University of Piraeus

Department of International and European Studies

MSc in International & European Studies

THE DISRUPTIVE FORCE OF TECHNOLOGY IN INTERNATIONAL RELATIONS:

THE CASE OF ARTIFICIAL INTELLIGENCE AND BIG DATA

Master Thesis

Angelos Alexopoulos

Supervisor: Dr. Athanasios Platias

Piraeus, 2026

The intellectual work fulfilled and submitted based on the delivered master thesis is exclusive property of mine personally. Appropriate credit has been given in this diploma thesis regarding any information and material included in it that have been derived from other sources. I am also fully aware that any misrepresentation in connection with this declaration may at any time result in immediate revocation of the degree title.

Angelos Alexopoulos

Abstract

This thesis investigates the transformative role of technology in the 21st century international system, analyzing how Artificial Intelligence (AI) and disruptive innovations function as structural modifiers of state power. Critically, this research addresses the question of how emerging technologies influence the balance of power and the security dilemma. Adopting a Neoclassical Realist framework, the study argues that technology is not merely an exogenous variable but a decisive determinant of national survival that is filtered through domestic structures and threat perceptions.

Through a qualitative analysis of two distinct case studies, the Russo-Ukrainian conflict and the US-China strategic rivalry, the research empirically tests the impact of technology on hegemony and stability. The findings from the Ukrainian theater demonstrate that low-cost, autonomous systems act as force multipliers, enabling weaker states to challenge materially superior adversaries and achieve asymmetric advantages. Conversely, the analysis of the Sino-American competition reveals that while China has leveraged "Military-Civil Fusion" to challenge the status quo, the United States preserves its hegemonic position by maintaining qualitative superiority in the AI ecosystem and employing "weaponized interdependence" strategies, particularly in the semiconductor supply chain.

Ultimately, the thesis concludes that the "opacity" and "dual-use" nature of AI exacerbate the security dilemma, validating the realist assertion that technological diffusion in an anarchic system intensifies strategic competition rather than fostering cooperation. By compressing decision-making time and introducing new layers of uncertainty, technology redefines the parameters of security and balance of power, confirming that material capability remains the ultimate arbiter of the international order.

Keywords: Artificial Intelligence, Big Data, Realism, Security Dilemma, Great Power Competition, Weaponized Interdependence, US-China rivalry, Military-Civil Fusion, Innovation Power.

Acknowledgements

I am incredibly grateful to my supervisor, Dr. Athanasios Platias, for his guidance and expertise. His constructive criticism and patient support were vital in helping me refine this research and resolve the challenges I faced along the way.

I also owe a debt of gratitude to the wider faculty members who, through their lectures and discussions, broadened my perspective and deepened my understanding of the field.

Finally, I must express my profound gratitude to my family. Their encouragement and support over the years have been essential to my success.

Contents

List of Figures

List of Tables

Introduction

In the 21st century, the international system is undergoing a profound transformation driven by the rapid advancement of disruptive technologies. While traditional International Relations theories have often treated technology as an exogenous variable or a mere tool of economic growth, this thesis argues that technology has emerged as a "structural modifier" of state power. It does not merely expand existing capabilities but fundamentally redefines the rules of the security dilemma and the hierarchy of international order, without altering its anarchic nature.

Current realities, characterized by the resurgence of Great Power competition between the United States and China, demonstrate that the struggle for hegemony is increasingly defined by the race for technological supremacy. The advent of Artificial Intelligence (AI), Big Data, and autonomous systems introduce unprecedented challenges. Unlike nuclear weapons, which functioned as "prestige technology" with high barriers to entry favoring the status quo, AI represents a "general-purpose technology" characterized by rapid diffusion and dual-use applicability. This distinction implies that the proliferation of AI is far more uncontrollable, intensifying the security dilemma by favoring offense over defense.

Critically, the primary objective of this research is to answer the following question: How does the integration of Artificial Intelligence and disruptive technologies affect the international balance of power and the intensity of the security dilemma?

To address this, the study adopts a Neoclassical Realist framework, utilizing the analytical categories proposed by Charles Weiss regarding the impact of technology on the international system. Specifically, the research focuses on two critical dimensions identified by Weiss: the "operational processes", examining how innovations like OODA loops and autonomous systems transform warfare, and the "systemic architecture", analyzing how technology reorders the distribution of power and creates new forms of structural inequality. By integrating John Mearsheimer's concept of "latent power" into this framework, the thesis further explains how technological innovation acts as a multiplier, converting socioeconomic potential into active military capability.

In this context, this realist approach is selected for its superior explanatory power compared to liberal institutionalism. While liberals argue that digital interconnectedness fosters peace through complex interdependence, reality reveals a paradox where increased connectivity leads to "weaponized interdependence". States utilize their control over central nodes of the global economy, such as semiconductor supply chains and financial networks, to impose costs on adversaries, turning interdependence into a tool of coercion.

Furthermore, the study is guided by five core hypotheses derived from theoretical analysis and applied to past data:

1. Technology as a power multiplier: Innovation functions as a crucial determinant of power, enabling weaker states to achieve asymmetric advantages against materially superior adversaries. This is evidenced by the "force multiplier" effect of low-cost autonomous systems in modern conflicts.

2. Structural Redistribution: Disruptive technologies can alter the balance of power and trigger a redistribution of capabilities, potentially leading to hegemonic transition.

3. Intensification of the security dilemma: The opaque and dual-use nature of AI exacerbates the security dilemma. The difficulty in distinguishing between civilian and military applications ("distinguishability problem") forces states to assume the worst-case scenario regarding their adversaries' intentions.

4. Persistence of current hegemony: Despite the rise of emerging powers, the United States retains hegemonic status through qualitative superiority in critical ecosystems (AI design, chips) and control over structural chokepoints, challenging the narrative of an immediate power transition.

5. Realist validity: The realist approach is the most robust framework for explaining the disruptive nature of technology, as it justifies strategic competition and the "self-help" logic that drives state behavior in the digital age.

The thesis is organized into three main chapters designed to test these hypotheses. Chapter 1 establishes the theoretical framework, analyzing the relationship between technology and International Relations theory, with a specific focus on realism, the concept of "weaponized interdependence," and the metrics of measuring power in the 21st century. Chapter 2 provides the empirical application, beginning with a historical overview of technological disruptions before examining two distinct case studies: the Russo-Ukrainian conflict, which illustrates the operational impact of AI in warfare, and the US-China strategic rivalry, which highlights the competition for technological supremacy. Finally, chapter 3 synthesizes the findings to offer general conclusions on the verification of the theoretical assumptions and the future of global order.

Research methodology

To effectively address the research question regarding the impact of Artificial Intelligence on the international balance of power, this thesis employs a qualitative research strategy. This methodological choice is dictated by the nature of the research object itself, as the "AI revolution" is an evolving, multifaceted phenomenon that cannot be fully captured through quantitative metrics alone. Instead, it requires an interpretive approach to understand the strategic, doctrinal, and political implications of technological change.

The core of the analysis relies on the comparative case study method. The research examines two distinct but complementary cases to test the hypotheses across different levels of analysis:

- The Russo-Ukrainian Conflict (operational level): This case was selected to examine the "force multiplier" effect of technology in active warfare. It provides empirical evidence on how low-cost autonomous systems (drones, USVs) allow a weaker state to challenge a materially superior adversary, validating the hypothesis regarding asymmetric advantages.
- The US-China strategic rivalry (systemic level): This case represents the "hegemonic competition" aspect. It is essential for analyzing the impact of AI on the global distribution of power, the security dilemma, and the weaponization of interdependence (semiconductors).

This dual approach allows for a holistic understanding of the phenomenon, connecting tactical battlefield innovations (Ukraine) with grand strategic competition (US-China).

The research is based on a wide range of primary and secondary sources to ensure validity. Primary sources include official government documents, such as the White House AI Action Plan. Secondary sources consist of academic literature from international relations scholars (e.g. Jervis, Mearsheimer, Horowitz, Allison), as well as reports from specialized think tanks (SIPRI, CSIS) and industrial data on computing power and semiconductor manufacturing.

Limitations

The research focuses exclusively on great power competition (US, China, Russia) and the Ukrainian theater. It does not thoroughly examine other geopolitical actors (e.g., the EU, Israel, India) or the full spectrum of emerging technologies (e.g., quantum computing). Therefore, findings are specific to the AI domain and may not be generalizable to all technological sectors.

Moreover, the analysis faces inherent challenges due to the classified nature of military programs and expenditure, particularly regarding China's "Military-Civil Fusion" strategy. To mitigate this, the study relies on cross-verification of open-source intelligence and official doctrinal texts, acknowledging a necessary degree of uncertainty.

1.Technology and International Relations: theoretical and conceptual framework

1.1 Defining technology and its relationship with global affairs

International Relations theorists have long recognized that a nation's power and its security as well consist of several structural factors, notably the economic, diplomatic, military, technological, demographic, and psychological ones (Platias & Koliopoulos, 2010, p. 1). Among these, the technological aspect is an important one, yet sometimes, it is perhaps overlooked or taken as a static given. Historical and emerging realities show that technology affects both the economic and military power of a state, while being a transformative force for the balance of power.

In this context, Artificial Intelligence, emerges not just as an instrument of state power, but as a "structural modifier". That implies that it doesn't only expand existing capabilities, but it also sets new rules in the security dilemma, without changing the anarchic nature of the international system. It accomplishes this by limiting the decision-making window (OODA loop) and elevating the significance of the digital world as a domain of conflict. However, it is first necessary to define technology within the international arena before reaching this conclusion.

Generally, technology is "the application of scientific knowledge and human skills to the solution of problems in the practical or industrial arts" (Plano & Olton, 1988, p. 112). According to Fred Bucy, "Technology is the design and manufacturing know-how required to produce goods," while science is "the systematic pursuit of knowledge" (Bucy, 1980, p. 134). Martin Van Creveld, whose work on technology and war is extensive, has a broader understanding of technology. He refers to it as "an abstract system of knowledge, an attitude towards life and a method for solving its problems" (Van Creveld, 1989, p. 312). He also thinks that "Technology" from an abstract standpoint can be applied in every moment and any place, while in reality, there are several technologies, which are usually used differently in each social context. (Van Creveld, 1989, p. 4)

Yet, Brook's definition sets the necessary theoretical framework for this analysis, as for him technology is the "knowledge of how to fulfill certain human purposes in a specifiable and reproducible way" (Brooks, 1980, p. 66). Based on this thought, this research defines technology not merely as hardware, but as the reproducible knowledge of how to fulfill strategic purposes, transforming latent economic power into offensive military capability. "Innovation, on the other hand, is the process by which technology is created and deployed in society, implying the creation as well of whatever support systems are necessary to install and use a technology" (Skolnikoff, 1993, p. 14). Extending this notion, how a country adopts an innovation plays a vital role in gaining strategic advantage over rivals.

It is though, crucial to understand that not all technologies impact the international system equally. Drezner proposes a vital typology based on fixed costs and sectoral orientations, arguing that there are 4 categories:

1. Strategic tech: Innovations that have high fixed costs and significant civilian applications, such as 5G networks.
2. Prestige tech: Innovations with high fixed costs and limited civilian applications, like nuclear weapons.
3. Public tech: Innovations with low fixed costs and limited civilian applications, such as vaccines, where governmental investment is necessary.
4. General purpose tech: Innovations characterized by low fixed costs and significant private sector possibilities, such as artificial intelligence. In this instance, commercial applications drive rapid global diffusion.

Therefore, the speed that an innovation will be diffused is correlated inversely with fixed costs and directly with private sector applicability, which explains why general purpose tech is the fastest to proliferate and prestige tech the most constrained. (Drezner, 2019, pp. 6-8)

From a security perspective, this means that the proliferation of AI (general purpose tech) will be much more uncontrollable compared to nuclear weapons (prestige tech), thereby creating distinct implications for the balance of power. While nuclear weapons sustain the status quo due to high barriers to entry, AI is being diffused uncontrollably due to the high interest of public and private actors alike. Consequently, while the status quo is strengthened by nuclear deterrence, AI seems to intensify the security dilemma by favoring offense. (Saghir, et al., 2025)

Deploying a technology can sometimes be disruptive, transforming the existing order, whether in business, and the economy, or international relations. By changing the established systems, a shift can be observed in power dynamics, which creates new operational paradigms, or new markets in the instance of the economy. Clayton Christensen who developed the theory of "Disruptive Innovation", argues that a new market can be created by an innovation that consists of a different set of values, displacing an existing market, while using new technologies or applying new business models or new ways to the use of existing technologies. (Leipziger & Dodev , 2016, p. 2) Accordingly, technological progress is a key factor in the redistribution of power in the international arena (Zacher, 2016, p. 50), thus changing its structure, and allowing the emergence of new players, as well as new ways to conduct conflict, which lead to the augmentation of the security dilemma. Such a disruption can be associated with a Revolution in Military Affairs (RMA), where a fundamental transformation takes place resulting from the combination of new technologies, innovative operational concepts, and organizational adaptations, which together produce a discontinuous and profound increase in military capability and effectiveness. (Krepinevich, 2002)

The extent to which disruptive technology affects power dynamics, depends not only on the technology itself, but also on the organizational adoption. While the British invented the aircraft carrier, they didn't see its full potential, that it could be a floating airfield, which was the case for the USA and Japan. This resulted in a major switch in naval supremacy, as history has shown. (Horowitz, et al., 2018, pp. 4-5)

To better outline the relationship between science, technology, and international relations, it is first necessary to understand that science and technology are not just instruments, but products of social processes influenced by economic, social, cultural, and political factors. Hence, there is a reciprocal relationship between science-technology and international relations, including direct and indirect effects. The next figure depicts this triangular relationship.

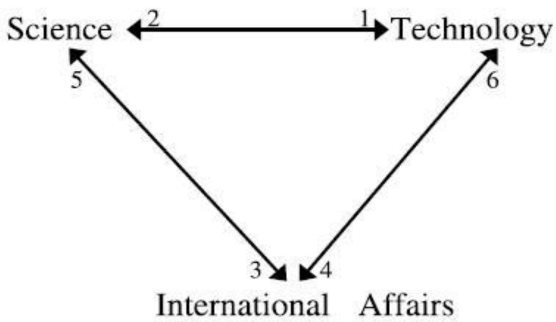

Figure 1. The triangular relationship (Weiss, 2005, p. 298)

To begin with, Figure 1 shows that there are mutual influences between technology and science; for example, scientific research on microwave radiation brought about the laser, while the Hubble telescope expanded scientific knowledge on the origins of the universe. International relations are affected by science in two ways. Firstly, scientific observations of the natural world reveal new phenomena, like climate change, which results in the creation of new policies. The second effect is that sometimes scientific cooperation or competition influences international relations, especially bilateral relations between states. At the same time, technology impacts international relations in four ways. The first is that innovation gives new options and abilities, such as was the case of nuclear weapons. The second influence is the diffusion of technology, which may lead to the proliferation of weapons of mass destruction. Another effect, which corresponds to the realist view, is technological competition among states, as seen in arms races. Lastly, the capacity to manage technology and the ability to innovate, as expressed by indicators of technological progress, affect not only economic but also political power. On the other hand, there are several direct and indirect effects of IR on science and technology; for example, a direct influence is the international agreements on the protection of intellectual property or indirectly, through the need for technology to adapt to the demands of the marketplace or other policies and regulations (Weiss, 2005, pp. 298-299).

This triangular relationship demonstrates that technology is not purely an exogenous variable, but fundamentally a product of political competition. Technology influences the architecture of the international system, by redefining the limits of state power, the speed of diplomacy, and war conditions, while at the same time the anarchic international system guides scientific progress, as states consume resources into innovation to achieve survival.

According to Weiss, there are four primary parts of the international system affected by science and technology; “its operational processes, its substance, its architecture, and the information, ideas and perceptions on which it is based.” (Weiss, 2005, p. 299) This research will mainly examine the first and third of these aspects. The first, namely the operational processes, include, among others, diplomacy, war, and intelligence. As Van Creveld argues, technology constitutes one of war’s inseparable elements, as it affects every level of it; among them planning and intelligence, as well as command, leadership, and strategy. (Van Creveld, 1989, p. 1)

Distinguishing between military and civilian technologies has become increasingly difficult. Technologies, like the railway, the jet engines, or even the Internet, prove this. Indeed, as we are moving further into the information age, civilian technologies are having a growing effect on the conduct of war. These are practically dual-use technologies. (Cohen, 2002, p. 247) Hence, equally important in warfare are also major tech firms, which “are essentially dual-use assets, in the sense that their civilian technologies can be repurposed as powerful weapons of asymmetric warfare.” (Helberg, 2020)

The architecture of the international system is also greatly affected by innovations. Specifically, they influence its structure by reordering the distribution of power among states and by empowering non-state actors like private firms or even terrorist groups. In addition, technology affects basic concepts of international relations, such as security, by expanding its content with new threats or, in the case of power, by enhancing the significance of “soft power.” Finally, innovations have a substantial impact on the international system as they can alter bilateral and multilateral relationships among states and other actors by rearranging military and economic power, creating new strategic resources, like uranium, offering new tools for collaboration and new places for cooperation and competition, such as space. (Weiss, 2005, pp. 301-303)

1.2 Technology through (Neo)realism and liberalism

1.2.1 The neoliberal approach

There is no denial that digital interconnection is an unavoidable reality, as instantaneous global communication, tight economic relations, and the architecture of networks seem incompatible with warfare. However, the great power competition unfolding today, in artificial intelligence, semiconductors, and digital infrastructure reveal a different reality. While technological interdependence expands, states seek more aggressive strategies of technological decoupling, weaponize economic networks, and accelerate arms race in domains that the liberal theory proclaims as fields of cooperation. This contradiction presents a paradox that liberal institutionalism struggles to explain, as increased connectivity is accompanied by increasing strategic competition.

Following the liberal tradition, Keohane and Nye, Jr. argue that economic interdependence fosters peace in global politics. Based on the notion of complex interdependence, they claim that the established and multichannel interconnection among states and societies raises the economic opportunity costs of conflict, while there is no hierarchical order of issues, and the military force is not an option (Viotti & Kauppi, 2012, p. 144), as such a disruption could jeopardize important mutual gains. Additionally, they offer the hypothesis that digital technologies reinforce this dynamic by reducing transaction costs, increasing information transparency, and producing mutual vulnerabilities that increase the cost of conflict. As a result, "soft power" comes to play a more substantial role in global affairs than "hard power", while power is being diffused to more actors in the international system. (McCarthy, 2015, p. 23)

Global information and communications technology enhanced their previous assumptions on power and interdependence. Liberals saw a democratization force in the diffusion of Internet, and the emergence of social media later, which even allowed the fall of established political elites. (Eriksson & Newlove-Eriksson, 2021, pp. 8-9) On the other hand, expanding the limits of liberal optimism, one can assume that the greater the amount of information available to actors, the easier it becomes to make mutually beneficial decisions, as transparency increases; uncertainty regarding the intentions of other actors is reduced, thus mitigating the security dilemma. Reality though, especially after Snowden revelations in 2013, showed that global interconnectedness through cyberspace instead of enhancing democratic forces, it augmented much stronger and far more intrusive systems of surveillance and unprecedented political control, making even liberals to reconsider their position. (Eriksson & Newlove-Eriksson, 2021, p. 9)

Liberalism, through economic and other forms of interdependence and interconnectedness observed among states and other non-state actors, claims that state adopts a less aggressive stance, even peaceful at times. (Viotti & Kauppi, 2012, p. 130) Extending this argument to technology, that means that AI development offers an opportunity of sharing datasets, computational resources, and enabling collaborative research among nations. If a state avoids participating in the global AI ecosystem, then this becomes self-defeating, as it loses the potential absolute gains from its participation.

Technoglobalism[1] complements this perspective; isolating a nation from the worldwide ecosystem creates liabilities rather than security, as barriers obstruct investments and cause the skilled workforce to migrate to foreign markets. Advocates of this theory maintain that open trade and financial integration reduce the costs and allow the leverage of complex supply chains. Eventually, innovation thrives when companies can profit from a global environment that nurtures openness and not seclusion. (Schoff, 2020)

However, AI systems have a transformative effect on balance of power, becoming a “power amplifier” for rival states. While the same system can be used to locate incoming missiles, it can also be applied in an offensive drone. This duality between defensive and offensive scope of AI, increases the security dilemma, as there are many obstacles in recognizing true intentions of adversaries who use this technology. Even if international norms were applied, it would be really difficult to identify any misuse, given the obscure dual nature of AI. (Saghir, et al., 2025, pp. 97,103,108) Therefore, it would be flawed to assume that states will seek absolute gains rather than relative ones, when security is at stake.

1.2.2 Big Tech and the techno-liberal view

The emergence of Big Tech companies and the accumulation of great economic power by them challenge the assumptions of classical IR theories. These private entities which control immense resources, and worldwide influence and interests, seem to be now part of contemporary politics, not just as participants but as policy makers, a role historically attributed and claimed by nations. (Khanal, et al., 2025) This conflicts with neoliberal institutionalism, which acknowledges nonstate actors, such NGOs and international corporations, but deems them secondary to state authority in regard to security and survival.

Major technology companies are disrupting this hierarchy, emerging as geopolitical actors who rival the traditional nation state in influence, controlling substantial digital infrastructure, military technologies, and data systems that

[1] The terms of technonationalism and Technoglobalism were coined by American economist and former U.S. Secretary of Labor Robert Reich, first appearing in his article “The Rise of Techno-Nationalism” in 1987.

were once exclusively state domains. The provision of Starlink and Palantir's military targeting software to Ukraine, demonstrate how these private actors can deliver core military and governance functions. Under these circumstances, a hybrid sovereignty is created, where states still set the rules through law, but often find themselves exercising their political power through corporate intermediaries. (Csernatoni, 2025) This is a form of authority that transcends the traditional Weberian monopoly on violence; it is in fact a monopoly on computational capability.

Pfister and Yang, tried to explain this dynamic in 2018, deploying the notion of technoliberalism[2], which they see as the intensification of neoliberal governing rationalities through digital computational technologies. They formulated five theses on this matter, with the most important being that "technoliberalism replaces public, democratically accountable power with the private, technical expertise of digital technology firms", as well as the hypothesis that "technoliberalism intensifies the commodification of attention, resulting in undemocratic forms of "noopower"". That is the manipulation of people's attention through feedback loops and algorithmic curation[3], as a form of power that exceeds what democracies can legitimate and citizens can adequately resist.

These circumstances create a paradox for liberal theory, as the more digitally integrated the global system becomes, the more concentrated power becomes in the hands of those who control the infrastructure, while democratic accountability weakens. New structures of international economic and technological interdependence, may limit state sovereignty if these ties become one sided. (Edler, et al., 2023, p. 5)

1.2.3 "Weaponized Interdependence": A challenge to Liberal IR theory

States which control substantial parts of digital infrastructure, such as the United States, are exploiting the asymmetries the deeply digitally interconnected world creates. They are weaponizing this control to gather intelligence and exercise coercion to support their interests; to achieve this, they are using data easily accessible in banks and internet terminals, as well as smartphones. This kind of accessibility creates a panopticon effect for states that have such access, giving them advantage of strategic importance in political affairs, as information and structural asymmetries emerge among

---

[2] As the authors mention, the term was coined by Thomas Malaby in 2009, who defined Technoliberalism as "a distinctive combination of distrust of vertical authority, faith in technology, and faith in the legitimacy of emergent effects".

[3] The automated process platforms use to select, sort, and present content (like posts, products, or videos) to users based on data analysis, aiming to personalize experiences and maximize engagement, but often creating filter bubbles, reinforcing biases, and shaping collective memory by favoring sensational or familiar information over diverse viewpoints.

nations. This phenomenon is called “Weaponized Interdependence”, coined by Henry Farrell and Abraham L. Newman, who claim that “states with political authority over the central nodes in the international networked structures through which money, goods, and information travel are uniquely positioned to impose costs on others. If they have appropriate domestic institutions, they can weaponize networks to gather information or choke off economic and informational flows, discover and exploit vulnerabilities, compel policy change, and deter unwanted actions.” (Farrell & Newman, 2019)

Hence, this argument demonstrates that the structure of digital networks itself is not neutral. Contrary to Keohane and Nye’s predictions, the architecture of the Internet, financial messaging systems (SWIFT), and semiconductor supply chains, reveal a tendency of centralization and the concentration of chokepoint power in the hands of whoever controls the hubs. The same applies to AI and Big Data; as Farell states, if the U.S. achieved the development of Artificial General Intelligence (AGI) first over China, that would create the right circumstances of long-term dominance, as the technological advantage would be tremendous (Farrell, 2025). Similarly, cloud hegemons, such as Google and AWS, through their dominance over AI training infrastructure and data networks, give the opportunity to their home states to pursue political gains by leveraging corporate dominance (Rikap, 2024).

1.2.4 The Realist logic

A fundamental disagreement between liberal and realist theories is about the way states calculate costs. Liberals argue that absolute gains matter the most, as all parties benefit from cooperation, thus cooperation is the rational choice. Contrarily, realists mark interdependence as a reason for increased conflict probabilities, given the observed asymmetries in dependency among involved states. Lower dependency means opportunity to coerce adversaries exploiting their vulnerabilities to increase gains, and for the realist view relative gains are the target, meaning that states aim to increase their power in relation to the other parties. (Levy & Thompson, 2010, p. 73)

Neorealist theory suggests that states compete in anarchic international system, and as Waltz (1979) argued, the fact that there is no central authority in global affairs, states are obliged to adopt self-help to survive, augmenting also their relative power. Absolute gains from cooperative research, for instance in AI, would be insignificant if China developed better AI capabilities than the USA, as these gains would be distributed unevenly. States will not measure their success by what they gained, but by comparing their gains to those of their adversaries (Saghir, et al., 2025, p. 97).

In this aspect, the “Weaponized Interdependence” theory as a structural theory that acknowledges mechanisms of coercion based on asymmetries, complements the neorealist theory. The chokepoint effect which is imposed by political powers that have possession of crucial nodes, exploiting vulnerabilities of their adversaries, proves that states prioritize relative gains. The competition observed in the semiconductor supply chain demonstrate this choice; if the USA confine chip exports to China, that is not imposed by market dynamics but as a tool of strategic coercion, and mainly to obstruct China's technological rise.

Furthermore, examining the nature of AI and the deep learning systems, one can realize there is a substantial difficulty in recognizing if these technologies are in compliance with any AI normative framework. (Saghir, et al., 2025, p. 103) There is no guarantee upon which rules an AI system is deciding, nor the exact parameters its neural network has considered. Contrary to conventional arms, the characteristics of AI military systems can be obscured, which means that states must act based upon the worst-case scenario, hypothesizing that other parties have better AI arms.

Horowitz argues that this intangible characteristics of AI development make threat assessment more complicated. While conventional arms are more visible, measuring an adversary's progress in AI is a difficult task; this is why states have to "assume the worst". This dynamic is intensified when a state has "the advantage of the first-mover" especially in military innovations. The scholar also notes that commercial technology diffuses rapidly, while complex military algorithms may be "excludable" technologies that are difficult to replicate; that would have a decisive effect on balance of power, providing advantage to the first that integrates such an exclusive military innovation. (Horowitz, 2018)

This is better understood through the theoretical lenses of Neoclassical Realism. As the distribution of power continues to be the primary driver of international politics, being an "independent variable", this power does not materialize into policy instantly. State perception is the key here along with domestic structure, as the "intervening variable". Therefore, policy being the "dependent variable" is not determined directly by the real distribution of power, but by the perceived distribution of power and the perceived intent of the adversary (Wu, et al., 2024). Since AI is a "black-box" (Johnson, 2019), and states have great difficulty in identifying the characteristics of such technologies, threat perception may play an even more crucial role than real power in decision-making.

1.2.5 State sovereignty and power Vs. Big Tech latent power

Despite the rise of technological behemoths and their economic superpower, states remain the primary actors in international relations, exercising power to secure their interests. More importantly, corporations not only do they not overcome state sovereignty, but also, they are subjected to the violence monopoly and legal authority of the state.

Political forces are subduing these private hegemons. As Evgeny Morozov argues, Silicon Valley has been “tamed”, as these leaders abandon protest state actions, adopting a more conforming attitude towards state administration imperatives. (Durand , et al., 2025) This alignment was symbolized by the attendance of the second inauguration of Trump by technology leaders, such as those of Amazon, Google, and Apple. Furthermore, the subsequent offensive trade policy measures at a global scale, unveil the relationship between state and big corporations, as the state chooses under certain circumstances to utilize policies that misalign with pure economic corporate interests. (Gabai, 2025) In authoritarian regimes, it is even more apparent that the state holds on its power, as China’s crackdown on Alibaba in 2020 has shown (Kang, 2021).

Beyond the dynamic of state-private corporations’ relationship, Big Tech power is attributed to the state means of geopolitical competition, as seen through the realist view. These corporations are producers of “strategic national security assets”, thus enhancing America’s national security, as they play a vital role in technological competition with China. (Aka, 2025) Moreover, USA is determined to keep its financial hegemony, so it directs technological development through legislation to achieve this; this is the approach for stablecoins, as the US administration through the GENIUS Act (U.S. Congress, 2025) seeks to ensure that cryptocurrencies are backed by U.S. Treasuries. (Durand , et al., 2025) This also applies to technological power; the U.S. government considering semiconductors as a strategic asset, will invest $8.9 billion in Intel (Intel Corporation, 2025), poised to enhance national security and to ensure staying on the cutting edge of AI globally.

Consequently, it is evident that political power precedes economic power. States have the power to coerce tech giants into compliance, while at the same time they utilize private sector capabilities to influence traditional geopolitical rivalries. This means that the latent power these companies possess is ultimately part of the state’s political power; while exercising its sovereignty, the state delegates power to private entities, in order to satisfy its strategic interests.

1.2.6 Theoretical Conclusions

This thesis argues that neorealism has a superior explanatory capacity, being a theory that recognizes technology’s role in international conflict; as technological interdependence creates new ways, through which the security dilemma is fueled. Therefore, there is no question that technology matters in global affairs, what is for debate is how countries fare in this aspect under anarchic conditions. The neoliberal view, as seen in Keohane and Nye’s concept of complex interdependence, lacks the explanatory power to address this issue. On the contrary, neorealism and neoclassical realism provide a better explanatory framework for the role of technology in global affairs.

Realism recognizes that technological development occurs within the structure of the anarchic international system and is affected by the competition this system creates. In this sense, technology is endogenous to the security dilemma, and states must resolve to self-help to deal with threats developing or manipulating technology to achieve this. This means that states develop technologies not because they are efficient, but because rivals develop them or because they have to as an answer to the conceived threats.

Another fundamental fact is the continuous competition among great powers. The strategic decoupling phenomenon clearly shows this as a means to foster national security. For China technological power is part of national power and the competition observed at a global scale. As the United States observed the rise of China's power, especially fearing the probability of developing superior AI innovations, they instigated policies that would allow the technological decoupling by restricting semiconductor sales to China. This was a rational choice, as the US wants to maintain the balance of power. (Wu, et al., 2024, p. 202) While the liberal approach would be to avoid decoupling, as cooperation brings higher absolute gains, this is insufficient when security is at stake. Eventually, realists claim that states' motivation is power, and the economic opportunity costs of war are minor when thinking of the long-term struggle for power. (Levy & Thompson, 2010, p. 73)

Governance is also a field where realism seems more sufficient. Liberal institutionalism can explain why cooperation contributes to AI safety research, as all states have common interest in eliminating the probability of an AI disaster (Saghir, et al., 2025, p. 109); however, as realist theory proves, such mechanisms have minimal impact as relative gains is the target. If AI supremacy is destined to determine military dominance in the future, there is no state that would voluntarily stop or share research, as that could set it to an inferior position.

Furthermore, connectivity among nations intensifies rather than resolves the security dilemma. The same applies to technological interconnectedness, as it creates new ways for security dilemma to unfold. Even if a state had more information about the adversary's capabilities, that would not cause reassurance, but a race to improve its capabilities to make things at least even. This becomes apparent even more in the digital era; as the Weaponized Interdependence theory showed, the very architecture of global computation depends on networks that for some states they are controlled by competitive states. In the end, states have acquired a new way to exercise coercion using their infrastructural or network power by weaponizing their hubs as chokepoints.

This does not mean that conflict is inevitable and that technology, such as AI, cannot be developed and guided to more cooperative goals. Instead, it means that the actors and the tools which liberals are promoting cannot overlook the structural conditions leading states to competition. This is why liberalism offers an insufficient explanatory framework in this aspect, while realism achieves to interpret the current state of IR affairs, as well as the role of technology in this aspect.

1.3 Technology and the status quo: A realist approach

1.3.1 Technological innovation and information superiority

Examining international security dynamics throughout history reveals that technology, especially military, has always played an important role in strategic thought and the balance of power. Innovations have functioned as crucial multipliers of power; Thucydides attributed the emergence and expansion of the Athenian Empire to its mastery of maritime technology and trade, which allowed the projection of power and threatened Spartan military supremacy in ancient Greece (Platias & Koliopoulos, 2010). This rise in naval power, along with financial resources and advancements in military infrastructure, transformed military force, enabling the formation of powerful alliances and expansive seaborne empires (Gilpin, 1988, p. 598). In this sense, maritime technology favors offense, while infrastructural development, such as the "Long Walls" of Athens contribute to defense and deterrence (Platias & Koliopoulos, 2010, pp. 45-46).

Another aspect in achieving dominance is informational superiority, which in the age of AI and Big Data seems even more prominent; Sun Tzu considered "foreknowledge" as essential for effective command that leads the wise general to victory. This knowledge is in fact precise insight regarding the enemy's situation, especially a deep understanding of their plans and intentions, as well as their own strengths and weaknesses, and the environment (McNeilly, 2015, p. 62). However, a SWOT analysis is not enough to succeed in informational dominance; the other half of the effort is to deny the adversary's access to this knowledge through deception (McNeilly, 2015, p. 82).

The necessity of information dominance still aligns with modern strategic goals, as states seek to increase their capacity in gathering, processing and disseminating information with increased speed and accuracy compared to the adversary. Contemporary and future combat operations are increasingly characterized by the digitalization of command and control in order to establish superior situational awareness, utilizing advanced innovations, such as drones and deepfakes to extract or manipulate information. Opponents compete in information warfare to degrade data infrastructure of the adversary through cyberattacks and deception while protecting their own intelligence capabilities. Ultimately, information dominance can be achieved when a country has the ability to overcome the adversary's decision-making process when it maximizes its own understanding and invalidates the enemy's intelligence capabilities (McNeilly, 2015, p. 87). In this context, intelligence capability is not based only on the analysis of the current situation, but also on behavioral prediction of the adversary's future actions because of AI innovations (Saghir, et al., 2025, p. 101).

1.3.2 Technology and power transition

Technological progress plays a crucial role in "uneven growth" among states, which means that it is one of the main driving forces affecting the redistribution of power and the potentially subsequent change in the international order, known as hegemonic war (Gilpin, 1988). The increasing difference in growth undermines the existing international hierarchy, leading to war as the perceived shifting balance of power can compel the declining state to initiate war while it still thinks it has advantage over the enemy. Eventually, the conflict between the primary power and the rising one may cause a new structure of the international system shaped by the victor.

Drawing on the theoretical framework Gilpin established, it is evident there is a technoeconomic gap, caused by the differential growth of technology as scientific and technological progress spreads unevenly across the world. This phenomenon is observed as more developed nations acquire relative superiority compared to those developing at a slower pace (Mallik, 2016, p. viii). This uneven diffusion can cause imbalance in the international system through several mechanisms.

Threat perception is augmented as countries compete to improve their position in the international system; the resulting power divergence among them is treated as a threat to their sovereignty. Concerning technology this means that competing countries seek to increase their technoeconomic capabilities and at the same time suppress their adversaries' potential. The latter is often accomplished when advanced countries shape norms and standards, which forces less developed countries to either follow them through alliances or to choose a path of disturbance effect on others to gain power (Mallik, 2004, p. ix). However, this imbalance can be also manifested in a converse way for hegemonic states in the 21st century; computational developments and information diffusion across the globe cause a loss of technological edge for these states, affecting security perceptions (Mallik, 2004, p. 4).

Additionally, there is another characteristic of innovations that affects the distribution of power. Emerging powers are often favored over hegemonic states because of technology diffusion and the "late-mover advantage". Challenging states often act as "smart buyers" seeking to acquire technology knowledge through the procurement, limiting the technology divide with the technologically advanced nations. While this is true, that does not mean that hegemonic powers, such as the USA, are willing to lose their technological prowess for economic gains (Mallik, 2004, p. 121). This is why they impose measures to protect their supremacy, with export control being one of the most prominent.

1.3.3 The role of internal factors in Neoclassical Realism

Examining internal variables in state behavior within a neoclassical realist framework provides an enhanced understanding of the reasons states react differently in systemic pressures, especially regarding technological competition. While structural realism suggests that the anarchic international system constantly pressures states to maximize security, neoclassical realism argues that there is no flawless causal relationship between functional competence and foreign affairs (Rose, 1998, pp. 146-147). States are often slow to respond to systemic influences as these have to be filtered through intervening variables, such as the way political leaders perceive them and the structure of the state (Rose, 1998, p. 152).

State power, which is the power a government can harness from its nation's power to serve its objectives in the international arena, defines the speed with which it responds to changes observed in this system (Rose, 1998, p. 162). This means that a country that has the same or equivalent material capacity with another country will not necessarily act the same; the weaker one having an unresponsive administration or divided political leaders may delay the widening of its foreign policy goals caused by an increase in its material capacity (Rose, 1998, p. 167). Moreover, "organizational capital" plays a crucial role in this matter, as organizations need immaterial assets that enable change when innovations become available for utilization. Bureaucratic obstacles are often seen in older organizations, where "veto points" hinder the integration of innovations (Horowitz, 2010, p. 10).

Furthermore, threat perception of political elites defines the direction and nature of the state's technological policy (Wu, et al., 2024, p. 202). This can enable the transition from technoliberalism as a strategic approach to technonationalism assuming threats are rising. The latter is defined by the implementation of policies that are set to protect and sometimes enhance a nation's technological edge and industrial know-how for national security reasons, as well as for the augmentation of economic power (Schoff, 2020, p. 17). According to neoclassical realist analysis, the implementation of such policies is shaped by the interplay between two variables; the objective distribution of technological power as the independent one, and the subjective threats assessments of political elites as the intervening one (Wu, et al., 2024).

In particular, when a state views a rising power in a collaborative way, this favors engagement and shared technological growth. However, as the gap among them narrows, the hegemonic state starts to view its partner state as a competitor or even a challenger, once the balance has shifted significantly (Wu, et al., 2024, p. 201). A state that views a rising power as a challenger, driven by fears of losing its supremacy and disrupting the established order it created, often adopts technonationalist policies. These can be either defensive in nature, such as export controls, or offensive by implementing direct support measures for homegrown innovation (Schoff, 2020, p. 17).

The state's power, especially its "national political power", namely "the ability of state leaders to mobilize their nation's human and material resources behind security policy initiatives" (Rose, 1998, p. 163), influences the conditions of implementing strategies of technonationalism. If there is a solid and well-organized state structure, it is easier to enforce standards and processes on technological companies, whereas a weaker state structure would result in delayed or incomplete and inconsistent implementation of such policies.

1.3.4 The offense-defense balance

The Offense-defense theory founded by Robert Jervis claims that current technological conditions determine if attack or defense is favored, which subsequently influences the security dilemma (Lieber, 2000, p. 71). Historically, technological innovations can be categorized based on mobility and firepower, where the first favors offense creating "first-move advantages" and the right conditions for preemptive war (Jervis, 1978, pp. 188-189). On the other hand, innovations that increase firepower tend to favor defense, making states feel more secure (Lieber, 2000, p. 80).

The emergence of nuclear weapons fundamentally altered this balance, as they are traditionally considered defense tools, prioritizing "deterrence by punishment" (Lieber, 2000, p. 97). These weapons are considered superior in defense, as it is far easier and costs less for a state to maintain the ability for a retaliatory second-strike than to deprive the enemy of its ability to deter. This cost of conflict becomes too excessive for a state to bear, greatly reducing the possibility of a major war among great powers. However, the emergence of AI and automated systems challenges this defensive environment. These technologies enhance mobility by compressing the time available for decision-making, which gives the first mover a significant advantage. In this sense, the concept of mobility is expanded to include the velocity of information processing available to actors in the global arena.

To better understand the impact of technology on the offense-defense balance one should consider three dimensions. Firstly, examine technology as a structural material constraint; technology is not just a tool but a structural factor that defines the ability of actors in terms of material power to interact with each other in the international system (Viotti & Kauppi, 2012, pp. 40-41). In this view, certain technological eras emerge, creating each time a different offense-defense balance that determines how easy or costly it is to adopt an offensive or defensive stance towards adversaries.

Furthermore, to avoid an approach of technological determinism assuming that material power suffices to foresee the result of a conflict, the concept of "force employment" is utilized within the neoclassical realistic approach (Horowitz, 2010, p. 7). This concept refers to the question of how organizations, especially militaries, choose to arrange and coordinate their resources, or as Horowitz argues in his "adoption-capacity theory", if organizations have the necessary "organizational capital" to adapt and integrate crucial innovations (Horowitz, 2010, p. 10). This explains why countries with similar technologies may have different security outcomes.

The third aspect is threat perception; as an intervening variable it reveals that states adopt techno-nationalist or offense strategic approaches when the gap in terms of material power narrows to a point where it causes a perceptual reaction affecting the adversaries and the international system. This logic sustains the argument of the offense-defense balance that technology may give an actor a first strike advantage or defensive dominance, but also it adds the subjective element of how internal factors such as political leaders interpret the state material power.

Finally, in this sense technology is treated as a structural material of a nation's power, whose impact is moderated by state behavior producing that way a specific balance or imbalance in the international arena. This approach enables a deeper analysis of how innovations can alter the global power equilibrium, while rejecting a fully deterministic view of technology in international relations.

1.4 Technological mechanisms and the balance of power

This chapter examines key processes through which technology and innovation influence power distribution in the international system. As the world becomes increasingly digitalized and augmented by AI, greater emphasis is placed on information power, technological diffusion and dependence, dual-use technologies, and normative power in the technology sector as a means of achieving technological supremacy rather than fostering cooperation.

1.4.1 Information power

After the information revolution observed in late 20th century and the continuous development of Artificial Intelligence, national power is being fundamentally redefined. In this context, information power does not just refer to knowledge possession, but to the capacity of a state to secure strategic advantage by influencing perceptions, decisions, and behaviors based on the available information technology and information content (Kohara, 2005, p. 41). This can be accomplished with the use of three main functions; particularly, the collection and processing of data into actionable intelligence, the protection of the infrastructure that makes this possible along with the knowledge gained against adversaries, and finally the projection of tailored narratives to support national interests (Piercy, 2023, p. 2).

To assess how Information Power is changing in the current technological environment, it is necessary to examine these changes at three stages, namely the volume of information, the processing speed of information, and its integration through connectivity. The informational volume has increased dramatically since the internet expansion across the globe, moving from fragmented information to information omnipresence. Furthermore, the development of powerful sensing technologies, such as high-resolution satellites and advanced acoustic sensors, and Big Data pools has provided states with unprecedented access to information even from great distances (Gompert, et al., 2014, p. 31). This kind of innovation greatly reduces blind spots at least in the natural world, allowing information to flow to governments anywhere at any time.

Subsequently, the exponential growth of data is accompanied by an increase in computational power that handles this information (Gompert, et al., 2014, p. 32). Artificial intelligence and the use of algorithms satisfy this need for speedy processing, even real-time, to pinpoint threats at a very early stage. In other words, AI effectively can surpass human perception, which enables states to process information at a pace that is biologically impossible (Amoore & Raley, 2016, p. 4). Lastly, connectivity plays a vital role in decision making processes as information power relies much on networks in the 21st century. As is expected in the next few years, Internet of Things (IoT) will dominate future warfare establishing a vast connectivity among several military assets both living and inanimate (Lele, 2019, p. 192).

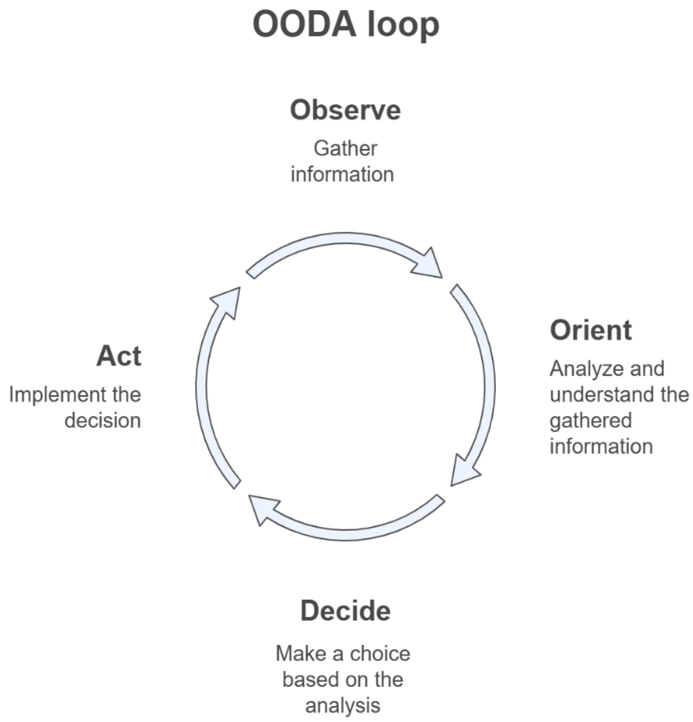

Figure 2: The OODA loop

If a state manages to effectively operate at these three stages, then it sets the foundation for decision dominance. In decision-making this is better understood by examining the OODA loop, a decision-making model developed by John Boyd in the early 1970s. According to the theory, victory depends not only on the ability to complete the loop faster than the opponent but also on disrupting the adversary's cycle for disorientation (Raska, 2025, p. 3). Today, the OODA loop is enhanced by technology and AI innovation; the Observe stage utilizes real-time and multi-source data accessed through interconnected systems, while the Orient phase has undergone a deep transformation. AI-driven data fusion and pattern recognition technologies automate information processing which limits the time needed. Accordingly, the Decide phase is increasingly dependent on AI-enabled support systems that enable predictive analytics and threat prioritization among others, hence optimizing the decision cycles while displacing in part human cognition. Finally, the Act stage employs semi-automated and networked systems capable of executing decisions at extreme speed (Raska, 2025, p. 10).

In the coming decades, the OODA loop is projected to result in "AI-Driven 'Super-OODA' Loops" (Raska, 2025, p. 10), where AI and autonomous systems will fundamentally transform the logic of decision-making cycles by automating each stage to a point that human involvement is limited to strategic oversight. As Kenneth Payne argues, an AI that completes its OODA loop significantly faster than a human or another AI will easily defeat them; hence, victory will depend on the relative speed between two AI systems (Payne, 2018, p. 181).

This dynamic creates conditions for an AI arms race, and in this case for achieving the integration of the most capable AI systems for states that want to cause strategic paralysis to their adversary, especially when it's combined with disinformation and other measures for information manipulation against them.

1.4.2 Technological diffusion

The international system is increasingly affected by the dynamics between the rapid spread of innovation and the efforts of hegemonic states to moderate this spread by implementing measures of strategic denial. This section analyzes technology transfer and diffusion, pinpointing how the flow of information is often exploited or weaponized as a crucial aspect of modern power.

As it was mentioned in the 1st chapter, technology is not just a commodity, but also it includes the design and the manufacturing know-how to produce an object or service. Furthermore, while trading products provides a temporary satisfaction of economic and consuming needs that creates a dependent relationship between the buyer and seller state, transferring the necessary technology to the buyer state discontinues or limits this dependency by satisfying both immediate and future needs (Bucy, 1980, pp. 134-135). Depending on the quantity and the quality of exporting technology, this can have a substantial impact on security, economy, and foreign affairs.

In the current globalized era, research and development has moved from the government-led model to innovation by the private sector. Technologies like semiconductors were developed for commercial markets years before being integrated into weapon systems. This shift has created a "transnational research and innovation ecosystem", where critical scientific progress follows transnational capital flows increasing the difficulty of monopolization by the states (Lewis, 2019, p. 3).

If technology transfer refers to the act of sharing know-how, technology diffusion describes the broader process by which these innovations are spreading through global channels over time among the international system actors (Horowitz, 2010, p. 19). The nature of modern technology, relying on intangible software and digital knowledge, has facilitated this global spread utilizing "high-speed networks and connectivity" (Lewis, 2019, p. 3). Technical information diffuses across borders with such speed that hegemonic states have great difficulty in containing scientific progress; for instance, setting barriers in the global AI innovation ecosystem including Silicon Valley as its epicenter, would negatively impact American innovation (Lewis, 2019, p. 4).

However, rising powers strategically exploit this dynamic gaining the "late-mover" advantage, which means that they can adopt mature technologies without having the high R&D costs the original innovators had to bear (Horowitz, 2010, p. 51). This has given the chance to states like China, to become "fast-followers", acquiring technology through a combination of aggressive intellectual property acquisition methods, attracting foreign academic human assets, and leveraging its internal market potential, gathering that way significant latent power (Davis & Nacht, 2018, pp. 27,31).

Adopting (or not) an innovation can indeed influence the balance of power; when hegemonic states lack the financial and organizational capacity to integrate an innovation crucial for their security, their supremacy is at stake. Particularly, innovations that are disruptive requiring great organizational change, are the most threatening for great powers, as they are often characterized by organizational inflexibility. On the other hand, "sustaining innovations" as they require high financial intensity, but low organizational capacity, tend to reinforce the established power. Furthermore, the first who try to adopt an innovation can profit from relative power gains, while they keep their advantage if they maintain the monopoly of the innovation, which means that innovations that require higher organizational capacity create longer lasting monopolies. These diffusion dynamics according to Horowitz, directly affect geography, speed, and intensity of warfare (Horowitz, 2010, pp. 42-51); meaning that major military innovations often expand the geographic range of lethal force, increase the speed of mobilization, and define war intensity.

Nevertheless, great powers have also other means of strategic denial to influence the distribution of technological power in the contemporary highly networked international system. Controlling the structural hubs of the international economy, such as financial messaging, or data hubs they can achieve technological containment against their adversaries for a long time (Farrell & Newman, 2019, p. 55). Hegemonic states can exploit these technological "chokepoints" to influence the distribution of tech power by controlling these points or even by excluding their opponents from accessing them. This capability allows a great power to define how quickly a rising power can obtain critical technologies for their military systems, such as the weaponization of the SWIFT system against Iran (Farrell & Newman, 2019, pp. 66-69). Consequently, this ability is not a mere tool of punishment or simple coercion when utilized for a prolonged period, but a strategic technological containment mechanism.

1.4.3 Dual-use technologies and civil-military fusion

Throughout the previous century, technological development was driven by the imperatives the defense sector and national security dictated. The competition of the Cold War forced governments to invest in large-scale R&D programs, which had positioned the state as the main producer of critical technology (Reuven & Shamir, 2025, p. 392). Innovations, such as jet engines, were originally developed within the military industry followed by their adoption by the civilian sector. This dynamic ensured that the state had always been in control of crucial defense technology and its transfer to the market, which also affected power dynamics in the previous century (Reuven & Shamir, 2025, p. 408).

Nonetheless, in the 21st century the roles have reversed and the private sector now dominates the technological sector with the emergence of international technology giants, which spend much more than states in critical domains, such as AI and autonomous systems (Reuven & Shamir, 2025, pp. 403,405). Consequently, the state has become now the consumer, adopting commercial innovations from the market for military uses. This shift ultimately implies that the state must integrate such civilian innovations into its defense ecosystem.

The primacy of private sector in technological advancement has highlighted the importance of "strategic latency", which is the inherent and dormant military potential of commercial or underdeveloped technologies that remains unexploited until a state utilizes it for such purpose (Davis & Nacht, 2018, p. 1). Latency defines the ambivalent nature of dual-use technologies, as they can cause at the same time societal benefits and strategic disruption, such as nuclear energy and nuclear weapons. Furthermore, this dynamic concerns not only emerging technologies but also existing ones that are used together to provoke a significant shift in the balance of power (Davis & Nacht, 2018, p. 188). AI and Big data fall in the same category, being inherently dual-use technologies that allow predictive strategic awareness having the potential to change information warfare (Davis & Nacht, 2018, p. 71).

In this context, Military-Civil Fusion (MCF) is a distinct strategy that allows a state to harness this latent power by integrating a nation's civilian industrial and innovation ecosystem into the defense supply chain (Can & Vieira, 2022, p. 85). Particularly, the strategic advantage of this mechanism is the synchronization of private sector innovation with national security mandates. Authoritarian regimes or "hard states" like China have advantage in accomplishing this integration between private and public sector (Can & Vieira, 2022, p. 89), while states that distinctively separate them may face increased challenges (Reuven & Shamir, 2025, p. 406).

1.4.4 Normative (structural) power

Normative power in this context is not a tool for securing public welfare or setting a framework for cooperation, it is more a part of structural state power used for technological supremacy. According to Susan Strange structural power refers to "the power to decide how things shall be done, the power to shape frameworks within which states relate to each other, relate to people, or relate to corporate enterprises” (Strange, 1994, p. 25). In this context, technical standards are fundamental elements of structural power in the international system. Their influence comes from the interoperability, which means that products that fail to comply with established standards are difficult to enter the global market (Rühlig, 2023, p. 55). As a result, states that control these standards have the regulatory power to influence the international market in a way that increases geopolitical tensions (Seaman, 2020, p. 3).

Furthermore, this structural power is observed in initiatives like China’s Belt and Road Initiative, which includes not only infrastructure but also technical standards that will give China political leverage to achieve its geopolitical goals (Rühlig, 2023, pp. 64-65). A good example is the spread of Chinese 5G technology that creates security concerns for USA, as some experts consider the low-frequency 5G chosen by Chinese industry to be less secure than the high-frequency technology, which means that offshore military activities will have to be carried out using potentially compromised Chinese technology.

The “Brussels Effect” is also a unique manifestation of this dynamic, as the EU exploits its internal market volume to impose regulations to foreign countries and markets (Bradford, 2016). As the EU has the largest single market in the world, global corporations are forced to comply with EU standards in order to access EU consumers. In essence, companies find it more cost-effective to adopt these standards rather than diversifying their production to match different legal frameworks. This is a silent power because it is applied through the market and not through direct competition. Ultimately, this is structural power produced by the common economic interests of the EU countries, expressed in an indirect way by imposing technical standards on their adversaries.

This dynamic of “weaponized interdependence” that unfolds in the current era, shows that standards tend to be a result of great power competition between China and the West (Rühlig, 2020, p. 6). Particularly, there are two distinct mechanisms that reveal this political power (Rühlig, 2023, p. 63); firstly, there are “lock-in effects” as supplying countries can leverage the dependence that critical technology creates for buying countries for their infrastructure. Additionally, countries imposing technical standards have also deep knowledge of possible vulnerabilities of their technological products, which can be later utilized against a potential adversary affecting their physical or digital security, and even international balance of power under the right circumstances.

In conclusion, a fundamental shift in the nature of power is unveiled when examining these four dimensions: information velocity, technology diffusion control, military-civil fusion, and standard-setting. Along with advanced military assets that will be examined later in this research, structural control over networks, flows and regulations has increased significance in the international security system. In this context, technological supremacy is not defined only by military hardware but also by state capacity to shape their adversaries' operating environments exploiting technology itself. Ultimately, the strategic objective is the same; to achieve relative gains and freedom of action by constraining enemies through systemic vulnerabilities.

1.5 Measuring power in the 21st century: economic and technological determinants

1.5.1 From latent to active power

According to John Mearsheimer, power in the international system is based on two different components: latent power which is "socioeconomic ingredients that go into building military power", and military power itself (Mearsheimer, 2001, p. 81). Historically, latent power was measured by a state's wealth as well as the size of its population, as these were the two main ingredients for raising large armies. However, in the current century, technology plays a greater role in influencing both military and latent power, especially wealth.

Technological innovation has become the primary multiplier of latent and military power. The capacity of a state to excel in the fields of Artificial Intelligence, advanced computing, and semiconductor manufacturing does not only increase wealth, but also provides the necessary infrastructure for modern warfare. In this sense, states that are leading dual-use technologies, such as AI algorithms, have the necessary latent power for modern military capabilities. As Mearsheimer notes, a state must have a conversion capability, turning its "mobilizable wealth" into military, while also "producing the newest and most sophisticated technologies" that will become part of its military assets (Mearsheimer, 2001, p. 89). In the current era, this means that commercial tech industry is both a source of revenue and a reservoir of national security assets.

Horowitz argues that Artificial Intelligence is the "ultimate enabler", meaning it is a general purpose technology that facilitates innovation-making in every field, from healthcare to weaponry (Horowitz, 2018, p. 41). Furthermore, AI has the capacity (given the necessary wealth) to overcome demographic challenges by substituting capital for labor (Horowitz, 2018, p. 46). Overall, technological innovation defines latent power by functioning as a multiplier of economic power and population dynamics. Nevertheless, there is an important criterion as the state must have the organizational capacity to channel this latent potential into military power for security purposes.

1.5.2 Indicators: Assessing technological power

Measuring technological power requires a multidimensional approach that includes indicators, such as GNI (Gross National Income), R&D spending, patent output, and high-technology exports.

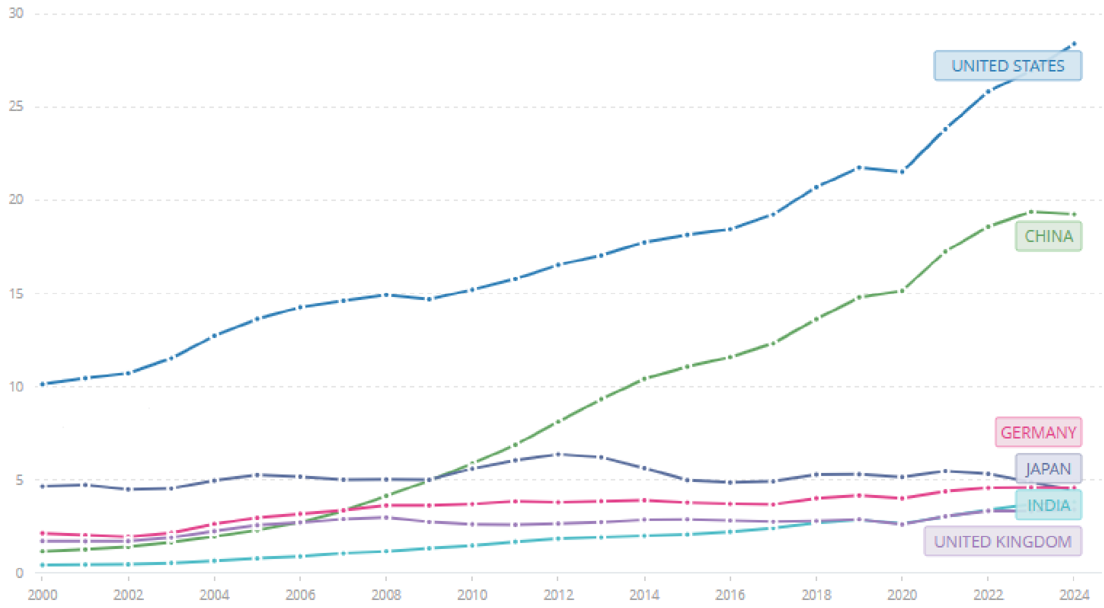

Figure 3: GNI, Atlas method (current US$) - United States, China, Japan, Germany, India, United Kingdom (Source: World Bank)

Country	Value
1 - Germany	0.42
2 - China	0.38
3 - Ireland	0.34
4 - Republic of Korea	0.33
5 - United States of America	0.32

Figure 4:Competitive Industrial Performance Index-Top 5 countries in 2023 (Source: United Nations Industrial Development Organization)

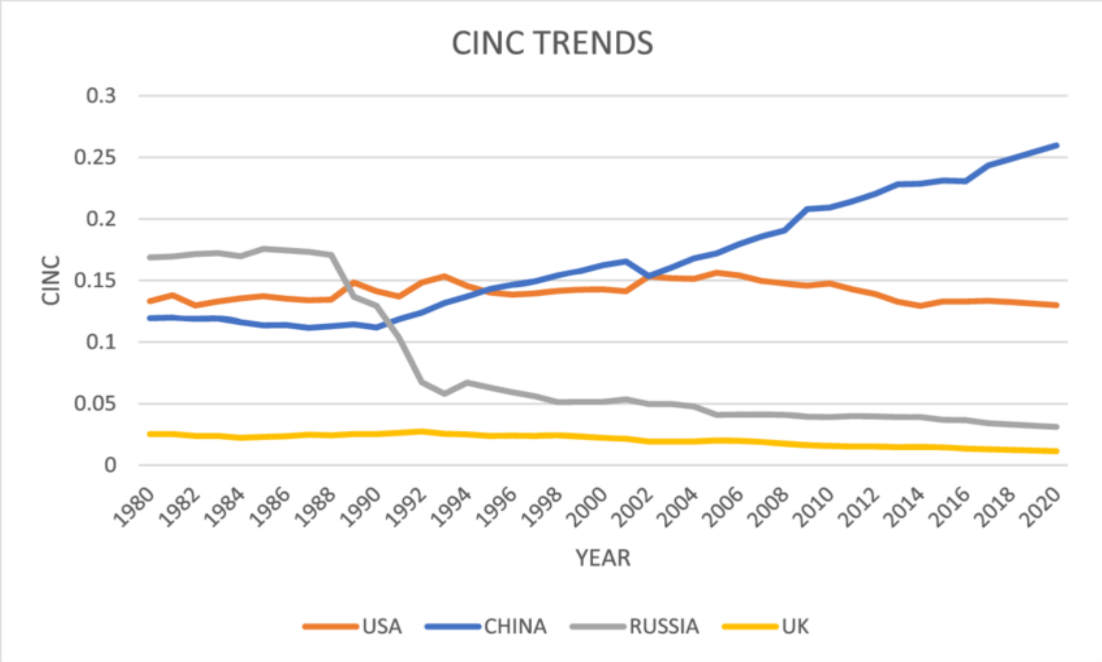

Figure 5: CINC Index Trends for USA, CHINA, RUSSIA and UK (Source: Bellos, Sotirios & Golitsis, Petros. (2023). The Nexus Between Financial and Investment Developments and State Capacity. The Case of G-20. Journal of Government and Economics. 11. 100081. 10.1016/j.jge.2023.100081)

Based on Mearsheimer's theory, the integration of Gross National Income (GNI), the Competitive Industrial Performance (CIP) Index, the Composite Index of National Capability (CINC), and the DiME index clearly unveils the shifting balance of latent power. This shift showcases the major rising power in the contemporary world, which is China. Mearsheimer originally mentioned that semi-industrialized China should not be compared to the USA based only on wealth (Mearsheimer, 2001, p. 93), but today China's GDP includes only a 6,8% of agriculture added value, and 36,5% of industry added value (CIA, 2024). Therefore, it can be argued that China has successfully converted its large population into massive wealth and industrial force, that is to say latent power.

Moreover, the Gross National Income (GNI) trends from 2000 to 2024 provide important evidence that the world is becoming bipolar or multipolar, or at least that the right conditions are being materialized. In fact, China by becoming a multi-trillion giant has gathered enough wealth for a hegemonic challenge with the USA. These conditions augment the security dilemma for the latter country, as China has continuously increased relative gains while the cost of containment for the US keeps rising. The Competitive Industrial Performance (CIP) index supports this argument, examining three aspects; "capacity to produce and export manufactured goods", "technological deepening and upgrading" and "world impact" (UNIDO, 2025, p. 32). The 2023 CIP data (Fig. 4) places China in the 2nd place behind Germany and ahead of the USA which are in the 5th place. This slight margin between them reveals that they are almost on par regarding competitiveness in the industrial sector, both producing high-tech innovations.

The CINC trends (Fig. 5) also showcase that China has already surpassed the United States in material capability long ago. However, in the past the country lacked the necessary industrial and wealth capacity; in other words, their latent power was insufficient to bring any change in balance of power. In the current era though, the high GNI and CIP scores signify that China has successfully activated its latent potential.

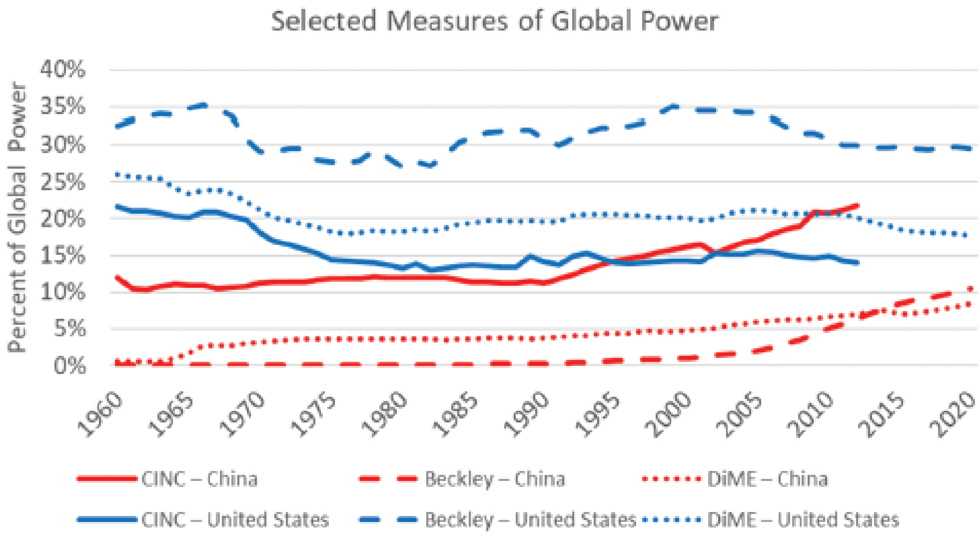

Figure 6: Comparison of Chinese and US global power according to the DiME Index, Beckley's measure, and the CINC (Source: Jonathan D. Moyer, Collin J. Meisel & Austin S. Matthews (2023) Measuring and Forecasting the Rise of China: Reality over Image, Journal of Contemporary China, 32:140, 191-206)

More recent research though tries to adopt a more comprehensive view of modern state power, including latent and military power. Utilizing the DiME index, which includes the dimensions of diplomatic representation, military spending, economic capacity, and nuclear weapons, it is argued that the CINC measurements are overstating power transition (Moyer, et al., 2023). This index presents a broader view of power changes, and more specifically that while China has not yet surpassed the USA in power, its past and current trajectory will eventually lead at least to a point of parity in the 2040s, creating a bipolar international system.

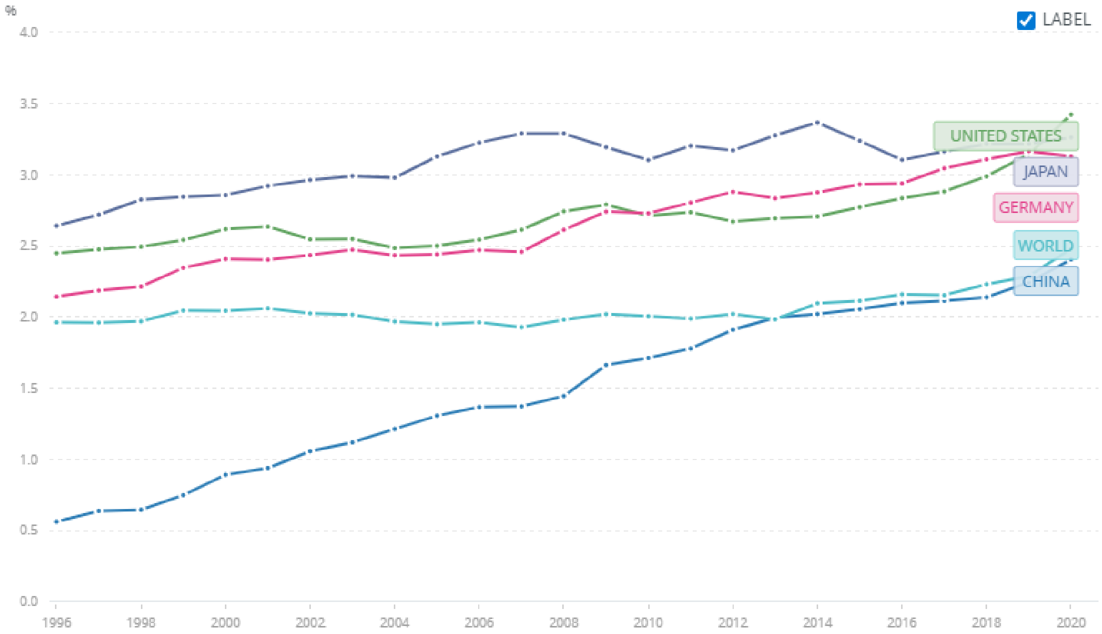

Figure 7:Research and development expenditure (% of GDP) - China, United States, Japan, Germany, World (Source: World Bank)

1.5.3 Innovation metrics: R&D, artificial intelligence (AI), and military spending

It is significant to examine how technology fits into this power transition claim. Firstly, the R&D spending (Fig. 7) reveals that competition is increasing; while the USA and some of its allies maintain or increase their R&D expenses, China is effectively channeling more assets to R&D narrowing the gap with their adversaries.

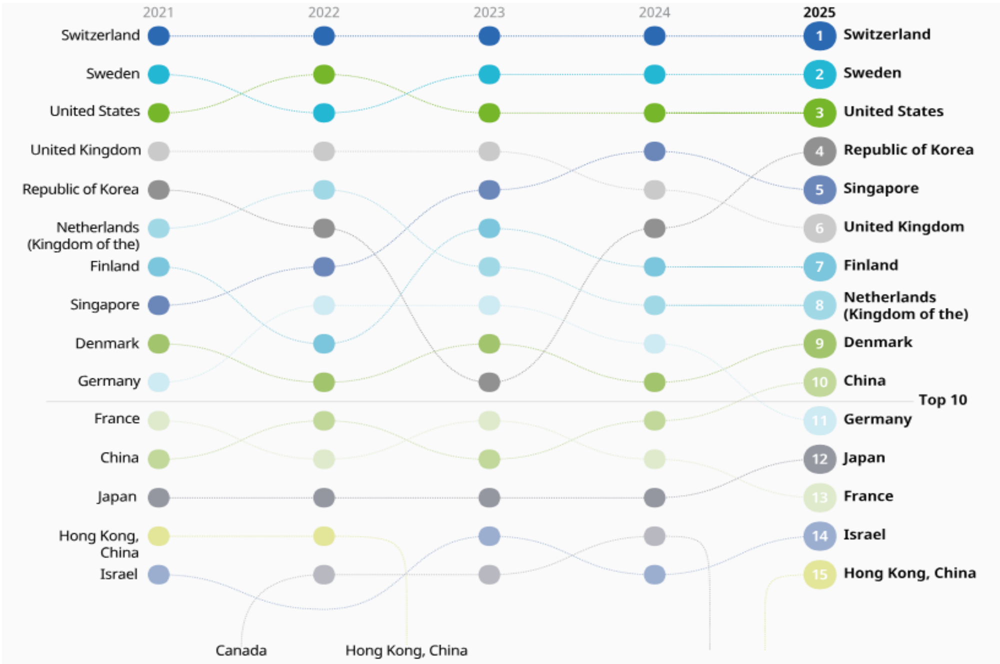

Figure 8: The GII dynamo: the top 15 innovators, 2021-2025 (Source: World Intellectual Property Organization)

Position	Country/territory	Count
1	China	44121
2	United States of America (USA)	32739
3	Germany	10956
4	United Kingdom (UK)	9909
5	Japan	6027
6	France	6054
7	South Korea	3644
8	India	2997
9	Canada	4776
10	Switzerland	4025

Table 1: Nature Index, Top 10 Countries in 2024 (Adapted from nature.com)

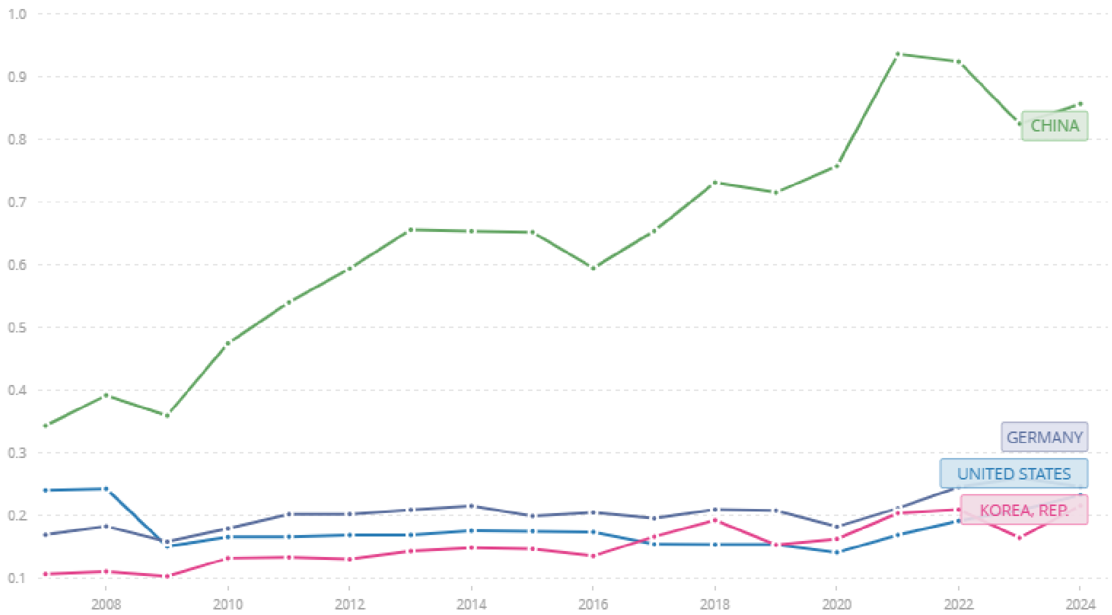

Figure 9: High-technology exports (current US$) - United States, China, Germany, Korea Rep. (Source: World Bank)

The Global Innovation Index (Fig. 8) reflects the American superiority in financial markets and startup ecosystems leading in innovation intensity (WIPO, 2025, p. 55), while it showcases the gradual ascent of China based on their world-leading innovation clusters, patent supremacy and impactful innovation hubs excelling in technologies like AI and semiconductors. Furthermore, the 2024 Nature Index (Table 1) shows that China is a leader in high-quality scientific output, while the country has an immense advantage in high-technology exports (Fig.9). In essence, it seems that the U.S. leads in design and innovation finance, while China excels in scientific volume and industrial output. Hence, it is evident that the foundations for the change of polarity in the international system have been set, as the U.S. hegemony is being threatened by the Chinese rise.

An emerging technology that is affecting this balance is Artificial Intelligence, and recent studies support this. Technologic power in the current digital era is mainly based on three interconnected elements: Artificial Intelligence models, computing power and hyperscale data centers (infrastructure), and the control of semiconductor supply chains. The most recent data unveil an important asymmetry; while the United States retains a structural advantage through a thriving innovation ecosystem and “chokepoint” control, China is challenging this dominance through rapid scaling and technology diffusion.

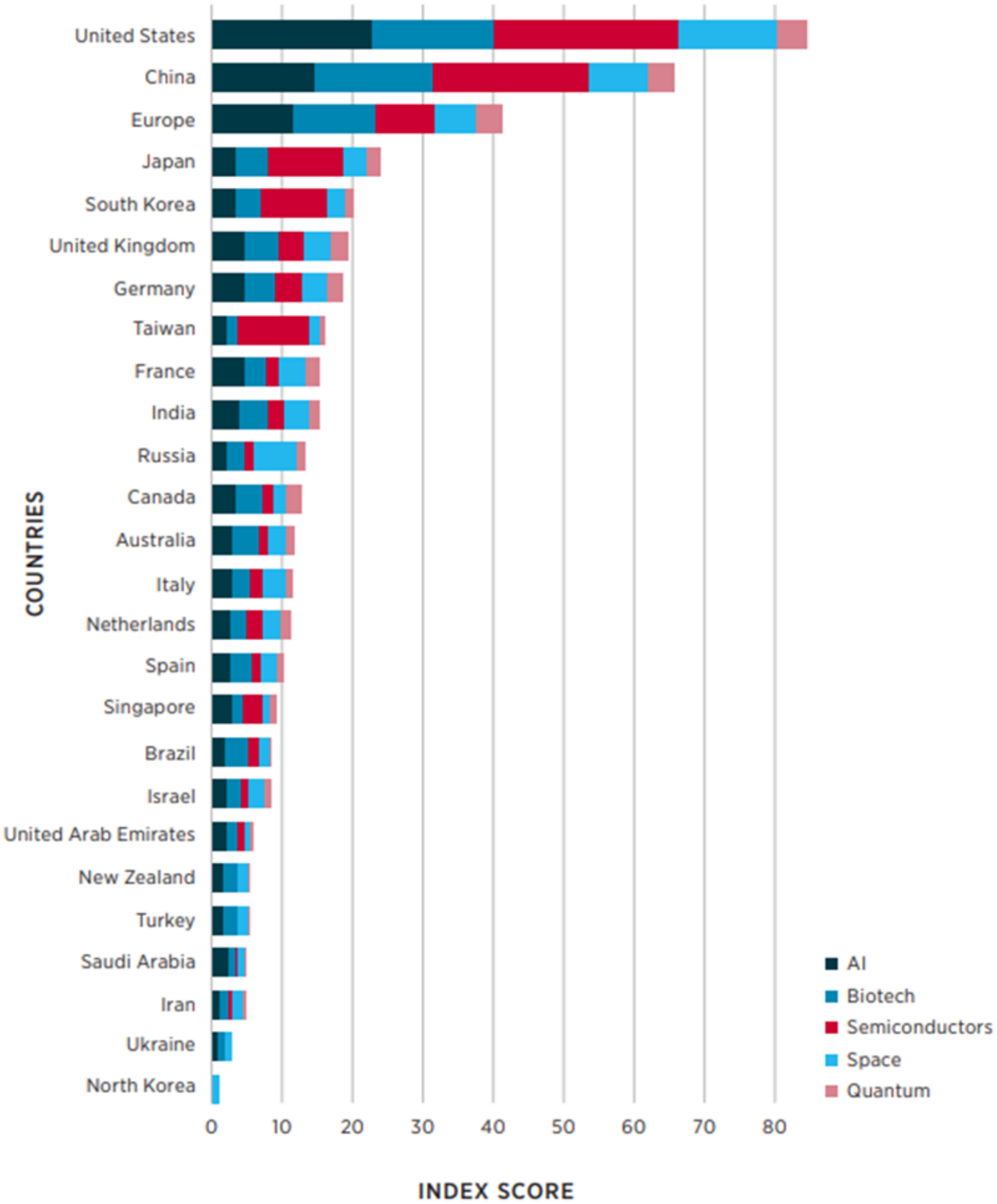

Figure 10: Critical and Emerging Technologies Index (Source: Harvard Kennedy School: Belfer Center for Science and International Affairs)

Firstly, AI competition is mainly defined by the two pioneering countries. The United States has secured its technological hegemony through immense private investments. In 2024, they have spent $109 billion dollars, which is almost 12 times more than China's $9 billion (Maslej, et al., 2025). This financial endeavor was successful as the U.S. maintained their leadership in producing significant AI models, particularly 40 models in 2024 Vs. 15 from China. Regarding research output, in 2023 China had 23.2% of global AI publications and 69.7% of AI patents. Another indicator worthy of mentioning is that important benchmarks such as the MMLU benchmark which evaluates the knowledge and reasoning capacity of large language models (LLMs), have almost reached parity for American and Chinese AI models by the end of 2024. This metric indicates that while the U.S. are spending much more financial assets, China has a "fast follower" strategy that allows them to have similar technical capabilities with 1/12 of the USA's costs.

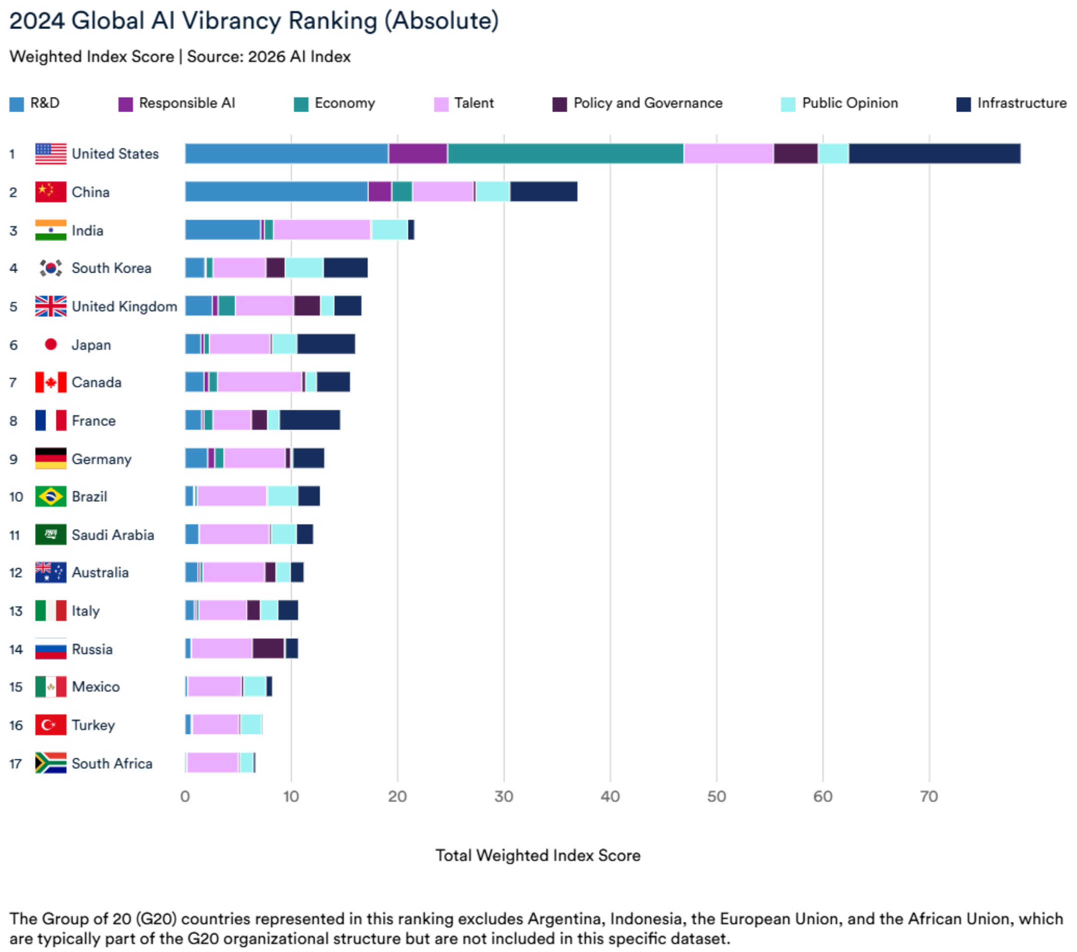

Figure 11: Global AI Vibrancy tool (Source: Stanford University)

According to 2022 data, the top 20% of AI researchers come from China (Fig. 12), while a significant majority of the whole group (42%) is employed in the U.S. followed by China with 28% as shown in Figure 13. This reflects the fact that China is suffering from "brain drain" as it produces the talent, and the U.S. utilizes it. Therefore, the United States has a clear advantage in AI research human capital having a more open working ecosystem.

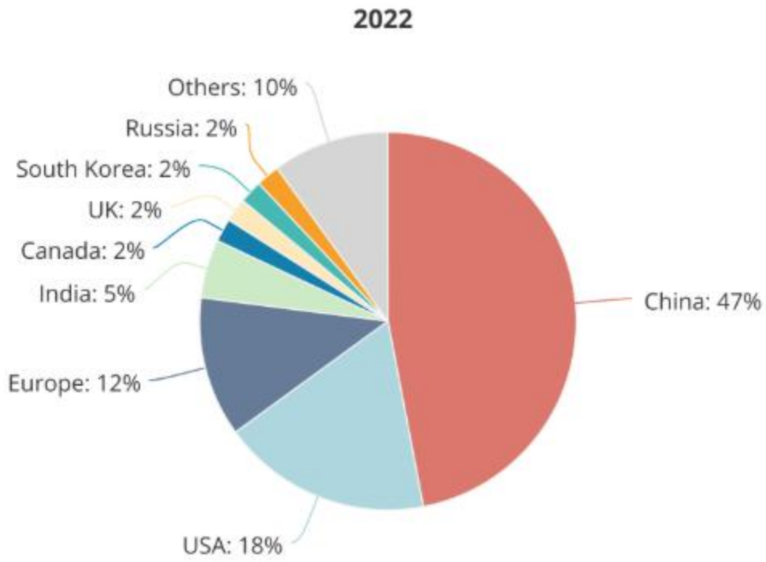

Figure 12: Countries of origin of top-tier AI researchers (top ~20%, based on undergraduate degrees), Source: https://archivemacropolo.org/ - Paulson Institute)

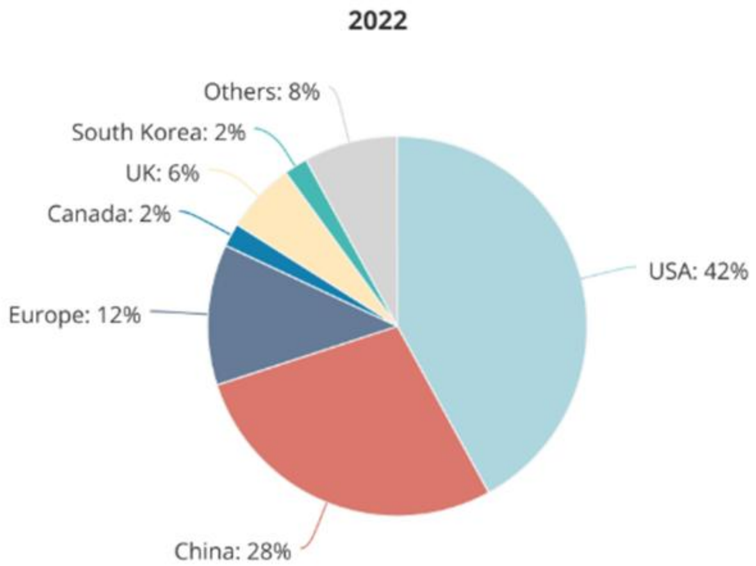

Figure 13: Leading countries where top-tier AI researchers (top ~20%) work), Source: https://archivemacropolo.org/ - Paulson Institute)

Infrastructural power coming from computing and data centers plays a vital role in identifying systemic balance and changes. Particularly, the infrastructure that trains and runs the AI models changes frequently; computing needs double every five months, data amounts every eight months, and electricity use double every single year (Maslej, et al., 2025). The U.S. maintains a significant advantage in computing power over their adversaries (Rosenbach, et al., 2025), as they possess far more supercomputers than the countries following in rank (table 2). Furthermore, the same supremacy is observed for hyperscale data centers that support AI model training, as seen in table 3.

	Countries	Count (Supercomputers)
1	United States	171
2	Japan	43
3	Germany	40
4	China	40
5	France	23
6	Canada	19
7	Italy	18
8	South Korea	15
9	Taiwan	10
10	Brazil	10

Table 2: Top 10 countries in supercomputer possession and power (adapted from top500.org

Country	Hyperscale DCs	% of Global Total
United States	642	54%
China	190	16%
Japan	71	6%
Germany	60	5%
United Kingdom	48	4%
Australia	36	3%
Canada	30	3%
Netherlands	24	2%
Singapore	21	2%
Ireland	18	2%
Other countries	49	3%
Global Total	1,189	100%

Table 3: Hyperscale Data Centers by Country (Top 10 as of November 2025), adapted from https://www.cargoson.com/en/blog/number-of-data-centers-by-country

Additionally, semiconductors are a strategic resource crucial for Artificial Intelligence, as they can enable “high-speed calculations, parallel processing, and energy efficiency” that are absolutely necessary for AI models operation (Bell, 2025). The U.S. and its allies, like Japan and Taiwan, maintain an oligopoly controlling critical chokepoints in the semiconductor value chain, potentially giving the West the upper hand (Rosenbach, et al., 2025). The

United States leads in crucial segments of the chain, such as chip design and tools, while China is dependent on foreign equipment staying behind in semiconductors and advanced AI.

Ultimately, while the U.S. remain leaders in innovation and investment, it is apparent that dominance cannot be assured through financial means. As the compute costs are getting lower, the open AI models are efficient, and China has an advantage in data and talent, the American supremacy is at stake. The balance of technological of power is gradually getting closer to a multipolar state, as any significant breakthrough can tip the balance. If the numbers are correct, the U.S. must depend on their allies to maintain their technological lead, at least in AI.

However, these metrics are insufficient, if the purpose is to understand all aspects of tech power; more specifically, it is necessary to examine also military spending in AI in order to reach a better understanding. Recent research supports this, as “adverse outcomes of AI technologies” are in the top five long term global risks for 2026 (World Economic Forum, 2026); Artificial Intelligence can indeed be disruptive creating a systemic failure across interconnected sectors. Furthermore, the balance of power can be disrupted through various uses, such as data poisoning, weaponized generative AI, lightning-fast AI operations, AI in nuclear weapons command and control, all resulting in a competitive AI arms race.

According to the Stockholm International Peace Research Institute (SIPRI), global military expenditure reached an all-time high of $2,718 billion in 2024, increased by 9.4%. The U.S. Department of Defense requested $143.2 billion for research, development, test and evaluation (RDT&E) for 2025, including $1.8 billion in artificial intelligence and investments to support “the fielding of uncrewed and autonomous systems that can operate in all domains” to enhance “deterrence in the Indo-Pacific” (U.S. Department of Defense, 2024), while China’s expenditure in the field is estimated to be on par (Simpson, et al., 2025).

1.6 Conclusion and synthesis

The metrics of military expenditure and technological capacity presented in the previous chapters validate the neoclassical realist assertion that the distribution of material power remains the primary driver of international politics. Furthermore, the current trajectory of China from a state of latent economic potential to a state that possesses advanced technological capabilities confirms that a shift is happening in the international system, which tends to abandon unipolarity. This transition is enhanced by uneven growth in technological progress, which undermines the established balance of power and creates the structural preconditions for hegemonic rivalry, as Gilpin would argue.

In essence, technology acts as a structural modifier or power multiplier that intensifies rather than suppresses the security dilemma. While liberals mention that interconnectivity raises the cost of conflict, there is a contradicting view that this interdependence is weaponized in order to support state interests and goals. Indeed, the centralization of digital infrastructure allows hegemonic powers to exploit asymmetries by utilizing “chokepoints” in semiconductor supply chains and financial systems. Consequently, the diffusion of technology becomes a security threat in an anarchic system compelling states to adopt techno-nationalist policies, which include strategic decoupling and containment.

Furthermore, the advent of Artificial Intelligence threatens to fundamentally alter the international system creating a dangerous strategic environment. By limiting the decision-making time and by enabling new mechanisms that produce insecurity, AI technologies favor offense. The difficulty in distinguishing between commercial and military AI innovations forces states to adopt worst-case assumptions about their adversaries’ intentions, which leads to a new arms race.

Ultimately, even though private corporations are currently the pioneers of innovation, they are forced to comply with the strategic interests of the state. This is more obvious in countries like China, where commercial technology is considered part of national defense through civil-military fusion strategies. Therefore, the technological competition observed in the current era is not merely a contest for economic growth and prosperity but a field of security struggle. As long as the technoeconomic gap narrows and relative gains are the target, technology will continue to play a critical role in power redistribution. What remains to be examined in the next chapters, is how specific technologies like Artificial Intelligence affect the international system and whether it leads it to instability and systemic changes.

2. Empirical application: AI and Big Data as instruments of strategic competition

2.1 Historical overview: Systemic disruption through technological development

The mechanism through which technology affects the international balance of power can be traced throughout human history. Technological breakthroughs, whether commercial or military, have always created conditions for systemic shocks that cause the redistribution of military and economic power among great powers. Examining historical examples from the trireme to the nuclear age, it seems that technology has consistently acted as a determining variable of hegemonic decline and the rise of new powers.

Consequently, to understand the strategic implications of Artificial Intelligence and Big Data in the current era, it is necessary to first analyze previous cases of technological upheaval. This part of the research analyzes how past disruptive technologies influenced the security dilemma and the nature of warfare. By examining certain historical examples, it is possible to pinpoint how states utilize innovation for survival, as well as the unique characteristics of the AI revolution as a potential determinant for instability.

2.1.1 From the trireme to nuclear weapons

There are many points in history that reveal the influential power of technology. Firstly, the advent and deployment of the trireme[4] by the ancient Athenians fundamentally affected the balance of power in the region, enabling Athens to rise as hegemon and threaten Spartan military superiority for a certain period. The trireme in this sense was not just a mere tool, but an enabler of the Athenian grand strategy based on its naval power (Platias & Koliopoulos, 2010, p. 105).

The trireme as a main unit of Athenian power supported continuous military dominance and wealth growth. Through its naval superiority, the city-state transformed the Delian League into an empire led by them while forcing their allies pay tribute (Platias & Koliopoulos, 2010, p. 26). Therefore, the trireme and the subsequent naval power played a critical role by producing spiraling gains which multiplied the Athenian growth compared to the other city-states.

In this context, the trireme allowed Athens to acquire control over the sea, which allowed power projection and strategic denial to its adversaries (Nash, 2018, pp. 122-123), while controlling its allies and neutralizing the land-based

---

[4] More information on the Athenian trireme and its technical specifications can be found in CASSON, L. (1971). Ships and Seamanship in the Ancient World. Princeton University Press. http://www.jstor.org/stable/j.ctt7zv2gz

superiority of Sparta for a time. Having enough fortifications around the city, Athens was metaphorically turned into an "island", making the infantry advantage of Sparta irrelevant. The mobility capacity of naval power allowed Athens to import essential resources, leading Spartan strategy to a "deadlock" (Platias & Koliopoulos, 2010, p. 39). Furthermore, this allowed Athens using commando tactics, raiding the coasts of Peloponnese avoiding a direct battle with the Spartan infantry (Nash, 2018, p. 134).

The balance of power eventually shifted when Sparta realized that hegemony can be conquered not only through land supremacy but also with the support of naval supremacy, which was made possible by allying with the Persians and turning their wealth into naval power (Platias & Koliopoulos, 2010, p. 72). It was the "Sparta's eventual transformation into a naval power" along with the Athenian inability to manage this change and its repercussions (Nash, 2018, p. 135) that led to the systemic change.

Another indicative example is the introduction of gunpowder into Europe, which has caused a fundamental transformation of political power contributing to the rise of the early modern state. This change which is recognized as a major Revolution in Military Affairs, allowed political entities such as Kingdoms, to adapt their military and administrative structure in order to survive.

The high costs of producing and maintaining artillery altered the domestic balance of power. As several historians have argued, the nobility did not possess enough wealth to gain access to this new technology, while the kings and queens of Europe had the necessary financial assets (DeVries, 1998, p. 128). Therefore, the monarch's authority over his dominion was reinforced, as military strength through gunpowder was drawn to the political center. This gave them the necessary power to crush rebellions, expand their influence, and increase taxing capacity. In fact, the French artillery train had a decisive role in the end of the Hundreds Year War and against rebelling nobility (DeVries, 1998, p. 133).

Initially, the gunpowder destabilized the European system, which later reached a new equilibrium. The invasion and rapid conquest over Italian city-states by the French in 1494 showcase the critical impact this technology had at that time (McNeill, 1982, p. 89). Ultimately, the necessity to defend against this new technology produced a way to defend against gunfire, as Italians thought of new ways of fortifications ("trace italienne") that could withstand the power of gunpowder along with outwork artillery. This development as well as the spread of gunpowder weaponry across Europe averted the hegemony of one power in the continent.

Finally, gunpowder technology affected the balance of power through its application in naval warfare. Particularly, the use of all-weather sailing ships along with the new type of firepower provided by canons allowed the distraction of enemies from a distance in the sea (McNeill, 1982, pp. 100-101), which altered the established Mediterranean way of fighting by ramming and boarding. These capabilities allowed European states to project their power across the rest of the world, as their newfound enemies were using obsolete naval warfare tactics.

Moreover, the railroad caused another RMA and systemic international change by shifting the distribution of power among great powers, and by expanding the strategic reach of the state. It augmented the "interaction capacity" of the international system by dramatically increasing the speed and volume of transportation (Herrera, 2006, p. 46), fueling also European colonialism. Indeed, railroad enabled the mobilization and deployment of mass armies that was previously impossible. While Napoleon moved approximately 500,000 soldiers in a fifteen-year period, the Prussians did the same but only in five months, and by 1914 Germany could rally three times this number in ten days (Herrera, 2006, p. 85). This development of course meant that the state was also capable of transferring at increased speed the corresponding logistical assets necessary for warfare in the industrial age.

It is evident that railroads in Europe had transformed the nature and application of military power by the late nineteenth century so much that the international system was reshaped entirely. At the same time Germany gained the most from this shift, while playing a leading role in the subsequent redistribution of power (Herrera, 2006, p. 87). In fact, the railroad was the key that enabled the process of German unification accomplished in 1871. They introduced a new method of concentrating forces by sending troops at the same time outside the main battlefield followed by the invasion into enemy territory (MacGregor & Williamson, 2001, p. 105). Railroad provided a solution to the "two-front problem", namely against French attacks from the West and Austian or Russian attacks in the East (Herrera, 2006, p. 9). Therefore, it can be argued that the railroad caused a major impact on the distribution of power by making the industrialization of war possible, increasing the costs and scale of conflict. And it did that not as autonomous power, but by being developed to serve certain political purposes.

Lastly, another instance of global upheaval by a disruptive technology was the advent of nuclear weapons. The introduction of nuclear weapons provoked yet another systemic transformation in international politics, as the 5th great RMA in the West by fundamentally changing the rules of war and diplomacy alike. Contrary to the railroad which favored offense, the nuclear revolution created a strategic environment where a victory may be synonymous to mutual annihilation between nuclear powers, as the "link between victory and self-preservation had been cut" (Gray, 2004, p. 207). As Kenneth Waltz put it simply but clearly, "In a nuclear world, one is uncertain about surviving or being annihilated" (Sagan & Waltz , 2002, p. 9).

Nuclear weapons reshaped international security in several major ways. They fundamentally changed how states could use military force by redefining the importance of distance, time, front lines, and mobilization. The Manhattan Project also transformed the relationship between states and society, expanding government involvement from industry into scientific research, which is often called as the “military industrial complex” or “the scientific state” (Herrera, 2006, p. 183). Additionally, this development enabled the redistribution of power by reinforcing the postwar dominance of the United States and the Soviet Union over traditional powers, such as the UK and Germany.

This systemic change brought forward deterrence by making the punishment for attacking first unacceptably high through retaliation strikes, regardless of the defender’s ability to repel an assault (Sagan & Waltz , 2002). This certainty of mutual destruction made great powers very cautious, as the possible costs of conflict became overwhelming. This created a paradox, where powerful military arsenals became operationally “unusable” for direct conquest, while great nuclear powers refrained from territorial competition channeling their efforts into increasing their scientific and technological capacity (Herrera, 2006, p. 190), as well as indirect confrontation, such as within economic competition.

Nonetheless, the stability created by nuclear military assets may be not so secure, as it relies on the assumption that states will behave rationally and the systems that control nuclear arsenal are working perfectly. Organizational theorists argue that professional military organizations must be checked by civilian authorities or else they may undermine the logic of deterrence because of biases leading to accidental or preemptive war (Sagan & Waltz , 2002, pp. 47-48). Clausewitz’s theory also support that technological development cannot change the nature of war which is characterized by a “paradoxical trinity of primordial violence, politics, and chance” (MacGregor & Williamson, 2001, p. 179). In this sense, this even more troubling if Artificial Intelligence and its biases were to be integrated into command-and-control systems, as it will be examined in the following chapters.

Ultimately, reality has shown until today that nuclear deterrence has defined the international system enforcing a long peace even after the fall of the Soviet Union. It remains to be seen whether states will continue to avoid direct conflict or emerging Revolutions in Military Affairs will once again alter the distribution of power on a global scale through pure military conflict.

2.1.2 The AI revolution

The current Revolution in Military Affairs is characterized by the integration of Artificial Intelligence (AI), autonomous systems, and advanced sensors into the state's toolkit. Michael Horowitz's view of the new shift is more inclusive, as he claims that these developments signify not just the arrival of a specific weapon, but of the "ultimate enabler", a general-purpose technology like electricity (Horowitz, 2018, pp. 41,54), which will affect both military and economic power, as well as societies. This is crucial for the current balance of power, as it means that AI will not merely be a weapon, but it will profoundly change the structure of the logistical, industrial, and organizational aspects of national power even before deploying it on the battlefield. Evidently, this shift does not correspond just to an RMA, but to a military revolution comparable to the nuclear age, as it threatens to fundamentally alter the state and its relationship to warfare (Morris, 2024).

Regarding warfare, these innovations are forcing a crucial reevaluation of the ways, the means, and the actors of war (Brose, 2019, p. 122). It will fundamentally alter the character of warfare by introducing competition at a cognitive and algorithmic level. Contrary to previous RMAs, the current change showcases a distinct paradox; while it favors operational efficiency, it challenges traditional mechanisms of strategic stability. In this context, even though there is a claim that Artificial Intelligence functions as a pendulum in the offense-defense balance, as it is not always clear if it favors offense or defense (Dong, 2025), it is likely a technology closer to offensive actions. Indeed, reality proves that swarms of intelligent drones favor the attacker by exploiting the first-mover advantage (Brose, 2019, p. 126). For example, by keeping air defenses occupied with low-cost autonomous drones, the attacker can overwhelm expensive and complex defensive systems built for high-value target interception. This dynamic resembles the destabilizing effect the railroad had rather than the stability created by nuclear weapons.

The nature of this technology appears indeed to shift strategic decision-making toward an offensive paradigm, which is contradictory to the stability offered by nuclear deterrence. This emerging paradigm suggests that the proliferation of numerous, low-cost and expendable autonomous systems will alter the future battlefield, rendering traditional and heavily manned systems unviable, while they will be capable of delivering violence at speeds and volume that exceed human capability (Brose, 2019, p. 124). As a result, it could be said that militaries will no longer be defined by the number of soldiers, but by the computational capacity and autonomous weapons a state can deploy. Clearly, this development could be beneficial for states that face a demographic decline, as the prospect of waging wars "without body bags" while keeping the lethality against the enemy can limit the political costs usually caused by human losses (Gill, 2019, p. 169). Naturally though, this substitution has its limits, as the Russo-Ukrainian war has shown, deploying AI systems to fight does not have the same political gravity as human soldiers on enemy territory (Morris, 2024).

Examining strategic implications of AI, it becomes apparent that the velocity of AI-enabled warfare introduces a significant imperative to strike first as these systems accelerate the “kill chain” (Brose, 2019, p. 123), limiting the chances of de-escalation. Particularly, by integrating AI into the OODA loop achieving speeds that surpass human cognitive capacity, decision-making cycles can be completed at machine speeds (Dong, 2025), especially in cyber and electronic warfare. In essence, the time necessary for diplomacy or de-escalation is in fact gone, which forces commanders to transfer authority to algorithms rather than risk delayed response that could prove to be decisive for victory. Modern conflict has already witnessed this algorithmic power; during the Israel-Hamas war, the IDF deployed an AI system known as “Habsora” which identifies targets at a superhuman rate leading to mass killings (Osimen, et al., 2024, p. 8). This phenomenon, which is termed “battlefield singularity” by the Chinese and “hyperwar” by the Americans, causes a security dilemma where states might lead themselves in a race to the bottom by deploying unsafe or incomplete AI systems to avoid falling behind (Horowitz & Scharre, 2021, pp. 5,8).

This dynamic can be understood as a prisoner’s dilemma in the context of Game Theory, given that a state will be at a disadvantage if it pauses AI development and its adversaries continue AI growth, therefore the only logical choice for major powers is to accelerate development despite the risks (Kuruc, 2024, pp. 51-52). One of these risks as Scharre explains is the danger of a “Flash War”; like in “Flash Crashes” seen in high-frequency stock trading, algorithms interacting in cyberspace could trigger an accidental escalation that could get out of human control before any chance to intervene (Scharre, 2018). This means that as algorithms are programmed to react to adversary actions in microseconds, they can cause an unintended continuous cycle of escalation that renders human intervention improbable. Another risk is the possibility of “cross-domain” warfare, as a false AI analysis could lead the system to propose a military attack to solve a cyber problem, turning a digital conflict into a physical one (Katagiri, 2024, p. 43).

A critical strategic concern is that while second-strike capabilities with nuclear weapons secure stability, AI-enabled sensors may soon be able to locate these weapons, increasing the possibility of a disarming first strike (Lin, 2025, p. 102). If this becomes a reality, it could mean that the principles of the “MAD” (Mutually Assured Destruction) strategic logic could be failing, as states could no longer secure that their retaliatory forces can survive a first strike by the enemy. This instability is even more apparent by the potential of AI to target Nuclear Command and Control Systems, providing them with false signals or fabricated data (Sharikov, 2018, p. 371). Particularly, fully autonomous systems are more resilient against communication disruption, which means that the defender cannot easily interfere with their trajectory and the attacker is not able to call off the attack, which can lead to escalation (Scharre, 2018). Evidently, these capabilities will depend also on the adoption capacity of military organizations, having the necessary culture and structure, that will enable effective use of this innovation, as well as on the suspected actions of their adversaries in this matter (Horowitz, 2018, p. 54).

Moreover, if human judgement is completely removed from this automated process, then the danger of escalation is significant (Scharre, 2018). Senior defense officials have called this dilemma the “Terminator Conundrum”; if humans are left out of the decision process autonomous weapons could prove to be more lethal, while AI-enhanced weapons that keep humans in the loop could make war more programmed and “civilized” (Scharre, 2018). Keeping humans in the loop, however, may not be enough if decision-makers lack information or time to challenge the AI system, which is why it is important to keep “meaningful human control” over this, so the outcome can be based on human judgement (Lin, 2025, p. 103).

Nevertheless, this dilemma gets even more complicated when examined through a psychological viewpoint. Maintaining human control may prove to be difficult due to “Automation bias”. Humans tend to trust computer decisions too much, which means that users of AI systems may approve whatever the system suggests, without really checking it (Erskine, et al., 2025, pp. 21-22). Particularly, the cognitive pressure in high-stress combat environments is so intense that commanders are psychologically inclined to minimize their oversight in favor of the hypothetically superior machine capabilities. This psychological vulnerability is intensified by the “illusion of control”, as the speed and analytical power of AI creates a false impression for commanders that they can control every aspect of war, leading to the “AI Commander Problem” as James Johnson called it, where AI systems become essential actors at a strategic level (Johnson, 2022, pp. 247, 251). Not to mention that flaws or biases in the system itself could drive states into disagreement and escalation no matter their initial intention (Katagiri, 2024, p. 42).

In addition, regarding the systemic distribution of power, AI technology is far more easily accessible than nuclear technology. The nuclear non-proliferation framework is based on scarcity and excludability of the necessary materials, while computational resources, despite the efforts for controlling semiconductor supply chains, are more accessible (Horowitz & Kahn, 2025). However, as computational power becomes a currency of state power, the balance of power is changing, creating states with high and low computational power (Kuruc, 2024, p. 50). This inequality extends beyond military capabilities to the economy. As Kenneth Payne argues AI threatens to render the “comparative advantage” obsolete as states may achieve self-sufficiency through automation, eroding interdependence and worsening the position of developing nations (Payne, 2024). Furthermore, while AI is a dual-use technology, the limits between civilian and military use are obscured, as the same system that helps create a useful new drug could also at the same time produce the formula for a new biological weapon (Klyman & Piliero, 2024).

	The Nuclear Age (Traditional Deterrence)	The AI Age (The New "Military Revolution")
Strategic level	**Mutually Assured Destruction (MAD)**: Stability is maintained because retaliation is guaranteed.	**First-mover advantage**: Stability is eroded because striking first offers a decisive advantage
Conflict level	**Human speed**: Decisions are made in minutes or hours, allowing for de-escalation.	**Machine speed** ("Hyperwar"): Decisions occur in microseconds, creating the risk of "Flash Wars"
Offense/Defense	**Defense/Deterrence dominant**: High cost of use discourages aggression.	**Offense dominant**: Swarms of low-cost, expendable drones favor the attacker
Accessibility	**Exclusive**: High barrier to entry (uranium scarcity, complex engineering).	**"Democratized"**: Low barrier to entry; dual-use technology accessible to smaller states and non-state actors
Control	**Centralized**: Strict human command and control hierarchies.	**Delegated**: Pressure to delegate lethal authority to algorithms to keep up with the enemy ("Terminator Conundrum").
Visibility	**Tangible**: Warheads and silos can be counted and verified (Arms Control possible)	**Intangible**: Algorithms are invisible and easily hidden or copied (Arms Control challenging)

Table 4: Comparison of characteristics of the Nuclear Age vs. the AI Age (source: Author's compilation based on the experts' arguments in this section)

Hybrid warfare is also affected by this new military revolution, as Artificial Intelligence alters the psychological and informational dimensions of conflict. AI gives its users the capability to weaponize information in a disruptive way utilizing deepfakes and digital propaganda, manipulating public perception and causing political instability without using physical force. As technology advances, more sophisticated algorithms could indeed create a realistic video of an enemy's leader announcing a false event or statement that could diminish their morale even before the start of the battle (Yan, 2020, pp. 11-12). Clearly, this brings the battlefield into civilian minds, as information is weaponized to achieve military goals.

Consequently, AI characteristics render traditional arms control challenging. Unlike conventional weaponry, algorithmic power is intangible and easily hidden; this hinders any effort to achieve international agreements that limit AI militarization (Lin, 2025, p. 105). Moreover, traditional deterrence strategies are probably useless; while testing a nuclear bomb proves its power, demonstrating a cyber weapon renders it obsolete as the adversaries could find a way to defend against it (Sharikov, 2018, p. 371). At the same time the democratization of this innovation means that the underlying technology necessary for creating lethal autonomous weapons could be exploited not only by states, but also by non-state actors, such as terrorists (Scharre, 2018).

In summary, the merging of these factors creates a structural crisis for international security that is distinct from previous military revolutions. While the nuclear age was defined by a terrifying but steady balance based on “MAD”, the AI age is defined by speed, opacity, and the incentive to make the first move. This aspect along with the compression of decision-making time potentially forces states to be constantly on alert, as the fear of falling behind in the technological sector could be stronger than the fear of accidental escalation. As a result, the international system may be losing its stability, as algorithms take a leading role in decision-making cycles.

Ultimately, the AI revolution remains an unpredictable factor that threatens to erode the strategic stability of the international system. If warfare stops being a political instrument of human interests because of algorithmic capabilities, the nature of war, as described by Clausewitz, may be altered profoundly, no longer serving as a continuation of politics. This emerging dynamic reveals that not only the potential of machine failure, but also the fact that they may work perfectly, can lead to increased conflicts that states or political leaders did not specifically choose.

2.2 Defining the new technological landscape: AI and Big Data

Having discussed major or significant technological disruptions, it becomes evident that the international system is currently witnessing a profound transformation. Unlike the previous military revolutions, the current era is defined by the rise of the “digital world” as a primary arena of competition for the modern state. This shift is characterized by two technological forces that are deeply linked together, namely Artificial Intelligence and Big Data.

These technologies are not just tools, but an ecosystem of cybertechnologies that reshape the nature of national power. As states transition to an AI-enhanced information age, the ability to collect, process and weaponize vast amounts of information becomes a crucial determinant for hegemony.

Therefore, it is necessary to define these technologies in order to better understand the geopolitical dynamics of the current century.

2.2.1 Fundamental dimensions of Artificial Intelligence

The current architecture of Artificial Intelligence consists of a group of technologies rather than a single technological tool. In this sense, AI is defined as “the science of engineering machines to simulate human intelligence processes, specifically learning, reasoning, and self-correction” (Lele, 2019, p. 140). It functions as an umbrella term that includes various and different subfields, such as robotics and machine automation. The ultimate goal of this innovation is not just to enhance computational capacity, but to comprehend “intelligent processes” regardless of their physical implementation and then simulate them in the human world (Lele, 2019, p. 143).

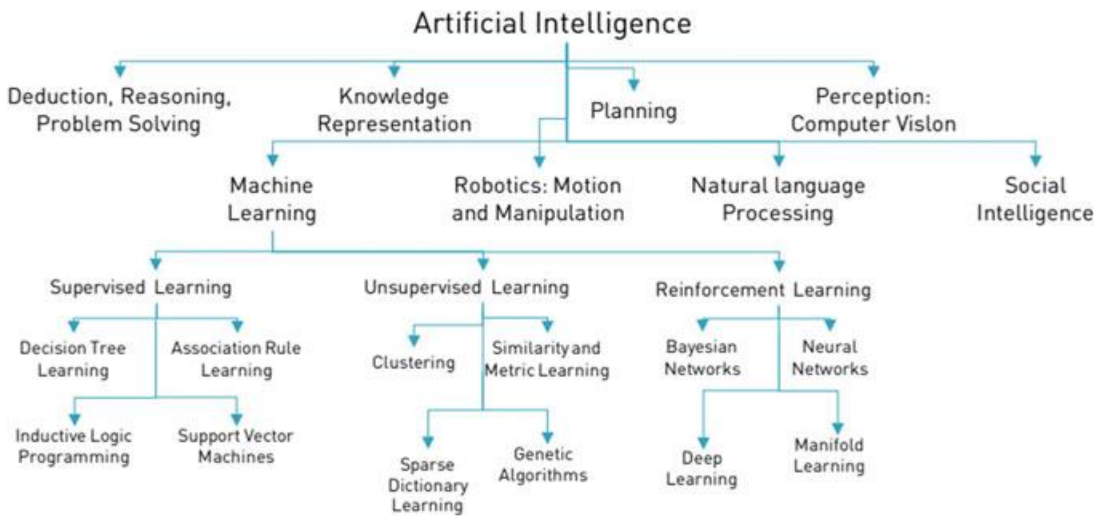

Figure 14: Artificial Intelligence and its subfields as of 2019 (Source: Lele, 2019, p.141)

One of the main sub-fields of AI is machine learning (ML), which contains critical methodological elements. Machine Learning relies on statistical and mathematical models that allow computer systems to learn and improve by processing data and by analyzing previous errors, rather than relying on static programming rules. In this context, machine learning can be understood as a program that often utilizes architectures such as “neural networks”, designed to train computers to locate answers in large datasets (Lele, 2019, p. 143).

Furthermore, Deep Learning is a specific methodology within the machine learning subdomain. This category includes the use of multi-layered AI neural networks to learn complex patterns from large amounts of data (Lele, 2019, p. 143). Consequently, the development of deep learning is dependent on the availability of massive datasets and high-performance computing power. It is apparent that AI is the broad field that studies how to make machines intelligent, while machine learning is a part of AI that focuses on algorithms that learn from data, and deep learning is a more advanced type of ML that uses multi-layered neural networks based on advanced computer systems. However, these systems can be fragile, in the sense that they may function exceptionally well in a controlled environment, but critically fail when come up against new environments or data that was not provided during trainings, such as is the case of self-driving cars (Horowitz & Scharre, 2021, p. 7).

Additionally, AI systems can be classified also based on capability and scope into two main categories, Artificial Narrow Intelligence (ANI) and Artificial General Intelligence (AGI). The current international system is dominated by ANI technologies, which are often characterized as “weak AI” (Lele, 2019, p. 142). This category includes systems that are designed for specific tasks executed in an efficient way, such as image recognition. Despite their advanced algorithmic capabilities, they function within specific limits and lack the necessary cognitive skill to operate outside their predefined parameters. Unlike human intelligence, ANI systems cannot adapt to broad or unclear political imperatives (Horowitz & Scharre, 2021, p. 8). Consequently, ANI is the only type of AI implemented so far in the current era, in both military and civilian sectors.

On the other hand, Artificial General Intelligence (AGI) or “strong AI”, represents AI systems that most experts argue have not yet been created. An AGI system is one with human-level intelligence, capable of understanding and reasoning about its environment similar to human cognition (Lele, 2019, p. 142). Unlike an ANI system, it can manage multiple unrelated thoughts, understand environmental stimuli, and adapt to new situations like a human without previous training. Some theorists go even further by introducing a third category, Artificial Super Intelligence (ASI), which theoretically surpasses human capabilities in every aspect. Therefore, it can be said that the current strategic competition and military applications are based on the capabilities and the limitations of narrow AI, while general AI is not yet tangible technology.

Additionally, a newer technological development known as Generative AI has emerged. This type of AI does not just focus on classifying data, but it is capable of simulating reasoning capabilities and responding to human questions, without reaching yet the level of Artificial General Intelligence. Particularly, these systems can generate new content, such as images or text, rather than just analyzing existing information (Brandt, et al., 2023).

This capability can be weaponized, as Generative AI can create “deepfakes” to manipulate according to the user’s political goals. The risk is not only that people could believe false information, but also that the use of these tools could have impact on the legitimacy of democratic governments. If societies cannot distinguish between real and fabricated stories, it becomes difficult to maintain their trust in political institutions (Brandt, et al., 2023).

2.2.2 Big Data as a strategic source

This section examines the nature and the role of Big Data in the current military revolution, as well as its connection with Artificial Intelligence. Particularly, Big Data can be defined as “the information assets characterized by such a high volume, velocity and variety that they necessitate specific technology and analytical methods to be transformed into value” (Puyvelde, et al., 2017, p. 1399). In other words, the main characteristics that define the nature of Big Data are the “three Vs”, namely Volume, Velocity, and Variety.

“Volume” refers to the amount of data produced, which continues to grow without stopping from terabytes to zettabytes (Lele, 2019, p. 156). This happens as datasets are so large they exceed the storage and processing capacities of traditional databases. Organizations now collect this information from diverse sources, including business transactions, social media, and sensor data.

“Velocity” refers to the unprecedented speed at which data is created, stored, and disseminated (Pencheva, et al., 2018). This characteristic implies that systems deal with data streams in near real-time, as information is generated continuously by sources such as social media platforms, mobile applications, and sensors. (Kulshrestha, 2016). The challenge of velocity involves not only the bandwidth required for uploading and downloading but also the information technology architecture needed to process data as it arrives (Zwitter, 2015).

Furthermore, “Variety” describes the diverse range of formats in which data exists. While traditional databases relied on structured, numeric data, modern Big Data integrates unstructured formats such as text documents, emails, video, audio, and geospatial data (Puyvelde, et al., 2017, p. 1402). In this context, unstructured data constitutes the fastest-growing category of information, requiring advanced technologies to store and organize in an effective way. Lastly, some definitions add one more characteristic, namely "Veracity," which concerns the reliability and biases within the data, though the core definition is based on the initial three dimensions.

This growth of data is an inseparable part of Artificial Intelligence technologies, including machine learning and natural language processing. The effectiveness and expansion of AI systems are dependent on the data accessibility to facilitate the computer learning process (Pencheva, et al., 2018). Neural networks try to mimic the human brain using many connected nodes that are simple on their own but together can learn from these data to solve complex problems (Lele, 2019, p. 143).

Consequently, Big Data provides the necessary training material for these systems. Without this massive data input the algorithms cannot acquire the rules and logic required for task automation or complex functions such as autonomous driving.

As data are proven to be a highly valuable and prized asset, it has been claimed many times that it constitutes the new oil in the digital era. From an economic perspective this analogy is inaccurate though, as oil is a scarce commodity while it becomes increasingly difficult to obtain it from new and undiscovered territories (Schlosser , 2018). Conversely, Big Data is characterized by abundance and the ease of production, which has led to an increasing rate of data growth by various sources. In other words, oil is a commodity that can be depleted entirely, while data has an infinite source.

Another difference lies in the fact that data is not a rivalrous asset like the single use of fossil fuels, as oil once consumed cannot be reused. On the other hand, data can be reused, shared and processed at the same time by multiple actors regardless of their purpose and without limiting their quantity or their quality (Schlosser , 2018). Moreover, increasing oil reserves augments the value of the stored product, but in the case of data, value is created through its processing and the resulting insights rather than their volume, which can prove to be a vulnerability under certain circumstances, such as unauthorized access.

These fundamental economic differences have significant implications for states from a liberal point of view. When they treat data as oil, they resort to data protectionism thinking that data is a scarce and exclusive product (Schlosser , 2018). By restricting data flows across the globe, the economic and social benefits of data utilization are limited. It is not the same logic as in oil industry, where controlling supply increases value, but inversely value is increased through connectivity.

Naturally, this might not be the case when examining Big Data from a military or a realist perspective. In fact, states treat information as a strategic resource for national security and technological superiority. By restricting data transmission states try to limit the vulnerabilities caused by cyber espionage and foreign surveillance (Lele, 2019, p. 160). In general, this strategic approach is one of the reasons that there is a divide between “data-rich” and “data-poor” states causing inequality in the international system (Pencheva, et al., 2018), creating strategic advantage for the former states. This is apparent in African-Western or African-Chinese technological relations, as African states have to deal with unequal access to data knowledge as they rely on foreign states and corporations for their critical data storage and processing (Calzati, 2022). Therefore, without the domestic capacity to control the whole data lifecycle, normative power will not be sufficient in limiting instances of “data colonialism” that threaten “data sovereignty”.

2.3 AI and Big Data in military strategy: applications and the transformation of warfare

2.3.1 Autonomous systems and warfare

The advent of Autonomous Weapon Systems (AWS), often called Lethal Autonomous Weapons Systems (LAWS), in battlefields showcase a fundamental shift in military technology, as the main functions of combat such as selecting and engaging a target, are delegated to machines. In this context, autonomy is the capacity of a system to "execute a task, or tasks, without human input, using interactions of computer programming with the environment" (Boulanin & Verbruggen, 2017, p. 5). These systems are based on three main capabilities: the ability to sense the environment, the computational capacity for decision making relying on processed data, and the technical means to execute this decision, passing all these stages without "intervention by a human operator" (Altmann & Sauer, 2017, p. 117).

A critical characteristic that defines the degree of autonomy of an AI system is indeed human involvement. In this context, there are three main types: the "semi-autonomous or human-in-the-loop" where human intervention is needed at some point, "human-supervised autonomous or human-on-the-loop" where the human role is mostly supervision and involvement only if it is necessary, and "fully autonomous or human-out-of-the-loop" where the system operation is characterized by the complete absence of human intervention (Boulanin & Verbruggen, 2017, pp. 5-6). This distinction is significant for military operations, as fully autonomous systems can be deployed in environments where communication is obstructed and human control is impossible, and in case a battle takes place in extreme speeds that exceed human reaction capability (Altmann & Sauer, 2017, p. 124).

Semi-autonomous military systems are actively being used in the modern battlefield, especially drones. For instance, systems like the US Switchblade 300 and 600 have been utilized by Ukrainian forces against Russia, where navigation and target recognition was executed by them and commands were given by human operators (Lee, 2025). Conversely, autonomous AI systems are increasingly put in action since 2020, when according to a UN report, an autonomous Turkish-made drone targeted and attacked a human without explicit order during the Libyan civil war (Froelich, 2021). Similarly, India utilized a fully autonomous loitering munition (SkyStriker) against terrorists in Pakistan and Kashmir (Manish & Dyarakoti, 2025, p. 13). Furthermore, these automatic capabilities have been delegated to defensive systems that defend against high-speed incoming projectiles where human reaction time is insufficient (Altmann & Sauer, 2017, p. 118). These developments signify a strategic shift, as states started introducing these kinds of weapons in their armies and in battlefields seeking machine-speed resolution, which could potentially lead to instability in the international system.

The integration of Unmanned Aerial Vehicles (UAVs), Unmanned Surface Vessels (USVs), loitering munitions, and other types of militarized autonomous systems into modern militaries reveals a fundamental transformation of warfare by connecting lethal force with machines rather than humans. These systems allow states to increase military efficiency and surveillance while limiting human casualties (Altmann & Sauer, 2017, p. 130; Manish & Dyarakoti, 2025, p. 2). Additionally, they operate with greater accuracy and agility, they do not suffer from physical or psychological attrition like humans, which gives the opportunity for operations that would be improbable before, and finally they lower overall manpower costs (Boulanin & Verbruggen, 2017, pp. 61-63). Furthermore, there are loitering munitions or "suicide drones" which refer to a hybrid of cruise missiles and Unmanned Combat Aerial Vehicles (UCAVs) which can remain in the air for an extended period of time over their target area, and be used either for surveillance[5] or to hit the target (Boulanin & Verbruggen, 2017, p. 50).

Another characteristic of this strategic shift is that quantity is once again a priority as inexpensive and disposable unmanned autonomous systems are appearing on the modern battlefield. The traditional defense strategy often follows "Augustine's Law", which says that the higher the cost of advanced military technology gets, the produced quantity decreases as states cannot keep up with the cost (Boulanin & Verbruggen, 2017, p. 79). Swarm technology disrupts this logic, as they introduce vast numbers of low-cost disposable systems that operate cohesively and are designed to be lost in combat (Boulanin & Verbruggen, 2017, p. 63).

Swarms can be advantageous as they can create a saturation attack by overwhelming the defense systems of the adversary with their numbers (Chin, 2026). This way the attacker forces the defender to increase defense expenses, compelling them to acquire expensive missiles to destroy cheap drones. Furthermore, while high-value manned aircraft create bigger impact both financially and morally when destroyed, swarms are much more resilient as they are based on distributed power and intelligence. As the mission objectives and decision-making process are shared across their network, the destruction of individual drones does not cause the entire swarm system to fail (Altmann & Sauer, 2017, p. 130).

Countries have been actively developing such systems with swarm capabilities. The United States for example have presented this kind of technology with the "Perdix" project, where 103 micro-drones were released from two fighter jets. These drones have collective decision-making, while they have adaptive movement and auto-repair capabilities (Altmann & Sauer, 2017, p. 123). China has also developed such technologies, reaching the U.S. technological prowess. The Chinese "Swarm 1" system demonstrates such a

[5] A loitering munition that has been deployed in the battlefield is "Harop" which was developed by the Israelis and used by Indian forces against Pakistan, as well as the Nagorno-Karabakh conflict in 2020 (Manish & Dyarakoti, 2025).

capability, as it can launch 48 drones simultaneously which can reach up to 200 drones using multiple launchers for various mission types (Chin, 2026). What is even more innovative is that they are also training drone algorithms based on animal behavior, such as dove maneuverability for attacking drones and hawk hunting moves for defensive drones.

2.3.2 AI and Big Data disruption in intelligence and logistics

Intelligence is also a sector that has been altered fundamentally, as UAVs, satellite images, and Artificial Intelligence have enabled ubiquitous surveillance in the modern military environment, where the volume of collected data surpasses human analytical capacity. To manage this situation, initiatives such as the US project “Maven” have been developed to analyze videos from UAVs utilizing deep learning and neural networks (Allen, 2017). This capability saves a lot of time, as analysts would normally spend a whole day just to utilize a small piece of the drone data.

Additionally, the resilience of AI systems has enabled a new dynamic of “persistent surveillance”. States can indeed deploy drones that can remain in the air for many hours while monitoring at great distances, far exceeding human endurance. This dynamic can create conditions for a” transparent” battlefield, where at least large military targets or other significant assets will not be able to conceal themselves from these digital spies.

Nevertheless, this transparency cannot eliminate the possibility of surprise attacks or the concept of the “fog of war” in general. While AI-enabled C4ISR[6] systems augment surveilling capabilities and situational awareness, they do not completely remove uncertainty (Yan, 2020, p. 9). Many times it depends on the characteristics of the environment, as well as target movement; for example, while objects in the air or on the sea are easily detected, stationary targets in concealed environments are much more difficult to be identified through computational means (Scharre, 2018). Additionally, adversaries can utilize various methods and means to counter these surveilling capabilities, by deploying decoys, electronic deception, and camouflage to manipulate the sensors and take advantage of the algorithmic rules’ inflexibility.

Another significant development is that AI has enabled anticipatory strategies through predictive analytics, as algorithms have the capacity to process immense amounts of datasets and pinpoint certain patterns that are not easily visible by human analysts. This capability gives states the potential to gain important intelligence advantage by predicting the actions of their adversaries, as well as internal failures before they happen.

---

[6] Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

Machine Learning can recognize patterns in ISR[7] data that humans could not possibly achieve, generating insights and predictions regarding potential security threats (Erskine, et al., 2025, p. 2). For instance, former U.S. Deputy Secretary of Defense Ash Carter claimed that these kinds of systems have the capability to identify the patterns of hybrid warfare, providing advance warning regarding gray zone conflicts and enabling actions within increasingly limited time (Yan, 2020, p. 8). Similarly, in the private sector there are firms that exploit metadata to produce predictions regarding security and geopolitical developments up to ten days in advance. Moreover, advanced Big Data analytics have been utilized to process Global System for Mobile (GSM) metadata of millions of users, for example in Pakistan, to locate specific persons, such as Osama Bin Laden (Boulanin & Verbruggen, 2017, p. 29). Similar is the effect of AI and Big Data on the OODA loop as it has already been discussed.

Anticipatory AI capabilities are not only useful in the battlefield, but also in logistics. Particularly, such systems can have the capacity to detect and diagnose faults before they become catastrophic for them (Boulanin & Verbruggen, 2017, p. 35). By monitoring their own status, these systems can predict issues and intervene, when possible, which could limit logistical problems and subsequently military operations delays.

Critically, military software will witness a further disruption with the introduction of “Agentic AI”, which refers to autonomous systems that execute complex tasks independently to achieve high-level objectives (Farnell & Coffey, 2024). According to Farnell and Coffey, the integration of AI Agents within the Joint Operational Planning Process[8] (JOPP), will enable the combined utilization of high volumes of traditional and non-traditional data to generate Courses of Action (COA) and rapidly transmit orders in the chain of commands. For instance, Agentic AI could effectively facilitate target prioritization, based on real-time battlefield conditions and even conduct “Red Teaming” simulations[9] to anticipate adversary countermoves.

Nonetheless, algorithmic prediction can prove to be risky, as machine learning processes predict the future based on the data they were trained which naturally belong to the past (Erskine, et al., 2025, p. 22). This can create vulnerabilities in case of new or unprecedented conditions, especially when state resistance to change is considered. Therefore, while AI has the potential

[7] Intelligence, Surveillance, and Reconnaissance

[8] The Joint Operation Planning Process (JOPP) is an orderly, analytical seven-step framework used by the U.S. military to develop actionable plans and orders for complex operations. It aligns missions with national strategic goals, allowing commanders to analyze missions, develop and compare courses of action (COA), and create effective plans.

[9] “Red teaming is a cybersecurity assessment method in which authorized specialists simulate a controlled, non-destructive cyberattack. This simulated intrusion enables an organization to uncover system weaknesses and implement targeted enhancements to its security practices.” (Source: IBM)

to predict adversarial movements and logistical hazards, bureaucratic inflexibility along with the algorithmic dependency on historical data complicates the integration of these systems in state decision-making.

2.3.3 Decision-making, Deterrence and the "Algorithmic fog of war"

Having studied the hardware and software dimensions of the AI revolution, it is important to understand how these technologies affect strategic decision-making and command. Particularly, being heavily reliant on algorithms creates a new type of Clausewitz's fog of war, namely an algorithmic fog. In this context, this section examines how the need for speed changes the way commanders perceive the battlefield, while it analyzes how the vulnerability of AI systems to manipulation and cognitive warfare challenges the stability coming from deterrence in the international system.

Regarding speed, the implementation of Joint All-Domain Command and Control (JADC2)[10] has fundamentally altered the OODA loop by compressing its stages into three, namely "sense, make sense, and act" (Huelss, 2025, p. 193). This new framework gives priority to machine learning algorithms over human cognition for decision-making cycles to be completed faster than the enemies' ones. As human observation becomes less important because of the AI sensing capabilities, Huelss observes that there is a phenomenon of "de-visualization", as non-visual AI-processed data is valued more than direct visual evidence (Huelss, 2025).

This change paradoxically creates a new type of fog of war, namely an algorithmic one (Huelss, 2025, p. 209). As operators rely more on insights and predictions made by machines, rather than on raw data from sensors, they must trust and be dependent on the presumed machine objectivity, becoming metaphorically blind. Ultimately, human control is maybe diminished and unimpactful, as the speed and complexity of automated information processing surpasses the operator's cognitive capacity by depriving him of the opportunity of critical evaluation before using (lethal) force.

Furthermore, the risks caused by this development are apparent, as AI systems have inherent vulnerabilities. Data corruption, through the process of model poisoning", is strategic method of manipulating these systems. Particularly, by getting access to the training data or the analytical framework of the algorithm, adversaries can infuse the system with hidden triggers or false data which will be considered valid by it. This corruption can force the AI to overlook certain threats or classify hostiles as friends, which of course could

[10] A strategic initiative by the United States Department of Defense designed to integrate sensors and platforms across all operational domains into a unified network, utilizing artificial intelligence to compress the traditional decision-making cycle into a streamlined process of "sensing," "making sense," and "acting" to secure a decisive information advantage at the speed of relevance

prove to be a catastrophic disruption for the defender (Benson & Goldstein, 2026). Additionally, as this “poisoning” is rather difficult to detect as the system seems to work effectively, it keeps deceiving the defender even in critical times of engagement. At the same time, adversarial attacks can trick computer vision during image analysis, as small digital changes or changes in the physical world, like image noise and simple stickers can cause AI to misidentify a target (Huelss, 2025, p. 204).

The integration of AI introduces also a new risk for traditional deterrence, which depends on a state’s ability to showcase both its capability and its willingness to impose costs. Although it could enhance and speed up this process, its vulnerability to manipulation helps create a cognitive fog of war which turns these benefits into a trap. Benson and Goldstein propose a concrete hypothetical scenario, where the Chinese before a blockade on Taiwan have already “poisoned” American decision-making systems in order to discourage them from sending forces, which in case it succeeds will cause further escalation and an AI-fueled disinformation campaign by China to maximize its strategic gains (Benson & Goldstein, 2026).

Finally, these developments unveil a cognitive war enhanced by AI capabilities, which allows them to target public sentiment and decision-makers’ perception. Utilizing generative AI, adversaries can use synthetic personas and deepfakes at massive scale to manipulate the political narrative eroding public trust (Yan, 2020, p. 11). In this context, a Chinese firm named “GoLaxy” has already utilized generative AI to create detailed psychological profiles and deploy synthetic personas to manipulate public opinion both in Taiwan and Hong Kong (Benson & Goldstein, 2026).

2.4 The Russo-Ukrainian conflict: strategic and operational implications by AI systems

The Russo-Ukrainian war represents a “watershed moment” in the history of warfare as the first conflict, where two adversaries significantly exploited artificial intelligence technologies for military operations (Goncharuk, 2024). This particular conflict is not a conventional conflict where the participants use the available military assets, but it insists on “innovation power” becoming a “contest of innovation”, where the capacity to create, adopt and utilize new technologies determines both military strength and soft power (Aviv & Ferri, 2023, p. 13). Furthermore, these developments have highlighted the role of private technological companies as a multiplier of state power, especially through the proliferation of autonomous systems.

Major American corporations, such as Microsoft and Google, have supported the war in favor of Ukraine, supporting its digital domain against Russia by enhancing its infrastructure (Aviv & Ferri, 2023). Evidently, these companies fortified Ukraine's digital sovereignty and cybersecurity by assisting in the rapid migration of critical governmental data in data centers outside of the country in order protect digital sovereignty and defend against cyber-espionage. Consequently, Ukraine's defense strategy has become dependent on the technological capabilities of its allies and their private sectors in the West.

Accordingly, AI is utilized to accelerate Ukraine's OODA cycles, analyzing massive data from satellites, drones, social media posts, and other reports to create a real-time flow of information for the war operations. Palantir's AI tech has played a crucial role in these endeavors, as it enabled unprecedented precise and rapid targeting in the battlefields (Bendett, 2023). Therefore, Ukraine with the help of its western allies managed to defend against adversarial attacks, which included cyberattacks with destructive malware such as WhisperGate, and physical attacks on its dual-use and governmental infrastructure (Aviv & Ferri, 2023).

More importantly, the necessities the conflict created have led to a continuously augmented AI arms race. Both the United States, as Ukrainian allies, and Russia are greatly investing in AI to increase their capabilities in surveillance, targeting, and autonomous systems augmenting the security dilemma among great powers (Akhtar, 2025, p. 516). In this context, AI is utilized in information warfare, for both disinformation campaigns and its detection. Particularly, Russians have used a AI tool called "Meliorator" which fabricated social media posts as well as bots for fake accounts, while Ukraine leverages American AI tech to counterbalance these fakes news, document war crimes and support in general its war efforts (Akhtar, 2025). As a result, AI can assist in cognitive warfare by influencing morale and public opinion.

Operationally, the use of unmanned vehicles has been decisive for the course of this war. Apart from aerial drones, Ukraine has deployed domestic-developed USVs (Unmanned Surface Vessels), such as the "Sea Baby" and the autonomous "Magura V-type", enabling significant disruption in the Black Sea theater (Mazzucco, 2025). Using swarm tactics Ukraine has achieved a form of denial in the sea against a far superior naval force. These unmanned vehicles have evolved from "kamikaze" type weapons into multi-role AI platforms capable of combat, surveillance, and search and rescue assets, forcing the Russian Navy to retreat into the safety of harbors. Naturally, Russia adapted its defense strategy in the area to protect its military assets by utilizing interceptor UAVs and electronic warfare to disrupt the guidance systems of Ukraine's naval drones. Consequently, the utilization of AI systems shows that the cheaper AI-enabled technology has the potential to counterbalance the advantages of massive and expensive military assets like battleships, being in essence a pure force multiplier at least at the operational level.

As a consequence, the Russo-Ukrainian conflict has introduced a new era for international security, as the future of warfare seems to be characterized by the advent of autonomous systems, cognitive and electronic warfare, logistic implications and the evolution of aerial conflict strategy (Slusher, 2025, p. 2). Particularly, a significant shift is that advanced military capabilities are being democratized through dual-use technologies, disrupting for example the monopoly on aerial power held by wealthy nations possessing expensive air fighters through the proliferation of affordable autonomous systems. Similarly, in the economic spectrum of warfare there is a significant asymmetry, as almost 2/3 of Russian tank losses were attributed to the less expensive Ukrainian drones (Slusher, 2025, p. 3), which could lead to a reevaluation of how military economics should be considered.

Additionally, the integration of Artificial Intelligence has made it more difficult to separate military and commercial technologies, which has led to strong interdependencies between states and the private sector. This development shows that the capacity to rapidly adapt commercial technologies for warfare is critical for future military endeavors (Bendett, 2023).

At the operational level, the integration of AI reveals a “tug of war” between machine speed decision-making and the strategic requirement to maintain human control over autonomous technologies (Mamediieva, 2025). Nonetheless, as communication between operators and military assets, such as UAVs, is being disrupted through electromagnetic means, a necessity for autonomous systems that can reach their target without guidance increases (Slusher, 2025). Eventually, these technological leaps create the right conditions for an arms race, that for some is like the nuclear race (Abdurasulov, 2025).

Ultimately, traditional military doctrines and the logistics of warfare are in need of rejuvenation based on lessons learned from this war, as institutions have to continuously adapt and humans begin to “cooperate” with machines (Slusher, 2025). The future security environment will be likely determined by merging advanced and basic capabilities, and success will depend on how effective strategic human oversight will be with lethal and non-lethal autonomous systems. In the end, the nature of war remains the same, but the means and actors are being radically altered, as new digital non-state actors are entering battlefields and other domains.

Level of war	Strategic Dimension (based on findings)	Traditional paradigm	AI-enabled paradigm (based on findings)
STRATEGIC	Center of Gravity	Mass & physical platforms (Tanks, Capital Ships).	Innovation power: Civil-Military fusion & rapid software adaptation.
	Economics of War	High-cost precision weapons vs. High-value targets	Asymmetric Attrition: Low-cost autonomous systems neutralizing expensive legacy assets.
OPERATIONAL	Command & Control (C2)	Hierarchical, rigid chains; slow information flow.	Networked/Distributed C2: Algorithmic compression of OODA loops and algorithmic fog of war (Cognitive Warfare)
	Intelligence (ISR)	State monopoly on high-altitude assets; siloed data.	Fusion of commercial satellite data & AI analytics
TACTICAL	Maneuver & Engagement	Human-centric fire & maneuver; visual concealment.	Ubiquitous Surveillance: "Transparent Battlefield" where concealment is nearly impossible; Swarm tactics.
	Naval Domain	Blue-water dominance via large surface combatants.	Sea Denial: Area access denial using low-profile, autonomous USVs (e.g., Sea Baby).

Table 5: Multi-level strategic shifts in the Russo-Ukrainian conflict

2.5 USA vs. China: an emerging AI Arms Race

This section analyzes the intensifying technological rivalry between the United States and China, examining it through the lens of an emerging Artificial Intelligence arms race. Firstly, the strategic frameworks guiding each nation's approach to AI dominance are compared to highlight diverging doctrinal priorities. Subsequently, the analysis examines the material basis of this competition, focusing on critical assets such as semiconductors, data centers, and raw materials that support AI supremacy. Finally, the section explores how the unique characteristics of AI, including speed and opacity, exacerbate the security dilemma between these two great powers, potentially destabilizing the international order.

2.5.1 Comparison of the USA’s and China’s strategic frameworks in AI

Artificial Intelligence and the Third Offset

The Third Offset recognizes that military supremacy can be maintained against strategic competitors, such as China and Russia, by advancing Artificial Intelligence and autonomous technologies, being the necessary “technological sauce” as former Deputy Secretary of Defense Bob Work put it in 2016 (Work, 2016). Unlike the First and the Second Offsets, which relied on nuclear deterrence and precision-guided munitions mainly developed through government research, the Third Offset is based on innovations that the private sector is leading, such as autonomous systems, Big Data analytics and advanced computing (Louth & Taylor, 2016). In this context, as Work mentioned, every country becomes a “fast follower”, and that’s why it is significant for the US and its allies to become “fast leaders” (Work, 2016), which strategically means that they must adopt and adapt successfully these technologies into their militaries faster than any other adversary in order to offset them.

A critical aspect of the Third Offset is to achieve a “human-machine symbiosis”, which gives priority to a collaborative-networked approach between humans and machines in warfare rather than fully autonomous lethal systems (LAWs), not only keeping the human in the loop but also empowering his capacity (Work, 2016). This approach tries to combine the speed and processing power of machines with human strategic judgement, which potentially enables the U.S. forces to disrupt decision-making cycles of their adversaries who may also possess similar systems. However, to achieve this requires building trust in the technology; particularly, decision-makers must participate in the development of algorithms to trust them (Hunter, et al., 2017, p. 10), as human operators will not be able to react fast enough to match the speed of autonomous systems.

Regarding Big Data, the Third Offset considers information processing as a crucial operational capability, especially for hybrid warfare. Work mentions big data analytics potential, as he essentially describes the "little green men" phenomenon, namely unmarked Russian forces, as a big data analytics problem that can be solved by collecting and analyzing open-source information, such as social media posts and geolocation data (Work, 2016). Furthermore, exploiting AI and automation allows U.S. forces to operate from greater distances and utilize "distributed capabilities" that are more difficult to engage with, ensuring that the destruction of a single high-value asset will not diminish its power on the field (Hunter, et al., 2017, p. 7). The Department of Defense tried to materialize these concepts through "pathfinder" projects, such as "Project Maven", which was a success (Gentile, et al., 2021, pp. 46-47), utilizing machine learning to process vast amounts of video recordings from UAVs to generate actionable insights to combat the Islamic State.

According to this strategic approach it is also necessary to achieve significant organizational innovation to successfully incorporate private sector technologies into state power (Gentile, et al., 2021, p. 53). As the Department of Defense (DoD) no longer holds the monopoly of technological innovation as it did during the previous Offsets, it had to cooperate with technological hubs, such as Silicon Valley, to exploit these technologies; this is why the DIU (Defense Innovation Unit) was created, to function as the connecting link between private sector and the state, and speed up the process of commercial technologies integration into the U.S. military. It is crucial for the DoD to adopt a "fail fast" culture, as successful integration depends on embracing the risk of failure, which is a natural characteristic of innovation, in order to find what works quickly (Hunter, et al., 2017, p. 3). Ultimately, the adoption and utilization of AI and Big Data is part of the broader effort of the USA, along with new organizational concepts and constructs, to maintain its supremacy through its deterrence capability (Work, 2016).

<u>Benefits and risks of the American AI Action Plan</u>

Following the Third Offset introduction, the Trump Administration presented an AI Action Plan in July 2025, that incorporates a comprehensive strategy to secure US hegemony in the ever-evolving AI domain. The document outlines a national security imperative to achieve technological dominance through three distinct pillars: "innovation, infrastructure, and international security and diplomacy" (The White House, 2025).

The first pillar, "Accelerate AI Innovation", focuses on creating a regulatory framework favorable for private sector's growth removing bureaucratic obstacles. The second pillar, "Build American AI Infrastructure", addresses the physical, and energy and environmental dimensions of the digital economy, prioritizing infrastructural growth, particularly data centers and semiconductor manufacturing to support military, intelligence and protect supply chains from adversaries. Finally, the third pillar, “Lead in International AI Diplomacy and Security”, concentrates on projecting American power globally and limit the influence of China in international organizations, by making dependent their allies on American AI technology utilizing financial instruments to facilitate deals and exports, and by setting the standards in the emerging AI global order.

This new strategic policy shows a significant shift in the United States grand strategy, giving priority to rapid technological acceleration and market-driven expansion to reinforce and keep its hegemony over the international system while powerful competing states arise. While this plan may offer critical methods to enhance American hard and soft power alike, it may also introduce risks regarding strategic stability, alliance unity, and the proliferation of dual-use technologies.

One strategic benefit associated with normative power is the plan’s all-inclusive export strategy - including hardware, software, data , cybersecurity, and applications - designed to set American technological standards as the global norm and limit China’s influence in this matter (CSIS, 2025). As Jonathan Hillman argued, this plan “takes a clear aim at China’s Digital Silk Road”; by enabling and facilitating the export of the full AI ecosystem, the US seeks to prevent allies from becoming dependent on adversarial technologies, such as those provided by Chinese Huawei (CFR, 2025).

However, this aggressive pursuit of power may bring forward significant diplomatic and geopolitical risks. Analysts argue that the plan is a “zero-sum” game for the US and its allies, the latter are viewed as customers for American exports rather than partners, which could lead to adverse results (CFR, 2025). Indeed, as Raul Brens claims, this model risks turning away key partners in Europe and Indo-Pacific who have prioritized their digital sovereignty and ethical AI development (Atlantic Council, 2025). Similarly, experts Unger and McLean mention that the American approach will probably pose challenges in partnerships with the Global South as the exported AI ecosystem is not infrastructurally appropriate for many countries, something that may lead them to China’s technological approach and infrastructure (CSIS, 2025).

Regarding national security, the AI plan discusses mechanisms of enhancing military operations, that may fundamentally alter the strategic landscape. Critically, the plan (The White House, 2025) includes measures that accelerate the adoption of autonomous technologies in warfighting, establishing for example an “AI & Autonomous Systems Virtual Proving Ground”. According to Horowitz (CFR, 2025), this is a crucial recommendation as it could enable “trusted confidence” and “scale adoption” for AI systems, which are nevertheless dependent on providing enough resources and prioritization. Additionally, the plan mandates access to private sector computing resources in case of national emergencies to secure use of AI in significant conflicts. As far as cybersecurity is concerned, the creation of an AI Information Sharing and

Analysis Center (AI-ISAC) is promoted as it could prove to be vital for defending against cyber threats and securing the digital industrial ecosystem.

Conversely, the rapid integration of AI into defense structures could create high risks of escalation or miscalculation. As Dumbacher (CFR, 2025) argues, while AI is able to transform military and back-office operations, it should not be applied in "strategic early warning" systems or anywhere else of strategic importance, as AI is a "black box" and introducing it in high-value decision-making processes where errors are not tolerated could prove to be catastrophic. Additionally, the administration's preference for open-source and open-weight models while it has positive influence on the private sector, researchers and the economy (Meinhardt , et al., 2025), it lowers at the same time the barrier to entry even for non-state actors providing them with advanced capabilities, including weapon creation and disinformation campaigns (CFR, 2025).

Following the AI Action Plan, the Department of Defense published a memorandum at the beginning of 2026 that puts the military on alert to accelerate AI adoption and become an "AI-first" force. The DoD's plan (U.S. Department of Defense, 2026) focuses on speed, launching seven projects that will surpass bureaucratic obstacles, reject social ideology and safety considerations, and bring commercial tech into battle swiftly. To execute this plan, the Department has launched seven projects in the fields of warfighting, intelligence and enterprise. These include AI Agents in OODA loops and kill chain executions ("Agent Network"), USA's elite troops AI-enhancement ("Swarm Forge"), timeline compression turning intelligence into weapons in hours ("Open Arsenal"), and empowering all personnel with the best AI models ("GenAI.Mil"). Finally, to support these projects, the Department has established unprecedented standards as expectations; for example, removing most barriers to data sharing and testing like it is wartime and deployment of the latest AI models to warfighters within 30 days of public release.

Ultimately, while the AI Action Plan addresses critical obstacles for the US hard power, the limitations on the developmental framework of AI along with an offensive diplomatic stance can increase the fragility of international security and the balance of power. Critically, the latest plan by the DoD shows that fully autonomous operations may be on the way, while any norm that slows down or hinders AI development and adoption is an obstacle that needs to be removed. In essence, it remains to be seen if the goal of winning the AI race will lead to a critical destabilization of the international system or not.

<u>China's strategy and the role of AI</u>

China's PLA (People's Liberation Army) is under a profound paradigm shift as it changes its focus from "informatized warfare"[11] to "intelligentized warfare"[12]. This transition posits that as the industrial age birthed mechanized warfare, and the information age the informatized warfare, similarly now the advent of Artificial Intelligence produces the "intelligentized warfare" (Masafumi, 2022). By mastering the emerging technologies, China aims to set new conditions for victory, not based on physical destruction but on decision superiority and cognitive supremacy.

A critical assumption in relation to Command and Control that leads this strategic approach, is that in modern combat the human brain does not have the capability to process the exponential volume of battlefield data in real-time, rendering the traditional vertical chain of command obsolete (Masafumi, 2022). In order to overcome this limitation, the PLA envisions a "command brain" characterized by "human-machine joint decision making", introducing a new type of command systems. Simultaneously, the PLA seems to prioritize the mass deployment of unmanned systems and autonomous swarms, as they can offer better value than conventional military assets in the battlefield because of their lower costs and effectiveness.

In this context, the operational environment expands from traditional physical dimensions, like the air and the sea, to include "virtual spaces", thus the cognitive domain emerges as a main battlefield. In this new space, the PLA prioritizes "cognitive confrontation" (Masafumi, 2022), a strategy that employs manipulation and morale targeting through the control of information and public opinion. The objective here is not to kinetically confront the enemy but to "blind, deafen, and paralyze" the opponent's decision-making capacity, to achieve victory before any physical confrontation by denying the enemy's option to wage war. Additionally, the PLA considers that future conflicts will be decided by a "game of algorithms" (Masafumi, 2022), where the quality of AI code determines who is superior in the battlefield. In this context, "intelligence dominance" which is the ability to control and process information faster than the enemy, becomes a decisive factor in future warfare.

Evidently, the PLA has operationalized the "Multi-Domain Precision Warfare" (MDPW) concept which functions as the practical application of the "intelligentized warfare". It employs a C4ISR network to unify forces under one command, rapidly combine multi-domain forces, and target weak points in the

[11] "The PLA describes **informatized warfare** as the use of information technology to create an operational system-of-systems, enabling the PLA to acquire, transmit, process, and use information during a conflict to conduct integrated joint military operations across the ground, maritime, air, space, cyberspace, and electromagnetic spectrum domains." (U.S. Department of Defense, 2024)

[12] The PLA is pursuing next-generation combat capabilities based on its vision of future conflict, which it calls "**intelligentized warfare**," defined by the expanded use of AI, quantum computing, big data, and other advanced technologies at every level of warfare. (U.S. Department of Defense, 2024)

U.S. military system (U.S. Department of Defense, 2025, p. 13). This approach prioritizes the use of Big Data and AI to swiftly evaluate immense amounts of data in order to accelerate OODA loops.

These operational imperatives are in need of a broader strategic framework to succeed in adopting and adapting AI technologies fast enough to deter or engage with the USA. In this context, the "Military-Civil Fusion" (MCF) strategy shows how China pivoted its approach to power by removing the barriers between the private and defense sector to create a "fused" ecosystem that feeds national power with critical assets. To put it simply, MCF's goal is to fully integrate civilian industry into the PLA's supply chain (Can & Vieira, 2022, p. 85), where various resources such as start-ups, researchers, and facilities, are considered of great importance (Masaaki, 2022, p. 29). The leveraging of academic research and talent is apparent, as the concept of "seven sons of national defense" reveals, where the most prominent Chinese universities supply state defense industry with graduates.

Moreover, Beijing always aims to implement and update this strategy, introducing periodically plans to achieve this. In this sense, the upcoming 15th Five Year Plan (2026-2030) is expected to expand the MCF, including also the AI-Plus initiative. The latter will include crucial regulatory imperatives that introduce "born dual-use" technologies, as a result of integrating military requirements into R&D for several civilian sectors, even public welfare (Wang, 2025), ensuring that innovations serve defense needs even before their birth. Evidently, by zeroing the time needed for a civilian tech to be adapted and adopted by the military, China seeks to close or surpass the gap with the USA, creating a structural advantage over their adversaries and obtaining the capability to execute the plan for "intelligentized warfare". For instance, LLMs[13] development by Chinese tech giants is expected to directly enhance military strength, including intelligence and autonomous weapons (Wang, 2025). Eventually, this means that a distinction between civilian tech companies and military contractors will be obscured, making power measurement even more difficult.

Regarding Big Data, it is a logical assumption that in the framework of Military-Civilian Fusion strategy, China exploits collected data to train algorithms for military purposes. For instance, according to evidence the deployment of surveillance technologies in the Uyghur region serves as a testing ground for state experiments including controversial ones (Can & Vieira, 2022, pp. 91-92). This approach enables Beijing to surpass ethical and legal frameworks that limit military AI development by the West, as internal security mechanisms are utilized to achieve any national goal.

[13] Large Language Models

This fusion strategy serves also as a mechanism that surpasses international restrictions on military technology transfer. Chinese civilian companies obtain foreign technologies, such as semiconductors and drones, for commercial use, and then they transform them and integrate them into the military (Descamps, et al., 2025, p. 4). Ultimately, removing the distinction between commercial and defense sector and reorganizing the economy to provide crucial advantages for strategic competition reveals a mechanism that rapidly accelerates the transformation of latent capabilities to traditional hard power.

Discussion

Critically, assessing the two strategic frameworks and various plans, it becomes evident that the two countries share some common rationales, while having distinct differences in certain aspects. Fundamentally, both nations share the assumption that human cognitive capacity is not enough for the complexity of modern warfare, while AI has the necessary processing power and speed to accomplish that. In this context, both powers seek to enhance warfighting with these technologies with a clear focus on disrupting decision-making loops.

However, the organizational approaches employed to achieve technological supremacy are significantly different. The US approach is defined by a market-driven logic where the state treats the private sector as a separate entity. Conversely, China's "Military-Civil Fusion" seeks to eliminate this separation, by integrating civilian R&D advances directly into its defense architecture, bypassing the bureaucratic friction the US must deal with. Nonetheless, more recent developments such as the AI action plan and the DoD memo reveal that the US is shifting to a more aggressive approach, maybe under the pressure of an intensified security dilemma.

2.5.2 The material basis of AI supremacy

Critically, the strategic and operational frameworks that define China's and USA's ambitions do not complete the geopolitical picture, as it is also necessary to discuss the material capacity that enables the realization of these approaches. In this sense, the AI arms race is not just about an algorithmic war, but a competition for material assets that build computational power. Therefore, it is logical to examine the role of semiconductors, datacenters, rare earths, and energy infrastructures that enable AI system development and strategic chokepoint actions.

Firstly, semiconductor supply chains have acquired strategic importance in the global security landscape, affecting the balance of power between major powers. Indeed, data centers and advanced chips have become strategic assets comparable to power plants and oil as they dictate national growth and national security (Esposito, 2025). Consequently, the Sino-American rivalry has evolved into a zero-sum game for technological supremacy, leading both nations to weaponize economic interdependence through aggressive politics (Jia, et al., 2025; Wu, et al., 2024).

Evidently, the US has utilized its dominance in the upstream segments of the semiconductor value chain (Jia, et al., 2025), such chip design software and semiconductor manufacturing equipment, to limit China's technological growth (Allen, 2022). USA has utilized its normative power through the "foreign direct product rule" which effectively extends its jurisdiction outside of the country to prevent foreign firms from supplying Chinese companies when US technology is part of the exported product. Additionally, Washington seeks to strengthen this control leveraging its alliances; particularly, it has formed the "Chip 4" alliance with Japan, South Korea, and Taiwan, aiming to strengthen export controls and restrain Chinese access to critical semiconductor nodes (Esposito, 2025).

Conversely, China is determined to counter these containment measures that are a threat to its growth, mobilizing several assets, such as intelligence services and the media, to attract U.S. security partners to its side (U.S. Department of Defense, 2025, pp. 51-52). Additionally, China leverages its comparative advantages in the midstream and downstream parts of the supply chain, like wafer fabrication, as it has a significant market share (Jia, et al., 2025). The country has also taken other measures to facilitate its technological development especially for the semiconductor industry such as the "Big Fund", which focuses on increasing "in-house" manufacturing capabilities and overcoming difficulties in upstream activities.

Furthermore, China utilizes a variety of tools and methods to surpass US restrictions and materialize its national goals. These include the accumulation of high-end chips, shell companies that acquire restricted technology and aggressive experts' recruitment (U.S. Department of Defense, 2025). In particular, talent acquisition is essential for Chinese technological supremacy, implemented by several policies such as state-funded exchange programs, academic cooperation with top-tier organizations, and encouraging overseas studies for Chinese researchers (Jia, et al., 2025). Naturally, the country leverages also the dependencies the Digital Silk Road create to expand its AI potential.

Another material aspect of driving AI competition is hyperscale datacenters[14], which possess the capacity to control data generation and processing, becoming in essence a strategic asset (Esposito, 2025). In this matter, there is

[14] A hyperscale data center is a massive data center that provides extreme scalability capabilities and is engineered for large-scale workloads with an optimized network infrastructure, streamlined network connectivity and minimized latency. (Source: IBM)

a significant asymmetry as the US has hegemonic influence, possessing 55% of global hyperscale capability (Synergy Research Group, 2025), and Amazon, Microsoft, and Google maintaining 58% of global capacity. This creates a major dependency on U.S. cloud services, which creates security vulnerabilities for allies and rivals alike. On the contrary, China, like some EU countries, seeks to enhance its digital sovereignty by enclosing sensitive data into national silos (Esposito, 2025).

Moreover, scarce minerals and energy infrastructure play a vital role in achieving superiority in AI technologies. Advanced and high-performance computing requires energy inputs that are similar to those of medium-size cities, which creates a logistic vulnerability, as LLMs and autonomous systems rely on stable and high-capacity power grids (Walden, 2025). Critically, datacenters are expected by 2035 to require globally almost the same electricity as India (Juani, et al., 2025). Such high energy demands create a dependency on sustainable power, such as nuclear, which creates limitations for rapid construction of data centers, while energy produced by fossil fuels continues to play a central role in sustaining and developing datacenters for USA and China alike.

Finally, there is a great dependence on rare earths, as they are necessary for datacenters, chips, and AI systems manufacturing. In this domain, China has a dominant monopoly in critical mineral supply chain; for example the country controls 98% of global gallium production and 60% of germanium refining, which are essential for top tier semiconductors and fiber optics (Leader, et al., 2025). While its monopoly has slightly decreased since 2011, this asymmetry enables Beijing to weaponize supply chains through export controls to constrain supplies for U.S. semiconductor and defense industries aiming at slowing down US technological progress (Walden, 2025). This has led the US to the aid of its allies to obtain significant mineral assets through bilateral agreements, for example with Greenland and Ukraine (Leader, et al., 2025). Interestingly, Greenland ranks 8th globally for its rare earth reserves, which provides a critical geoeconomic rationale for the second Trump administration's strategic interest in acquiring the island (Swartz & Baskaran, 2026).

2.5.3 Artificial Intelligence and the security dilemma

Under the technological evolution and the integration of Artificial Intelligence into national security strategies, the security dilemma is crucially affected by unprecedented speed, opacity, and dual-use complexities. This dynamic is best understood through the concept of "dual-use distinguishability", referring to the ambiguity a state encounters when trying to distinguish whether another state's technological developments serve military or civilian goals (Kot, 2025). In this sense, low distinguishability worsens the security dilemma as states are uncertain of the other's intentions, leading to the worst assumptions and adopting competitive measures to secure themselves (Kot, 2025).

Figure 15: Conceptual Framework of AI's Impact on the Security Dilemma (Source: Author's elaboration)

In this context, a "technological security dilemma"[15] emerges, wherein the measures a state takes to enhance its technological security are considered threats by adversaries, causing a "tit-for-tat" approach that threatens stability (Lim & Ferguson, 2020). Regarding AI, this dilemma is intensified by the imperative for speed, as the need to accelerate OODA loops has proven (U.S. Department of Defense, 2026).

Particularly, the inherent characteristics of AI strengthen the security dilemma between the US and China in multiple ways, and as Graham Allison argues, this technology "will continue to be at the forefront of the fiercest Thucydidean rivalry history has ever seen". It is evident there is a race to achieve dominance in AI capabilities, driven by the fear that the competitor might utilize a technology that threatens national survival (Allison, 2024). Responding to this imperative, the US military intends to aggressively integrate AI and become an AI-first force (U.S. Department of Defense, 2026). Furthermore, the dilemma is exacerbated by the fact that AI development is heavily dependent on the private sector, creating a complex strategic environment. China's response is the Military-Civil Fusion strategy, which creates another risk for the USA, as Chinese companies could act as spies for their government (Lim & Ferguson, 2020). This is why interdependence is considered a vulnerability, leading to US-China decoupling, reducing exposure to foreign influence.

Moreover, the uncertainty that accompanies AI creates another cause for instability in the international system, as the risks are unknown and impossible to deal with (Allison, 2024). Unlike nuclear weapons, AI is not under strict control, but a democratized technology that spreads AI capabilities to multiple actors.

[15] Or "dual-use security dilemma" (Kot, 2025)

In this context, China's technological advance threatens American hegemony, intensifying this way the security dilemma. As Eric Schmidt maintained, China is now a "full spectrum peer competitor" in AI (Allison, et al., 2021). Evidently, China has already surpassed the United States in certain areas, such as AI patents and the deployment of 5G infrastructure, acquiring first-mover advantages. Moreover, this threat is evidenced by China's structural advantages, like the immense data pool, a supportive policy environment, and a rapid pace of implementation (Allison, et al., 2021). As a result, Washington sees these developments not as normal progress, but as a direct threat to international order, reinforcing the security dilemma and triggering a defensive reaction that further escalates the instability.

3. Conclusion and Synthesis

The analysis conducted in this research confirms the hypothesis that technology is not merely a tool for economic growth, but a structural modifier of the international system capable of redistributing power. As demonstrated in the theoretical framework and verified through the historical analysis of military revolutions—from the trireme to the nuclear age—disruptive innovations create conditions for systemic change. This dynamic is fully evidenced in the 21st century by the case of the Russo-Ukrainian conflict.

The empirical data from the war in Ukraine validates the argument that technology functions as a force multiplier, giving a comparative advantage to a weaker state against a materially superior adversary. The successful deployment of low-cost autonomous systems, such as drones and loitering munitions, against Russia's conventional heavy armor, proves that innovation power can counterbalance traditional mass. Furthermore, the strategic use of unmanned surface vessels (USVs) by Ukraine to achieve sea denial against the Russian Navy confirms that relatively inexpensive technological solutions can neutralize expensive assets, effectively altering the operational balance of power.

This reality explains why states are engaged in intense technological competition. As shown in the analysis of the US-China rivalry, the race for Artificial Intelligence is driven by the realization that technological supremacy equates to national survival. The integration of AI into military strategies, as seen in China's "Intelligentized Warfare" and the US "Third Offset", proves that great powers view technology as the primary means to increase their relative power and secure their position in the anarchic international system.

Furthermore, despite China's rapid rise and its status as a "full-spectrum peer competitor", the findings of this research suggest that the United States maintains its technological hegemony in critical qualitative metrics. While China has successfully utilized the "late-mover advantage" to become a leader in manufacturing and scientific output (e.g. patents and publications), the US retains a structural advantage in the "center of gravity" of the AI ecosystem.

The comparative analysis of material capabilities reveals that the US dominates in high-performance computing, controlling 58% of global hyperscale data centers compared to China's 16% . Furthermore, the American private sector's investment in AI remains vastly superior, spending almost 12 times more than China in 2024. Crucially, the US control over the upstream segments of the semiconductor supply chain (chip design and tools) allows Washington to weaponize this interdependence.

This empirical evidence validates the theory of "Weaponized Interdependence" presented in the first chapter. Contrary to liberal institutionalist expectations that connectivity fosters peace, the US has successfully turned central hubs of the global economy — specifically the semiconductor chokepoints — into instruments of coercion to contain China's rise. Therefore, while the gap is narrowing, the structural hierarchy of the international system has not yet been overturned.

Ultimately, this thesis argues that the realist approach, and specifically Neoclassical Realism, offers the most robust explanatory framework for understanding the disruptive nature of technology in global affairs. The transition from a unipolar to a potential bipolar system is driven by the distribution of material power, but state behavior is defined by internal structures and threat perception.

The analysis of the US-China competition confirms Michael Horowitz's "Adoption-Capacity Theory". China's ability to implement a "Military-Civil Fusion" strategy demonstrates how internal state structure facilitates the rapid conversion of civilian innovation into military power, acting as a crucial variable in the balance of power. Conversely, the US response, characterized by the shift to a "wartime footing" and the rejection of bureaucratic hurdles, reveals how the perception of an existential threat mobilizes state resources.

Finally, the findings verify Robert Jervis's theory on the security dilemma. The inherent opacity and dual-use nature of Artificial Intelligence create a problem of distinguishability, where defensive technological advancements are inevitably perceived as offensive preparations. This uncertainty, combined with the compression of decision-making time — as predicted by the evolution of the OODA loop into machine-speed cycles — intensifies the security dilemma. Consequently, states are trapped in a self-reinforcing spiral of instability, where the pursuit of absolute security through AI supremacy paradoxically leads to greater systemic insecurity.

In conclusion, Artificial Intelligence is not just another technological tool; it is a structural determinant of 21st century international relations. By redefining the parameters of speed and power, Artificial Intelligence reinforces the realist assertion that technological innovation remains a decisive factor for state survival in an anarchic international system.

Recommendations for future research:

While this thesis focused on the technological aspect of great power competition, future scholarship should broaden the scope to examine the strategic influence of "middle powers" and the Global South, as well as the disruptive combination of AI with quantum computing and biotechnology. Additionally, scholars should investigate the feasibility of international AI arms control regimes within an anarchic system. Most critically, further inquiry is required into the emergence of Artificial Intelligence as a potential non-state actor, analyzing how algorithmic agency and the rise of Big Tech challenge the traditional state-centric security architecture and the international balance of power.

Bibliography

Abdurasulov, A., 2025. The new AI arms race changing the war in Ukraine. *BBC*, 10 October.

Aka, H., 2025. Why Big Tech Matters for National Security. *Information Technology & Innovation Foundation*, 24 January.

Akhtar, A., 2025. The Role of AI in U.S. and Russian Military Operations and Its Implications on Ukraine's Cyber and National Security. *Journal of Regional Studies Review,* 4(1), pp. 516-525.

Allen, G. C., 2017. Project Maven brings AI to the fight against ISIS. *Bulletin of the Atomic Scientists*, 21 December .

Allen, G. C., 2022. *Choking off China's Access to the Future of AI.* s.l.:Center for Strategic and International Studies.

Allison, G., 2024. *The National Insecurity of AI.* s.l.:Aspen Strategy Group.

Allison, G., Klyman, K., Barbesino , K. & Yen, H., 2021. *The Great Tech Rivalry: China vs the U.S.,* s.l.: Harvard Kennedy School.

Altmann, J. & Sauer, F., 2017. Autonomous Weapon Systems and Strategic Stability. *Survival,* 59(5), pp. 117-142.

Amoore, L. & Raley, R., 2016. Securing with algorithms: Knowledge, decision, sovereignty. *Security Dialogue,* 48(1), pp. 3-10.

Atlantic Council, 2025. *Experts react: What Trump's new AI Action Plan means for tech, energy, the economy, and more.* Washington, DC: Atlantic Council.

Aviv, I. & Ferri, U., 2023. Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. *International Journal of Critical Infrastructure Protection,* Τόμος 43.

Bell, A., 2025. *The Motley Fool.* [Ηλεκτρονικό]
Available at: https://www.fool.com.au/2025/09/26/what-in-the-world-is-a-semiconductor-and-why-is-it-the-backbone-of-artificial-intelligence/
[Πρόσβαση 30 December 2025].

Bendett, S., 2023. *Roles and Implications of AI in the Russian-Ukrainian Conflict.* s.l.: Belfer Center for Science and International Affairs.

Benson, B. V. & Goldstein, B. J., 2026. The Fog of AI: What the Technology Means for Deterrence and War. *Forreign Affairs*, 6 January .

Boulanin , V. & Verbruggen, M., 2017. *Mapping the Development of Autonomy in Weapon Systems,* Stockholm : Stockholm International Peace Reasearch Institute.

Bradford, A., 2016. *The EU as a regulatory power,* s.l.: European Council on Foreign Relations.

Brandt, J., Sacks, S., Schaake, M. & Meserole, C., 2023. *The geopolitics of generative AI.* s.l.:The Brookings Institution.

Brooks, H., 1980. Technology, Evolution, and Purpose. *Daedalus*, Winter, 109(1), pp. 65-81.

Brose, C., 2019. The New Revolution in Military Affairs: War's Sci-Fi Future. *Foreign Affairs,* 98(3), pp. 122-134.

Bucy, J. F., 1980. Technology Transfer and East-West Trade: A Reappraisal. *International Security,* , 5(3), pp. 132-151.

Calzati, S., 2022. ‘Data sovereignty’ or ‘Data colonialism’? Exploring the Chinese involvement in Africa’s ICTs: a document review on Kenya. *Journal of Contemporary African Studies,* 40(2), pp. 270-285.

Can, M. & Vieira, A., 2022. The Chinese Military-Civil Fusion Strategy: A State Action Theory Perspective. *The International Spectator,* 57(3), pp. 85-102.

Can, M. & Vieira, A., 2022. The Chinese Military-Civil Fusion Strategy: A State Action. *THE INTERNATIONAL SPECTATOR,* 57(3), pp. 85-102.

CFR, 2025. *The Opportunities and Risks of Trump’s AI Action Plan.* New York, NY: Council on Foreign Relations.

Chin, J., 2026. China Trains AI-Controlled Weapons With Learning From Hawks, Coyotes. *The Wall Street Journal*, 24 January.

CIA, 2024. *www.cia.gov.* [Ηλεκτρονικό]
Available at: https://www.cia.gov/the-world-factbook/field/gdp-composition-by-sector-of-origin/
[Πρόσβαση 24 December 2025].

Cohen, E., 2002. Technology and Warfare. Στο: J. Baylis, J. Wirtz, E. Cohen & C. Gray, επιμ. *Strategy in the Contemporary World: An Introduction to Strategic Studies.* New York: Oxford University Press, p. 247.

Csernatoni, R., 2025. Corporate Geopolitics: When Billionaires Rival States. *Strategic Europe*, 30 October.

CSIS, 2025. *Experts React: Unpacking the Trump Administration’s Plan to Win the AI Race.* Washington, DC: Center for Strategic and International Studies.

Davis, Z. S. & Nacht, M., 2018. *Strategic Latency: Red, White, and Blue, Managing the National and International Security Consequences of Disruptive Technologies.* 1st επιμ. Livermore: Lawrence Livermore National Laboratory.

Descamps, M., Yuan, J. & Zhu, Y., 2025. *Military-civil fusion is a key Chinese strategy with long-term implications.* Stockholm: Institute for Security & Development Policy.

DeVries, K., 1998. Gunpowder Weaponry and the Rise of the Early Modern State. *War in History,* 5(2), pp. 127-145.

Dong, J., 2025. Rethinking Offense and Defense in the AI Era. *The Diplomat,* 28 October.

Drezner, D., 2019. Technological change and international relations. *International Relations*, March, pp. 6-8.

Durand , C., Morozov, E. & Watkins, S., 2025. How Big Tech Became Part of the State. *Jacobin*, 24 November.

Edler, J., Blind, K., Kroll, H. & Schubert, T., 2023. Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. *Research Policy*, 28 March, 52(6).

Eriksson, J. & Newlove-Eriksson, L. M., 2021. Theorizing technology and international relations: prevailing perspectives and new horizons. Στο: G. Giacomello, F. N. Moro & M. Valigi, επιμ. *Technology and International Relations: The New Frontier in Global Power.* Cheltenham: Edward Elgar Publishing, pp. 3-22.

Erskine, T. και συν., 2025. *AI, Automated Systems, and Resort-to-Force Decision Making – Policy Recommendations,* Canberra: Australian National University.

Esposito, M., 2025. *AI geopolitics and data centres in the age of technological rivalry.* s.l.:World Economic Forum.

Farnell, R. & Coffey, K., 2024. *AI's New Frontier in War Planning: How AI Agents Can Revolutionize Military Decision-Making.* s.l.:Belfer Center for Science and International Affairs.

Farrell, H., 2025. The twilight of tech unilateralism. *Programmable Mutter*, 19 August.

Farrell, H. & Newman, A. L., 2019. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security* , 1 July, pp. 42-79.

Fred, B. J., 1980-1981. Technology Transfer and East-West Trade: A Reappraisal. *International Security* , p. 134.

Froelich, P., 2021. Killer drone 'hunted down a human target' without being told to. *New York Post*, 29 May.

Gabai, U., 2025. States vs. silicon: The global balance of power. *Geopolitical Intelligence Services*, 28 August.

Gentile, G. και συν., 2021. *A History of the Third Offset, 2014–2018,* Santa Monica, CA: RAND Corporation.

Gill, A. S., 2019. Artificial Intelligence and International Security: The Long View. *Ethics & International Affairs,* 33(2), pp. 169-179.

Gilpin, R., 1988. The Theory of Hegemonic War. *The Journal of Interdisciplinary History,* 18(4), pp. 591-613.

Gompert, D. C., Binnendijk, H. & Lin, B., 2014. The Information Value Chain and the Use of Information for Strategic. Στο: *Blinders, Blunders, and Wars: What America and China Can Learn.* s.l.:RAND Corporation, pp. 25-40.

Goncharuk, V., 2024. *Artificial Intelligence in Defence of Ukraine,* Tallinn: International Centre for Defence and Security.

Gray, C. S., 2004. *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History.* 1st Edition επιμ. London: Routledge.

Helberg, J., 2020. *foreignpolicy.com.* [Online]
Available at: https://foreignpolicy.com/2020/06/22/zoom-china-us-cold-war-unsafe/
[Accessed 25 June 2020].

Herrera, G. L., 2006. *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change.* 1st edition επιμ. Albany: State University of New York Press.

Horowitz, M. C., 2010. *The Diffusion of Military Power: Causes and Consequences for International Politics.* Course Book ed. επιμ. Princeton: Princeton University Press.

Horowitz, M. C., 2018. Artificial Intelligence, International Competition, and the Balance of Power. *Texas National Security Review*, May, 1(3), pp. 36-57.

Horowitz, M. C. & Kahn, L. A., 2025. Nuclear Non-Proliferation Is the Wrong Framework for AI Governance. *AI Frontiers,* 27 June.

Horowitz, M. C. & Scharre, P., 2021. *AI and International Stability: Risks and Confidence-Building Measures,* Washington, DC: Center for a New American Security.

Horowitz, M., Kania, E., Allen, G. & Scharre, P., 2018. Strategic Competition in an Era of Articial Intelliegence. 25 July, pp. 4-5.

Huelss, H., 2025. Transcending the fog of war? US military 'AI', vision, and the emergent post-scopic regime. *European Journal of International Security,* 10(2), pp. 190-210.

Hunter, A. P., Coll, G. & Hicks, K. H., 2017. *Assessing the Third Offset Strategy,* Washington, DC: Center for Strategic and International Studies.

Intel Corporation, 2025. Intel and Trump Administration Reach Historic Agreement to Accelerate American Technology and Manufacturing Leadership. 22 August.

Jervis, R., 1978. Cooperation Under the Security Dilemma. *World Politics,* 30(2), pp. 167-214.

Jia, F. και συν., 2025. Global semiconductor supply chain: a national competitiveness analysis. *International Journal of Production Research.*

Johnson, J., 2019. Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*, 24 April, 35(2), p. 147–169.

Johnson, J., 2022. The AI Commander Problem: Ethical, Political, and Psychological Dilemmas of Human-Machine Interactions in AI-enabled Warfare. *Journal of Military Ethics,* 21(3-4), pp. 246-271.

Juani, A., Doris, A., Alam, M. & Carlson, A., 2025. *Powering the AI Era: Meeting energy goals amid the AI boom in Washington State,* s.l.: Foreign Policy.

Kang, S. C., 2021. China's crackdown on Alibaba goes beyond teaching Jack Ma a lesson. *S&P Global*, 19 January.

Katagiri, N., 2024. Artificial Intelligence and Cross-Domain Warfare: Balance of Power and Unintended Escalation. *Global Society,* 38(1), pp. 34-48.

Khanal, S., Zhang, H. & Taeihagh, . A., 2025. Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. *Policy and Society*, January, 44(1), pp. 52-69.

Klyman, K. & Piliero, R., 2024. AI and the A-bomb: What the analogy captures and misses. *Bulletin of the Atomic Scientists,* 9 September.

Kohara, M., 2005. Information Power and international security. *Porgress in Informatics,* Issue 1, pp. 39-46.

Kot, C. H. B., 2025. *Dual-use security dilemma and the U.S.-China AI technology race [Master's thesis],* Oxford: University of Oxford.

Krepinevich, A. F., 2002. *The Military-Technical Revolution: A Preliminary Assessment.* Washington: Center for Strategic and Budgetary Assessments.

Kulshrestha, S., 2016. *Big Data in Military Information & Intelligence.* s.l.:IndraStra Global.

Kuruc, M., 2024. Geopolitics of Artificial Intelligence: Development & Regulation in the Age of AI Race. *SAIS Review of International Affairs,* 44(2), pp. 47-55.

Leader, A., Doris, A., Juani, A. & Carlson, A., 2025. *Artificial Intelligence and the Critical Minerals Crunch: Strategies for resilient supply chains,* s.l.: Foreign Affairs.

Lee, E., 2025. *What are Autonomous Weapon Systems?.* s.l.:Belfer Center for Science and International Affairs.

Leipziger , D. & Dodev , V., 2016. *Disruptive Technologies and their Implications for Economic Policy: Some Preliminary Observations.* 1 επιμ. Washington: Institute for International Economic Policy, George Washington University.

Lele, A., 2019. *Disruptive Technologies for the Militaries and Security.* 1st επιμ. Singapore: Springer Singapore.

Levy, J. S. & Thompson, W. R., 2010. *Cuases of War.* 1st edition επιμ. Chichester,: Wiley-Blackwell.

Lewis, J. A., 2019. *The Risk of Technology Transfer." Emerging Technologies and Managing the Risk of Tech Transfer to China,* Washington, DC: Center for Strategic and International Studies (CSIS).

Lieber, K. A., 2000. Grasping the Technological Peace: The Offense-Defense Balance and International Security. *International Security,* 25(1), pp. 71-104.

Lim, D. J. & Ferguson, V., 2020. CONSCIOUS DECOUPLING: THE TECHNOLOGY SECURITY DILEMMA. Στο: J. Golley, L. Jaivin, B. Hillman & S. Strange, επιμ. *China Dreams.* s.l.:ANU Press.

Lin, H., 2025. Artificial Intelligence and Nuclear Weapons: A Commonsense Approach to Understanding Costs and Benefits. *Texas National Security Review,* 8(3), pp. 98-109.

Louth, J. & Taylor, T., 2016. The US Third Offset Strategy. *The RUSI Journal,* 161(3), pp. 66-71.

MacGregor, K. & Williamson, M., 2001. *The dynamics of military revolution: 1300-2050.* 1st edition επιμ. New York: Cambridge University Press.

Mallik, A., 2004. *Technology and Securityin the 21st Century: A Demand-side Perspective,* New York: Oxford University Press.

Mallik, A., 2016. *Role of Technology in International Affairs.* 1st edition επιμ. New Delhi: Pentagon Press.

Mamediieva, G., 2025. *Military AI: Lessons from Ukraine,* s.l.: Tech Policy Press.

Manish & Dyarakoti, A. S., 2025. Drones in India–Pakistan conflict: a comparative study with special focus on Operation Sindoor. *Small Wars & Insurgencies,* pp. 1-20.

Masaaki, Y., 2022. PLA's Intelligentized Warfare: The Politics on China's Military Strategy. *Security & Strategy,* Τόμος 2, pp. 17-36.

Masafumi, I., 2022. PLA's Perception about the Impact of AI on Military Affairs. *Security & Strategy,* Τόμος 2.

Maslej, N., Fattorini, L. & Raymond Perrault, Y. G. V. P. N. K. E. C. A. R. E., 2025. *The AI Index 2025 Annual Report,* Stanford: Stanford University.

Mazzucco, L. J. M., 2025. *How Ukraine's Unmanned Surface Vessels Have Reshaped Modern Naval Warfare in the Black Sea.* s.l.:Rabdan Security and Defence Institute.

McCarthy, D. R., 2015. *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and Internet.* 1st edition επιμ. London: Palgrave Macmillan.

McNeill, W. H., 1982. *The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000.* 1st edition επιμ. Chicago: University of Chicago Press.

McNeilly, M. R., 2015. *Sun Tzu and the Art of Modern Warfare.* 1st edition επιμ. New York: Oxford University Press.

Mearsheimer, J., 2001. *The Tragedy of Great Power Politics.* 1st επιμ. New York: W. W. Norton & Company.

Meinhardt , C. και συν., 2025. *Inside Trump's Ambitious AI Action Plan.* Stanford: Stanford Institute for Human-Centered AI (HAI).

Morris, J. F., 2024. *https://mwi.westpoint.edu/the-class-of-1982-modern-war-journal-issue-1-leadership-and-the-emerging-battlefield/.* [Ηλεκτρονικό]
Available at: https://mwi.westpoint.edu/the-class-of-1982-modern-war-journal-issue-1-leadership-and-the-emerging-battlefield/
[Πρόσβαση 18 December 2025].

Moyer, J. D., Meisel, C. J. & Matthews, A. S., 2023. Measuring and Forecasting the Rise of China: Reality over Image. *Journal of Contemporary China,* 32(140), pp. 191-206.

Nash, J., 2018. Sea Power in the Peloponnesian War. *Naval War College Review,* 71(1), pp. 119-139.

Osimen, G. U., Newo, O. & Fulani, O. M., 2024. Artificial intelligence and arms control in modern warfare. *Cogent Social Sciences,* 10(1).

Payne, K., 2018. *Strategy, Evolution, and War: From Apes to Artificial Intelligence.* 1st επιμ. Washington, DC: Georgetown University Press.

Payne, K., 2024. The Geopolitics of AI. *The RUSI Journal,* 169(5), pp. 54-55.

Pencheva, I., Esteve, M. & Mikhaylov, S. J., 2018. Big Data and AI – A transformational shift for government: So, what next for research?. *Public Policy and Administration,* 35(1), pp. 24-44.

Piercy, K., 2023. “I Do Not Think It Means What You Think": Information Power and Deterrence. *Wright Flyer Papers*, 31 January, p. 32.

Plano, J. C. & Olton, R., 1988. *The International Relations Dictionary.* 4th ed. Santa Barbara and Oxford: ABC-CLIO.

Platias, A. & Koliopoulos, C., 2010. *Thucydides on Strategy: Grand Strategies in the Peloponesian War and Their Relevance Today.* New York: Columbia University Press.

Puyvelde, D. V., Coulthart, S. & Hossain, S., 2017. Beyond the buzzword: big data and national security decision-making. *International Affairs,* 93(6), pp. 1397-1416.

Raska, M., 2025. *Mitigating the Risks of AI-Driven OODA Loops in Military Decision-Making,* The Hague: The Hague Centre for Strategic Studies .

Reuven, N. & Shamir, E., 2025. The shift in technological dominance and the adaption of open innovation by the defence sector. *Defense & Security Analysis,* 41(3), pp. 392-415.

Rikap, C., 2024. Antitrust Policy and Artificial Intelligence: Some Neglected Issues. *Institute for New Economic Thinking,* 10 June.

Rose, G., 1998. Neoclassical realism and theories of foreign policy. *World Politics,* 51(1), pp. 144-172.

Rosenbach, E. και συν., 2025. *Critical and Emerging Technologies Index,* Cambridge, MA: Belfer Center for Science and International Affairs.

Rühlig, T., 2020. *Technical standardisation, China and the future international order,* Brussels: Heinrich-Böll-Stiftung.

Rühlig, T., 2023. Chinese Influence through Technical Standardization Power. *Journal of Contemporary China,* 32(139), pp. 54-72.

Sagan, S. D. & Waltz , K. N., 2002. *The Spread of Nuclear Weapons: A Debate Renewed.* 2nd edition επιμ. New York: W. W. Norton & Company.

Saghir, A., Karim, A. & Hussain, R., 2025. Artificial Intelligence as the New Security Dilemma: A Neorealist Analysis. *Social Sciences Spectrum*, 27 October, pp. 96-116.

Scharre, P., 2018. *Army of None: Autonomous Weapons and the Futurre of War.* 1st edition επιμ. New York: W. W. Norton & Company.

Schlosser , A., 2018. *You may have heard data is the new oil. It's not.* s.l.:World Economic Forum.

Schoff, J. L., 2020. *U.S.-Japan Technology Policy Coordination: Balancing Technonationalism With a Globalized World,* Washington, D.C.: Carnegie Endowment for International Peace.

Seaman, J., 2020. *China and the New Geopolitics of Technical Standardization,* Paris: French Institute of International Relations (Ifri).

Sharikov, P., 2018. Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination. *Bulletin of the Atomic Scientists,* 74(6), pp. 368-373.

Simpson, K. H., Paquette, S., Racicot, R. & Villanove, S., 2025. *Militarizing AI: How to Catch the Digital Dragon?,* Waterloo, ON: Centre fro International Governance Innovation.

Skolnikoff, E., 1993. *The Elusive Transformation: Science, Technology, and the Evolution of International Politics.* Princeton, New Jersey: Princeton University Press.

Slusher, M. N., 2025. *Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience,* Washington, DC: Center for Strategic and International Studies.

Strange, S., 1994. *States and Markets.* 2nd επιμ. London: Continuoum.

Swartz, M. & Baskaran, G., 2026. *Greenland, Rare Earths, and Arctic Security.* Washington, DC: Center for Strategic and International Studies.

Synergy Research Group, 2025. *Hyperscale Spending Spree is Driving Dramatic Growth in Data Center Capacity.* s.l.:Synergy Research Group.

The White House, 2025. *Winning the Race: Amerca's AI Action Plan.* Washington, DC: The White House.

U.S. Congress, 2025. *S.1582 - GENIUS Act.* s.l.:119th Congress.

U.S. Department of Defense, 2024. *Military and Security Developments Involving the People’s Republic of China,* s.l.: U.S. Department of Defense.

U.S. Department of Defense, 2024. *U.S. Department of War.* [Ηλεκτρονικό]
Available at: https://www.war.gov/News/Releases/Release/Article/3703410/department-of-defense-releases-the-presidents-fiscal-year-2025-defense-budget/
[Πρόσβαση 22 December 2025].

U.S. Department of Defense, 2025. *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China,* Washington, D.C.: Department of Defense.

U.S. Department of Defense, 2026. *Artificial Intelligence Strategy for the Department of War.* Washington, DC: Department of Defense.

UNIDO, 2025. *International Yearbook of Industrial Statistics,* Vienna: United Nations Inducstrial Development Organization (UNIDO).

Van Creveld, M., 1989. *Technology and War: From 2000 B.C. to the Present.* New York, London: The Free Press.

Viotti, P. R. & Kauppi, M. V., 2012. *International Relations Theory.* 5th edition επιμ. Longman: Pearson Education.

Walden, J., 2025. *The New Cold War: Rare Earths, AI, and Strategic Competition with China.* s.l.:American Security Project.

Wang, X. J., 2025. How China’s Coming 15th Five-Year Plan Will Reshape Military Innovation. *The Diplomat*, 25 October.

Weiss, C., 2005. Science, technology and international relations. *Technology in Society*, 27(3), pp. 295-313.

WIPO, 2025. *Global Innovation Index 2025: Innovation at Crossroads,* Geneva: World Intellectual Property Organization (WIPO).

Work, B., 2016. *Remarks by Deputy Secretary Work on Third Offset Strategy.* Brussels: U.S. Department of Defense.

World Economic Forum, 2026. *The Global Risks Report 2026,* Geneva: World Economic Forum.

Wu, Y., Lee, J.-s. & Tangonan, K., 2024. U.S. Technological Decoupling from China: A Neoclassical Realist Explanation. *International Area Studies Review,* 27(3), pp. 197-218.

Yan, G., 2020. The impact of Artificial Intelligence on hybrid warfare. *Small Wars & Insurgencies,* 31(4), p. 898–917.

Zacher, L., 2016. Technology and a New International Distribution of Power. Στο: M. Szkarłat & K. Mojska, επιμ. *New Technologies as a Factor of Internmational Relations.* Newcastle upon Tyn: Cambridge Scholars Publishing, p. 50.

Zwitter, A., 2015. Big Data and International Relations. *Ethics & International Affairs,* 29(4), pp. 377-389.