions against Chinese companies linked to the development of cybersecurity and espionage tools, while the European Union has promoted initiatives to strengthen the digital resilience of its strategic infrastructures. However, the speed with which China is advancing in the development of artificial intelligence applied to cybersecurity poses a considerable challenge for Western democracies, which must balance the protection of their systems with respect for the fundamental rights and privacy of their citizens.

The impact of artificial intelligence on Chinese national security is undeniable. Its application in military, cybersecurity and information warfare has allowed the Chinese government to consolidate its position in the global strategic competition. However, the lack of clear regulations and the risk of escalation in the use of these technologies in international conflicts mean that artificial intelligence represents not only an opportunity, but also a challenge to global stability. As these technologies continue to evolve, the international community faces the challenge of defining the ethical and strategic limits on their application, preventing their development from leading to a new era of digital and military confrontation based on the automation of power.

4 AI and the global balance of power: geopolitical competition

Artificial intelligence has become a central element in global strategic competition, reshaping power relations between the major powers. While its development has generated technological advances with applications in multiple sectors, its impact

on security and defense has been the determining factor in the growing rivalry between the United States and China. In this context, artificial intelligence not only represents a tool for innovation, but has also become a multiplier of military power, a platform for geopolitical influence and a terrain of confrontation in the struggle for technological dominance in the 21st century (Kania, 2022: 68-71).

As China moves forward with its strategy to consolidate its position as a leader in artificial intelligence, the United States and its allies have implemented measures to curb its development and protect their own strategic interests. This dynamic has generated a series of initiatives aimed at restricting China's access to advanced technology, strengthening AI governance in the West, and strengthening international alliances to counter Chinese influence in the Indo-Pacific and other key regions.

4.1 United States vs. China: technological race and militarization of AI

The competition between the United States and China in the field of artificial intelligence is not limited to the economic arena but has moved decisively into the military and strategic sphere. Both powers have identified AI as an essential component in the modernization of their armed forces, with the aim of expanding their defensive capabilities, optimizing decision-making and consolidating their technological superiority in conflict scenarios.

From a geo-economic perspective, the advance of artificial intelligence is also profoundly reshaping labor markets and production structures on a global scale. According to the International Monetary Fund (IMF), approximately 40 % of jobs globally could be significantly transformed by AI, with a particularly intense impact in advanced economies, where up to 60 % of existing jobs are potentially exposed to automation and task reallocation (Cazzaniga *et al.*, 2024). This technological transformation directly links leadership in artificial intelligence with social stability, economic security and the global projection capacity of states, making AI an integral strategic asset.

In the case of the United States, the Department of Defense has driven multiple projects to integrate artificial intelligence into military operations, highlighting initiatives such as *Project Maven* and the Defense Advanced Research Projects Agency (DARPA) programs. *Project Maven*, launched in 2017, represents one of the Pentagon's most ambitious efforts in applying artificial intelligence to military surveillance and reconnaissance (Taddeo *et al.*, 2024). Its main objective is to use advanced algorithms to analyze images captured by drones and automate the identification of threats on the battlefield. This initiative has optimized the responsiveness of U.S. forces, reducing reliance on human analysts and accelerating decision making in complex operational environments.

On the other hand, DARPA has led the development of emerging technologies for defense, with a particular focus on artificial intelligence applied to autonomous

systems, cybersecurity and information operations. Among its most prominent projects are programs aimed at creating autonomous weapons, explainable artificial intelligence algorithms and machine learning-based electronic warfare platforms.

In the face of these advances, China has intensified its investment in artificial intelligence with a similar approach, promoting the development of autonomous combat systems, AI-based surveillance platforms and hybrid warfare strategies (Qiao-Franco and Bode, 2023). This race has raised concerns in the international community about the possibility of an escalation in the militarization of AI, especially in a context where regulation of these technologies remains insufficient.

To contain China's advance in this field, the United States has implemented a series of technological restrictions and sanctions aimed at limiting the Asian country's access to key components in the development of artificial intelligence (Chu, 2024). Among the most significant measures are restrictions on the export of advanced semiconductors and high-performance processors, critical for training artificial intelligence models. Chinese companies such as *Huawei*, *SMIC* and *ByteDance* have been subject to sanctions and trade restrictions, with the aim of curbing their capacity for innovation and development in strategic sectors.

These measures have generated a reaction from China, which has intensified its efforts to achieve self-sufficiency in advanced technology. China's strategy has focused on investing in semiconductor manufacturing, expanding its cloud computing infrastructure, and strengthening its artificial intelligence research capabilities. Between 2017 and 2022, China registered more than 50 % of global patents related to advanced technologies, evidencing the weight of its industrial policy aimed at leadership in strategic sectors (Stanford University, 2024). In addition, it is estimated that more than 270 technology companies have received state financial support for the development of dual-use technologies, facilitating their application in both commercial sectors and national defense (Kania, 2022). These figures confirm the central role of the Chinese state in boosting its technological sovereignty as a tool for geopolitical projection.

4.2 Europe and the governance of AI: regulation and security

While the United States and China have focused their competition on the militarization and strategic development of artificial intelligence, Europe has adopted a more regulatory approach, prioritizing AI security and governance. The European Union has sought to position itself as a leader in the regulation of artificial intelligence, promoting initiatives aimed at establishing ethical and legal standards for its development and application (Araya and King, 2022).

One of the most significant efforts in this area has been the drafting of the *EU Artificial Intelligence Regulation*, which seeks to establish clear rules on the use of AI in different sectors, including its application in security and defense. This regulatory

framework establishes restrictions on the use of mass surveillance systems, decision-making algorithms in judicial processes and the automation of autonomous weapons.

However, AI governance in Europe faces significant challenges in terms of transatlantic cooperation and coordination with other powers (Calderaro and Blumfelde, 2022). The lack of a global consensus on AI regulation has hindered the implementation of international standards, while differences in AI policies between the EU and the United States have led to tensions in the area of security and technological innovation.

Despite these obstacles, the European Union has reinforced its efforts to strengthen its cybersecurity resilience and reduce its dependence on foreign technology (Cavelty and Wenger, 2022). Initiatives such as the *European Defense Fund* and the *European Cybersecurity Strategy* seek to increase the bloc's strategic autonomy and ensure the protection of critical infrastructure from external threats, including potential cyber attacks driven by artificial intelligence.

4.3 International alliances and the global response to Chinese AI

In the face of China's growth as a power in artificial intelligence, several countries have established strategic alliances to contain its influence and strengthen their security cooperation. In the Indo-Pacific region, India, Japan and Australia have played a key role in forming coalitions aimed at countering Chinese technological dominance and strengthening regional stability (Admass *et al.*,2024).

The partnership between India, Japan and Australia has been based on the development of joint technological capabilities, cooperation in cybersecurity and the creation of digital infrastructures independent of Chinese influence. In particular, India has strengthened its relationship with the United States in defense and technology, engaging in information sharing programs and cybersecurity initiatives to reduce the vulnerability of its critical infrastructures to artificial intelligence-driven attacks.

For its part, NATO has taken an increasingly active stance in the debate on artificial intelligence and its impact on collective defense (Hunter *et al.*, 2023). The organization has identified AI as one of the main emerging technologies that could affect global security, promoting the development of regulatory frameworks and cooperation among member countries in the integration of artificial intelligence in defense systems.

As artificial intelligence continues to evolve, the global balance of power will be influenced not only by technological development, but also by the ability of states to establish strategic alliances and effective regulations (Zeng, 2022: 94-96). Competition between the United States and China continues to set the global agenda, but the response of Europe and other emerging powers will play a key role in shaping the future of artificial intelligence in the realm of security and international geopolitics.

5 Challenges and risks of Chinese AI in international security

China's accelerated development of artificial intelligence has established the country as a technological powerhouse with advanced applications in security, defense and information control (Raska and Bitzinger, 2023). However, its approach has raised significant concerns in the international community, both in terms of governance and transparency and the impact these technologies may have on global stability. The lack of effective regulations, the use of artificial intelligence to bolster authoritarian surveillance structures, and the growing risk of autonomous weapons proliferation have led to intense debate about the challenges posed by the Chinese model of artificial intelligence. As these technologies expand and become integrated into security and defense strategies, the world faces a dilemma: how to balance technological advancement with the need to establish regulations that prevent abuses and avoid an escalation of confrontations driven by the automation of conflict.

5.1 Lack of transparency and ethical issues

One of the most controversial aspects of the development of artificial intelligence in China is its use for mass surveillance and the reinforcement of social control policies (Calderaro and Blumfelde, 2022). The implementation of advanced technologies for facial recognition, behavioral analysis and digital monitoring has allowed the Chinese government to establish an unprecedented surveillance system, with special emphasis on regions considered politically sensitive. The case of Xinjiang is a clear example of how artificial intelligence can be used as a tool of repression. In this region, the government has deployed a complex AI-based monitoring system that allows tracking and analyzing the activities of the Uyghur population, identifying patterns of behavior and signaling potential "threats" based on machine learning algorithms. These systems, combined with the use of biometric data and mass communications analysis, have been denounced by international bodies as an example of systematic human rights violations.

Beyond Xinjiang, the use of artificial intelligence in Chinese governance raises questions about authoritarian control of information. Automated censorship, driven by algorithms capable of identifying and blocking content deemed sensitive by the Chinese Communist Party, represents a significant risk to freedom of expression and access to information. Technology companies such as *Baidu* and *Tencent* have developed advanced filtering systems that restrict the circulation of certain narratives on the internet, consolidating a digital ecosystem in which the state has almost absolute control over information flows. This model could set a precedent for other regimes with authoritarian tendencies, which could adopt similar systems to strengthen their control over the population.

Another ethical problem posed by Chinese artificial intelligence is the lack of transparency in its development and application processes (Kanellopoulos, 2024).

The absence of external audits and limited public information on the performance of algorithms used in security and defense make it difficult to assess the biases and errors that may arise in these systems. Since artificial intelligence relies on large volumes of data for training, the lack of diversity in the data sets used can generate biases that perpetuate discrimination and errors in decision making. In a context where artificial intelligence becomes a pillar of national security, opacity in its design and application represents a challenge for accountability and responsible governance of these technologies.

5.2 Risks of proliferation of autonomous weapons

The expansion of artificial intelligence in the military has led the international community to question the impact of autonomous weapons and the possibility of effective regulation (Khan *et al.*, 2021). China has made significant progress in developing artificial intelligence-driven combat systems, including autonomous drones, automated defense systems, and electronic warfare platforms capable of operating without direct human intervention. These developments have intensified the debate on the proliferation of autonomous weapons and the need to establish control mechanisms to prevent their indiscriminate use.

The main challenge in the regulation of autonomous weapons lies in the lack of consensus among the major powers. While countries such as the United States and China have invested in combat automation as part of their military modernization strategy, other international actors, including the European Union, have advocated stricter regulation to limit the use of lethal systems without human supervision. At the United Nations, debates on banning or limiting autonomous weapons have been divisive, with proposals ranging from a total ban to more flexible regulations allowing their use in certain circumstances.

The central problem with the proliferation of autonomous weapons is their potential to trigger a new arms race based on artificial intelligence. Unlike conventional weapons, which require large production and deployment infrastructures, autonomous systems can be developed and replicated with relative ease, increasing the risk that non-state actors, including terrorist groups and criminal organizations, can gain access to these technologies (Qiao-Franco and Bode, 2023). In addition, the lack of clarity in security protocols to avoid failures in automated decision making represents a significant risk, as an error in the algorithms of these systems could lead to incidents with catastrophic consequences.

The possibility of establishing an effective regulatory framework will depend on the international community's ability to negotiate agreements that balance innovation with global security. The creation of mechanisms for verification, auditing and oversight of developments in artificial intelligence applied to defense will be crucial to avoid an uncontrolled escalation in the use of these technologies in armed conflicts.

5.3 Future scenarios: How will technological competition evolve?

The future of artificial intelligence in the field of international security will depend on how technological competition between the major powers evolves (Hunter, 2025). There are multiple possible scenarios, each with different implications for global stability. One of the most plausible scenarios is China's dominance in the development of artificial intelligence, consolidating its leadership in key sectors such as natural language processing, defense automation and cybersecurity. This scenario would imply a shift in the global power structure, with China's increased influence on regulation and international standards for artificial intelligence (Khalid, 2025).

Another possible scenario is the fragmentation of technological power, with competition among multiple players developing their own digital infrastructures and artificial intelligence platforms. In this context, the United States, the European Union and their allies would seek to reduce their dependence on Chinese technology by promoting the development of independent artificial intelligence ecosystems. This fragmentation could lead to greater polarization in access to technology and a dispute over digital sovereignty in different regions of the world.

In terms of security and defense, the hot spots around artificial intelligence could intensify in areas such as cybersecurity, electronic warfare, and information manipulation. Artificial intelligence will continue to be a key factor in hybrid warfare strategies, increasing the need for more sophisticated digital defense mechanisms (Admass *et al.*, 2024). In addition, the potential integration of artificial intelligence into strategic weapons and deterrence systems could generate new dynamics in nuclear stability and international conflict management.

The development of artificial intelligence poses both opportunities and challenges for international security. While its potential to improve efficiency and decision-making is undeniable, its use without clear regulations could destabilize the global balance and generate new forms of conflict (Cavelty and Wenger, 2022). In this context, the international community faces the challenge of defining the limits and control mechanisms that guarantee the responsible development of these technologies, preventing them from becoming a threat to world peace and security.

6 Conclusions and recommendations

The development of artificial intelligence in China has significantly transformed the global security and geopolitical landscape. Throughout this analysis, multiple dimensions have been identified in which artificial intelligence has been used as a strategic enabler, from its integration into defense and cybersecurity systems to its application in mass surveillance and information control. Artificial intelligence has not only enabled China to enhance its military and intelligence capabilities, but has also strengthened its influence in the global technological arena, challenging the traditional leadership of the United States and raising concerns about the impact of these technologies on international stability.

One of the key findings of this study is the central role of artificial intelligence in China's military modernization. Through combat automation, the development of autonomous weapons, and the application of advanced algorithms in intelligence, surveillance, and reconnaissance, the PLA has consolidated its position as one of the most advanced military forces in the use of AI. However, the lack of transparency in the development of these systems and the absence of clear regulations at the international level pose significant risks, especially with regard to the proliferation of autonomous weapons and the potential use of artificial intelligence in hybrid conflicts and cyber-attacks.

In the field of digital security, China has used artificial intelligence to strengthen its capabilities in cyber espionage and information manipulation. Automating cyberattacks and using algorithms to influence public opinion have been key strategies in expanding its power in cyberspace, leading to a response from the United States, the European Union and its allies in the form of sanctions, technological restrictions and the development of more sophisticated cyber defense strategies. However, the speed with which China is advancing in this field poses a considerable challenge for Western democracies, which must strike a balance between security and the protection of fundamental rights in the development and regulation of artificial intelligence.

Likewise, the use of artificial intelligence in mass surveillance and social control has generated international concern. The implementation of facial recognition technologies, biometric data analysis and automated censorship has consolidated a model of digital governance based on monitoring and restricting freedom of expression. This approach not only raises questions about the ethical limits of artificial intelligence, but could also serve as a reference for other authoritarian regimes seeking to strengthen their control through the use of these technologies.

6.1 Proposals for a global governance of AI in security

Given these challenges, it is essential to develop a global governance framework for artificial intelligence that guarantees its responsible use and reduces the risks associated with its uncontrolled proliferation. One of the main challenges in this regard is the need to establish international standards to regulate the use of artificial intelligence in the military and security sphere. The creation of multilateral treaties prohibiting or limiting the use of autonomous weapons without human intervention would be a first step in this direction, although their implementation faces obstacles due to the lack of consensus among the major powers.

In the field of cybersecurity, it is crucial to strengthen international cooperation to prevent and mitigate the effects of artificial intelligence-driven cyberattacks. Collaboration between countries in sharing cyber threat information and creating joint response mechanisms could improve the resilience of critical digital infrastructures and reduce vulnerability to automated attacks.

Another key aspect of the global governance of artificial intelligence is the regulation of the use of these technologies in surveillance and social control (Calderaro and Blumfelde, 2022). The international community must promote standards that protect human rights and establish clear limits on the collection and use of personal data in artificial intelligence systems. In this regard, the European Union has taken significant steps with its proposed Artificial Intelligence Regulation, which could serve as a reference for the development of regulations at the global level.

In addition, there is a need to encourage the development of artificial intelligence with a focus on transparency and accountability. The creation of independent bodies responsible for auditing the operation of algorithms used in security and defense could help prevent abuses and ensure that these technologies are used in an ethical and responsible manner.

6.2 Implications for Spain: risks, capabilities and strategic challenges

The advance of artificial intelligence as a geopolitical asset —especially in the case of China— has important implications for Spain at various levels. From the defense point of view, the increasing automation of conflict and the integration of AI-based technologies in the military doctrines of strategic actors force the Spanish Armed Forces to adapt to highly digitized operational scenarios. In this sense, it is a priority to strengthen capabilities in areas such as cyber defense, electronic warfare, autonomous systems and predictive analytics, in coordination with the initiatives promoted by NATO and the European Union. As the Department of Homeland Security points out in its Homeland Security Report 2023, technological transformation represents a source of both opportunity and vulnerability, being essential to anticipate the "strategic impacts of disruptive technologies such as artificial intelligence in the field of defense and digital sovereignty" (Department of Homeland Security, 2023).

In the field of Public Administrations, the growing dependence on intelligent systems in critical sectors —such as infrastructure management, telecommunications or e-government— requires a national resilience strategy that combines technological robustness, solid regulatory frameworks and public-private cooperation to mitigate the risks associated with the malicious use of AI, especially in contexts of espionage, disinformation or foreign interference. The recent approval of the European Regulation on Artificial Intelligence offers Spain an advanced regulatory platform from which to contribute to the formulation of international standards of technological governance, ensuring compatibility between innovation, security and fundamental rights.

Finally, from a social perspective, Spanish civil society is also challenged by the effects that artificial intelligence may have on employment, privacy and democratic quality. The automation of processes, massive data collection and the possibility of algorithmic manipulation of information demand a proactive approach based on digital education, institutional transparency and citizen participation in technological decision-making. In this context, it is essential to prevent the digital transformation, marked by competition between powers such as China and the United States,

from resulting in structural vulnerabilities, and instead promote a model of ethical, inclusive and strategically autonomous technological development for Spain.

6.3 Future lines of research

The advance of artificial intelligence in the field of security raises multiple questions about its impact on global power dynamics and future military doctrines. Among the main lines of research to be addressed in the coming years, the following stand out:

- **How will AI affect future military doctrines?** The automation of combat, the integration of autonomous systems into strategic planning and the possibility of artificial intelligence making operational decisions without human intervention could completely transform the nature of armed conflict. It is critical to analyze the implications of these changes and assess the risks associated with the loss of human control in military operations.
- **What role will international alliances play in AI regulation?** The fragmentation of technological power and the growing rivalry between major powers could make it difficult to adopt global regulations on artificial intelligence. It will be crucial to study how alliances between the United States, the European Union, Japan, India and other strategic players can influence the creation of regulatory frameworks that promote the responsible use of AI in security and defense.
- **Can China consolidate its position as the dominant power in AI or will there be a fragmentation of power?** While China has made significant progress in the development of artificial intelligence, the United States and its allies have taken steps to restrict its access to key technologies, such as advanced semiconductors and high-performance processors. In this context, it is important to analyze whether China will achieve technological self-sufficiency and consolidate its leadership in AI or whether, on the contrary, there will be a fragmentation of power with multiple poles of technological development.
- **How can the risks of autonomous weapons proliferation be mitigated?** The possibility of these technologies being used by non-state actors or in conflicts without clear regulation represents one of the most pressing challenges in international security. Future research should focus on strategies to prevent unauthorized access to these technologies and on the creation of effective verification and control mechanisms.

Artificial intelligence is redefining the global balance of power and its impact on international security will remain a central issue on the geopolitical agenda for decades to come. While its development offers unprecedented opportunities for innovation and optimization of strategic processes, it also poses significant challenges that must be addressed with a holistic approach. The international community faces the challenge of establishing a governance framework that ensures that artificial intelligence is used ethically, securely and for the benefit of global stability. Without effective regulation

and strong international cooperation, the risk of artificial intelligence becoming a factor of destabilization and conflict will continue to grow, with unforeseeable consequences for the global order.

Bibliography

Admass, W. S., Munaye, Y. Y. y Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*. 2, p. 100031. [Accessed: 11 may 2025]. Available at: https://doi.org/10.1016/j.csa.2023.100031

Araya, D. y King, M. (2022). The impact of artificial intelligence on military defence and security. *CIGI Papers* Centre for International Governance Innovation. 263. [Accessed: 11 may 2025]. Available at: https://www.cigionline.org/publications/the-impact-of-artificial-intelligence-on-military-defence-and-security/

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*. 9, pp. 27-40. [Accessed: 11 may 2025]. Abailable at: https://doi.org/10.3316/QRJ0902027

Buzan, B., Wæver, O. y Wilde, J. de. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers. ISBN 978-1-55587-784-2

Calderaro, A. y Blumfelde, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty. *European Security*. 31(3), pp. 415-434. [Accessed: 11 may 2025]. Available at: https://doi.org/10.1080/09662839.2022.2101885

Carlo, A. (2021). Artificial Intelligence in the Defence Sector. In: Mazal, J., Fagiolini, A., Vasik, P. y Turi, M. (eds.). *Modelling and Simulation for Autonomous Systems*. Springer International Publishing, Cham, pp. 269-278. [Accessed: 11 may 2025]. Available at: https://doi.org/10.1007/978-3-030-70740-8_17

Cavelty, M. D., Wenger, A. (2022). *Cyber Security Politics. Socio-Technological Transformations and Political Fragmentation*. London, Routledge. ISBN 978-0-367-62664-8. [Accessed: 11 may 2025]. Available at: https://doi.org/10.4324/9781003110224

Chu, M. C. M. (2023). China's defence semiconductor industrial base in an age of globalisation: Cross-strait dynamics and regional security implications. *Journal of Strategic Studies*. 47(5), pp. 643-668. [Accessed: 11 may 2025]. Available at: https://doi.org/10.1080/01402390.2023.2164852

DeepSeek-AI *et al.* (2025). DeepSeek-R1: Incentivizing Reasoning Capability in LLMs via Reinforcement Learning. Cornell University. [Accessed: 11 may 2025]. Available at: https://doi.org/10.48550/arXiv.2501.12948

Departamento de Seguridad Nacional. (2023). Informe Anual de Seguridad Nacional. Departamento de Seguridad Nacional. [Accessed: 11 may 2025]. Available at: https://www.dsn.gob.es/es/publicaciones/informes-anuales/IASN2023

Hunter, L. Y. (2025). Artificial Intelligence, Data Centers, Energy Capabilities, and International Security: An Exploratory Analysis. *Armed Forces & Society*. 0(0). [Accessed: 11 may 2025]. Available at: https://doi.org/10.1177/0095327X241308839

Hunter, L. Y., Albert, C. D., Henningan, C. y Rutland, J. (2023). The military application of artificial intelligence technology in the United States, China, and Russia and the implications for global security. *Defense and Security Analysis*. 39, pp. 207-232. [Accessed: 11 may 2025]. Available at: https://doi.org/10.1080/14751798.2023.2210367

Jahankhani, H., Kendzierskyj, S., Chelvachandran, N. & Ibarra, J. (2020). *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity, Advanced Sciences and Technologies for Security Applications*. Springer International Publishing, Cham. ISBN: 978-3-030-35745-0. [Accessed: 11 may 2025]. Available at: https://doi.org/10.1007/978-3-030-35746-7

Kanellopoulos, A. N. (2024). Counterintelligence, Artificial Intelligence and National Security: Synergy and Challenges. Journal of Politics and Ethics in New Technologies and AI. 3(1). [Accessed: 11 may 2025]. Available at: https://doi.org/10.12681/jpentai.35617

Kania, E. B. (2022). *Artificial intelligence in China's revolution in military affairs, in: Defence Innovation and the 4th Industrial Revolution*. Abingdon, Routledge, pp. 83-98. ISBN 978-1-032-21399-6.

Khalid, S. (2025). Role of artificial intelligence and cyberwar in America and China influencing Pakistan. *SocSciSpec*. 4, pp. 13-20. [Accessed: 11 mayo 2025]. Available at: https://sss.org.pk/index.php/sss/article/view/191

Khan, A., Imam, I. & Azam, A. (2021). Role of Artificial Intelligence in Defence Strategy: Implications for Global and National Security. *Strategic Studies*. 41, pp. 19-40. [Accessed: 11 may 2025]. Available at: https://www.jstor.org/stable/48732266

Konaev, M., Fedasiuk, R., Corrigan, J., Lu, E., Stephenson, A., Toner, H. & Gelles, R. (2023). *U.S. and Chinese Military AI Purchases*. Center for Security and Emerging Technology. [Accessed: 11 may 2025]. Available at: https://doi.org/10.51593/20200090

Cazzaniga, M., Jaumotte, F., Li, L., Melina, G., Panton, A. J., Pizzinelli, C., Rockall, E. J. & Mendes Tavares, M. (2024). Gen-AI: Artificial Intelligence and the Future of Work. Staff Discussion Notes. International Monetary Fund. [Accessed: 11 may 2025]. Available at: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2024/01/14/Gen-AI-Artificial-Intelligence-and-the-Future-of-Work-542379

Mearsheimer, J. J. (2001). *The Tragedy of Great Power Politics*. W. W. Norton & Company. ISBN 978-0-393-34927-6.

Microsoft. (2023). Microsoft Digital Defense Report and Security Intelligence Insights. [Accessed: 11 may 2025]. Available at: https://www.microsoft.com/en-us/security/business/security-intelligence-report

Qiao-Franco, G. & Bode, I. (2023). Weaponised Artificial Intelligence and Chinese Practices of Human–Machine Interaction. *The Chinese Journal of International*

Politics. 16, pp. 106-128. [Accessed: 11 may 2025]. Available at: https://doi.org/10.1093/cjip/poac024

Raska, M. & Bitzinger, R. A. (2023). *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*. Taylor & Francis. ISBN 978-1-032-11075-2

Stanford University. (2024). The 2025 AI Index Report. Stanford HAI. [Accessed: 11 may 2025]. Available at: https://hai.stanford.edu/ai-index/2025-ai-index-report

Taddeo, M., Blanchard, A. & Thomas, C. (2024). From AI Ethics Principles to Practices: A Teleological Methodology to Apply AI Ethics Principles in The Defence Domain. *Philos. Technol.* 37, p. 42. [Accessed: 11 may 2025]. Available at: https://doi.org/10.1007/s13347-024-00710-6

Zeng, J. (2022). *Artificial Intelligence with Chinese Characteristics: National Strategy, Security and Authoritarian Governance*. Springer, Singapore. ISBN: 978-981-19-0721-0. [Accessed: 11 may 2025]. Available at: https://link.springer.com/book/10.1007/978-981-19-0722-7

Article received: February 16, 2025
Article accepted: June 5, 2025