

The U.S and China's Competition for AI Supremacy and its Security Consequences

Mahdi Karimi*- Assistant Professor, Asian Cultural Documentations Center, Institute for Humanities and Cultural Studies, Tehran, Iran.

Received: 21/05/2024

Accepted: 06/10/2024

Abstract

Artificial Intelligence has emerged as a transformative technology with implications for global security. This article using descriptive-analytic method aims to explore the US and China's Competition for AI supremacy and its security consequences for global security. The research main question is that "what ramifications do the US and China's competition for AI supremacy have for global security?" This article argues that the competition between China and the U.S in the realm of AI technologies has significant ramifications for global security, with implications spanning economic, military, and geopolitical spheres. This multifaceted competition casts a profound shadow over the contemporary international landscape and necessitates a nuanced understanding of its consequences. This article also discusses that international collaboration, dialogue, and the establishment of norms and regulations are crucial in harnessing the benefits of AI while mitigating its risks. The final section of this article addresses recommendations to robust AI systems that prioritize human rights. By embracing a responsible approach to AI, we can strive towards a safer and more secure world.

Keywords: Artificial Intelligence; Global Security; the U.S; China.

* E-mail : M.karimi@ihcs.ac.ir

1. Introduction

The rapid advancements in AI have brought about significant transformations in various fields, including global security. Technology and AI impact within the realm of global security is profound (e.g. Mousavi Zare and Others,2017; Dehghani Firoozabadi and Chehrazad,2022; Malek Mohammadi,2014). While some military groups expressed interest in AI during the Cold War, the broader association of AI with international relations and security policy became more apparent following the release of three key AI strategic reports by the U.S. government in 2016. While the widely-acknowledged transformative nature of AI and its extensive applications are predicted to drive economic advancement, AI technologies are increasingly viewed through a security lens, with potential implications for both national and global security concerns. While some articles influenced by neo-realist perspectives focus on the AI's potential to alter systemic power dynamics, the scholarly community has not yet sufficiently addressed the dynamic and evolving nature of this technology. Importantly, the conventional treatment of technology as an external and opaque factor does not provide the field with the necessary analytical framework, particularly considering that global technology companies and research institutions are the entities currently influencing the design and development of AI (Fischer and Wenger,2021).

Both China and the U.S are striving to be leaders in the field of AI technology that is becoming increasingly important in today's world. This competition for dominance in AI technologies is a key aspect of the ongoing rivalry between these two Great Powers. As they continue to invest heavily in research and development, it is clear that both countries see AI as a critical tool for maintaining their position as global leaders. The race to harness the potential of AI is likely to have far-reaching implications for the future of technology and international relations. The U.S and China today compete over the future of AI (Sullivan,2021). Although, the advancement of AI technologies offers promising opportunities, but it poses significant challenges in the domain of global security, regarding the competitive contest of the U.S and China and their zero-sum approach towards AI.

This article aims to explore the multifaceted relationship between AI and global security, emphasizing the transformative potential of AI technologies in enhancing security measures, as well as the intricate implications and ethical considerations of these advancements. After defining AI and its

terminology and exploring challenges and opportunities of IA in global security, the US and China's AI strategies will be reviewed and their competition's impact on global security will be discussed. The final section of this article also will address recommendations to robust AI systems that prioritize human rights. The following section outlines defining AI and its terminology.

2. Research Method

This research is descriptive-analytic in terms of method, and data gathering procedure is based on library findings. Formal documents and regulations issued by the U.S and China's administrations are investigated to answer the following questions: what are the implications of AI on global security? What significant ramifications have had the competition between China and the U.S in the realm of AI technologies for global security? And how this competition can be handled?

3. The literature Review

Several studies focused on how AI enhances surveillance capabilities and improves threat detection. Smith and Others (2019) explores the use of AI algorithms for object recognition, behavior analysis, and anomaly detection in surveillance systems. They emphasize the potential of AI to enhance security measures by identifying suspicious activities, recognizing threats, and automating alert systems. Additionally, Zhang and Yang (2020) discuss how AI-powered facial recognition technology helps in identifying individuals of interest, enhancing border control, and countering terrorism. Some scholars investigated the intersection of AI and cybersecurity and highlight the role of AI in defending against cyber threats. Jones et al. (2021) discusses the use of AI-driven systems for real-time threat detection, malware analysis, and network protection. They emphasize the need for leveraging AI in cybersecurity to stay ahead of rapidly evolving cyber threats. Furthermore, Gunasekaran and Others (2020) explore the use of AI algorithms in predicting and preventing cyberattacks, reducing vulnerability, and enhancing resilience.

The ethical implications of AI in global security constitute another significant area of researches. Scholars such as Floridi and Taddeo (2018) discuss the ethical aspects of AI, including privacy concerns, biases in data, and the need for transparency and accountability. They propose ethical frameworks to guide the development and deployment of AI technologies in

security contexts. Additionally, Zhao and Others. (2022) examine the governance challenges associated with the proliferation of AI in security and argue for the need to establish international norms and regulations to ensure responsible and ethical use of AI.

Some studies explored the use of AI in conflict analysis and risk assessment. Jensen and Others. (2019) investigate how AI techniques, such as machine learning and natural language processing, can analyze large-scale data sources, including news articles and social media feeds, to predict and understand conflict dynamics. They highlight the potential of AI in providing timely and accurate risk assessments, aiding decision-making in conflict prevention and resolution efforts.

The importance of international cooperation and governance frameworks in the context of AI and global security is also a focus of some researches. For example, Kreps (2020) discusses the challenges of AI in security, emphasizing the need for collaboration among states to prevent an AI arms race and ensure responsible use of AI technologies. They argue for the establishment of international agreements and norms to regulate the development and use of AI in security contexts.

Overall, the literature on AI and global security highlights the potential benefits, challenges, and ethical considerations of integrating AI technologies into security domains. The research examines AI in military, surveillance, cyber warfare, peacekeeping and political stability.

4. AI and its Terminology

AI represents a collection of technologies and processes designed to enable machines to simulate human intelligence, encompassing aspects such as learning, reasoning and problem-solving. According to Russell and Norvig (2021), AI refers to "the study of agents that receive percepts from the environment and perform actions." This broad definition underscores the focus on developing intelligent agents capable of perception and action. In other words, AI refers to the development of machines and software capable of performing tasks that typically require human intelligence. It involves the creation of smart algorithms that enable computers to learn from data, recognize patterns, and make decisions. Through machine learning, neural networks, natural language processing, Deep Learning and Reinforcement Learning, AI technologies aim to mimic human cognitive functions and enhance automation, problem-solving, and decision-making capacities,

shaping the foundation for a wide array of applications in industries such as healthcare, finance, and transportation.

Understanding the definitions and terminology within the realm of AI plays a critical role in fostering clarity and precision in discourse. It aids researchers, practitioners, and enthusiasts in effectively communicating key concepts, developments, and challenges within the field. Furthermore, a comprehensive grasp of AI definitions and terminology is vital for addressing ethical considerations, policy frameworks, and the societal impact of these transformative technologies. The study of AI entails a rich tapestry of definitions and terminology that captures the essence of intelligent systems and their components. A clear understanding of these concepts not only illuminates the multi-faceted nature of AI but also provides a foundation for innovation, collaboration, and ethical deployment. These concepts are as follows:

1. Machine Learning

Machine Learning encompasses algorithms and models that enable systems to learn from data to make predictions, recognize patterns, and make decisions without being explicitly programmed. “Machine learning describes the capacity of systems to learn from problem-specific training data to automate the process of analytical model building and solve associated tasks” (Janiesch and Others,2021:685).

2. Neural Networks

Neural networks are a core component of AI, inspired by the structure and function of the human brain. They encompass interconnected nodes configured in layers, allowing systems to learn complex patterns and relationships within data. LeCun and Others, (2015) describe neural networks as machine learning models that are inspired by the way biological neural networks in the human brain process information.

3. Natural Language Processing

Natural Language Processing focuses on enabling machines to understand, interpret, and generate human language in an effective and meaningful way. Jurafsky and Martin (2019) define Natural Language Processing as the ability of a computer program to understand and generate human language as it is spoken and written.

4. Deep Learning

Deep learning, a subfield of Machine Learning, involves training neural networks with large volumes of data to uncover intricate patterns. It has shown exceptional performance in various AI applications. Schmidhuber (2015) defines deep learning as the machine learning technique that learns features directly from the data, often using deep neural networks with many layers.

5. Reinforcement Learning

This technique encompasses training AI agents to make sequential decisions by learning from feedback obtained through interaction with an environment. According to Sutton and Barto (2018), reinforcement learning is a type of machine learning that enables the agent to learn optimal behavior by experimenting and receiving rewards or penalties.

5. Theoretical Framework

The importance of the technological factor is particularly evident in shaping structure of the international system (e.g. Mousavi Zare and Others,2017). Various schools of International Relations have attempted to explain this issue. For example, Hans Morgenthau as a realist stated that the destiny of nations and civilizations has often been determined by a technological gap in warfare that the weaker side could not compensate for in other ways. According to Morgenthau, the emergence of new military technologies, particularly nuclear weapons led to the transformation of the bipolar system, characterized by clearly defined major powers, into a multipolar system with multiple actors empowered by military technologies. Similarly, Waltz, as a (neo)realist, acknowledged the role of technology in shaping the capabilities of states and indirectly influencing the structure of the international system. Additionally, Robert Gilpin, as a (neo)realist, argued that technology, along with differential growth in power among states, was the primary factor responsible for systemic imbalances. In summary, realists view technology as an independent variable that affects the economic and military potential of a state, thereby contributing to systemic changes (Sajduk,2019:160).

Neoliberals, in contrast, hold a more optimistic view regarding the role of technological innovations, particularly information technologies, as a fundamental driver of economic globalization. They consider technology essential for the establishment of new international institutions, including

non-state actors, and as a prerequisite for increasing interdependence (Dehghani Firoozabadi and Chehrazad,2023:16).

Alexander Wendt, representing the constructivist paradigm, views the technological factor as part of structural forces, imposing material constraints on states and shaping their identity. Specifically, the significance of military technologies -offensive or defensive- in international relations stems from the ideas, interests, and roles they generate and support, whether fostering enmity or friendship (Sajduk,2019:161).

In summary, neorealists perceive technology as an independent variable critical for building national power and state capacity. Liberals view technology as a key facilitator of economic growth and a driving force behind interdependence among actors in the international system. Constructivists, on the other hand, interpret technology as a contextual variable that exerts structural pressure on states while also being shaped by social forces.

The current paper will apply neorealist theory to explain implications of AI on global security, the US and China's competition for AI supremacy and its security consequences.

6. Research Findings

6-1.AI and Global Security: Opportunities and Challenges

This section aims to explore the implications of AI on global security, focusing on both the potential benefits and challenges it presents. By examining the applications of AI in military, surveillance, cyber warfare, peacekeeping and political stability we can gain insights into its impact on the global security landscape.

6-1-1.AI in Military

AI technologies have significant implications for military operations, potentially transforming the nature of warfare. One area where AI is being integrated into military systems is autonomous weapons systems. These systems, such as unmanned aerial vehicles (UAVs) and ground robots, can operate without direct human control and make decisions based on AI algorithms (Shook and Others,2020). The benefits of AI in the military are numerous. Autonomous weapons can carry out missions that are too dangerous or impractical for humans, reducing the risk to human lives. They can also provide enhanced surveillance capabilities, gather intelligence, and assist in reconnaissance activities. AI algorithms can process vast amounts

of data quickly, enabling faster decision-making and responses on the battlefield.

However, the use of AI in military contexts raises ethical concerns (Rayhan and Rayhan,2023). One primary concern is the potential for AI algorithms to make life-or-death decisions without direct human intervention. The lack of human judgment and accountability in combat scenarios raises questions about the legality and morality of autonomous weapons. Transparency and explainability of AI systems are also crucial (Feldstein,2019). The lack of transparency in AI algorithms can make it challenging to understand the decision-making process of autonomous weapons. Ensuring that AI systems are auditable and accountable is essential to maintain human oversight and prevent unintended consequences or misuse of AI in military operations. Striking a balance between leveraging AI advancements and ensuring human oversight and accountability is crucial in harnessing the full potential of AI in the military while upholding ethical standards and international norms.

6-1-2.AI in Surveillance and Threat Detection

AI technologies have revolutionized the landscape of surveillance and threat detection on a global scale. Advanced algorithms have enabled the development of smart surveillance systems capable of analyzing vast amounts of data from various sources, such as video feeds, satellite imagery, and social media activity. Such systems can swiftly identify and flag potential security threats, anomalous behavior, and patterns of interest, thereby bolstering the capabilities of security agencies and law enforcement. Smith and Others (2019) underscored the significance of AI-driven video analytics in bolstering surveillance capabilities, offering enhanced real-time threat detection and rapid response mechanisms. Furthermore, advances in behavioral analysis and anomaly detection have enriched the precision and efficiency of threat recognition, emphasizing the indispensable role of AI in augmenting surveillance strategies in the global security landscape.

Today, AI has become a significant aspect of modern surveillance systems, helping to enhance security, improve efficiency, and streamline operations. Feldstein (2019) argues that there are several ways that AI is utilized in surveillance:

- a) Object recognition: AI algorithms can analyze video footage and identify various objects such as people, vehicles, and even specific

objects like backpacks or weapons. This helps in detecting potential threats or suspicious activities in real-time.

- b) Behavior analysis: AI can recognize and understand patterns of human behavior, such as loitering, fighting, or unusual activity. By analyzing patterns over time, the system can identify potential risks and alert security personnel.
- c) Facial recognition: AI-based facial recognition technology can detect, recognize, and match faces in real-time against a database of known individuals. It helps in identifying criminals, locating missing persons, or monitoring and controlling access to restricted areas.
- d) Anomaly detection: AI algorithms can learn what normal behavior looks like in a specific environment and identify anomalies or deviations from the norm. This could include detecting unauthorized access, unusual movement patterns, or abandoned objects.
- e) Automated alert systems: AI-powered surveillance systems can automatically generate alerts or notifications based on predefined rules or thresholds. For example, if someone crosses a virtual boundary or a certain number of people gather in a specific area, an alert can be sent to security personnel for further investigation.
- f) Video analytics: AI can process and analyze large volumes of video data quickly and accurately. It can extract valuable information, such as license plate numbers, facial expressions, or even specific actions like person falling or running. This helps in conducting investigations, collecting evidence, and enhancing situational awareness.

However, it is essential to balance the potential benefits of AI surveillance with privacy concerns (Rayhan & Rayhan, 2023). The use of facial recognition technology and video monitoring raises questions about personal privacy and surveillance ethics (Floridi & Taddeo, 2018). It is crucial to ensure that appropriate safeguards and regulations are in place to protect individuals' rights while utilizing AI in surveillance. Overall, AI in surveillance has the potential to significantly enhance public safety, improve response times, and mitigate risks. Combining the power of AI with robust surveillance systems enables more efficient and effective security operations.

6-1-3.AI and Cyber Warfare

The integration of AI in the context of cyber warfare has significantly transformed the landscape of cyber threats and defensive strategies. AI

technologies, particularly machine learning and deep learning, have become crucial tools in detecting, mitigating, and orchestrating cyber operations. The dynamic and evolving nature of cyber threats has necessitated the adoption of AI in cyber warfare. AI-powered algorithms empower security systems to swiftly detect, analyze, and respond to sophisticated cyberattacks, enhancing the ability to recognize patterns and anomalies within the vast volumes of network data (Baczyk and Others,2019). These patterns could be indicative of cyber intrusions, malware activity, or other security breaches.

AI plays a dual role in cyber warfare. On the offensive front, state and non-state actors utilize AI to develop advanced cyber weapons, automate attacks, and breach secure systems. The use of AI enhances the efficiency and speed of cyber offensives, posing significant challenges to defensive measures (Lewis,2019). Conversely, on the defensive front, AI technologies bolster the resilience of critical infrastructure, networks, and sensitive data repositories by providing real-time threat analysis, automated response mechanisms, and predictive insights.

But, as AI becomes increasingly integrated into cyber warfare strategies, ethical considerations and policy frameworks have come to the forefront. The development and deployment of AI-enabled cyber weapons raise concerns regarding proportionality, accountability, and the potential for autonomous decision-making in cyber operations (Lin and Singer,2014). Moreover, there is a growing need for international cooperation to establish norms that govern the responsible and ethical use of AI in cyber warfare, ensuring that these technologies are employed within the bounds of international law and ethical standards.

6-1-4.AI and Peacekeeping Efforts

AI has the potential to significantly impact peacekeeping efforts by enhancing situational awareness, improving decision-making capabilities, and enabling more efficient resource allocation. Here are some key areas where AI can contribute to peacekeeping:

- a) **Information and Intelligence Analysis:** AI can help peacekeeping missions analyze vast amounts of data and extract actionable intelligence. By processing information gathered from various sources, such as social media, news articles, and sensor networks, AI algorithms can identify patterns, trends, and potential threats (Smith and Others,2019). This information can aid in understanding the dynamics

of the conflict, identifying key stakeholders, and making informed decisions.

- b) **Early Warning Systems:** AI algorithms can monitor and analyze data in real-time to detect early warning signs of potential conflicts, violence, or human rights abuses. By identifying patterns and indicators, AI can provide timely alerts to peacekeeping forces, enabling proactive intervention and prevention strategies. Early warning systems can help save lives, mitigate the escalation of conflicts, and promote stability.
- c) **Predictive Analytics:** AI can leverage historical data, demographic information, and socio-economic factors to make predictions about the likelihood of conflict or violence in certain regions (Lazaro and Rizzi, 2023). Predictive analytics can assist peacekeeping missions in resource planning, prepositioning forces, and allocating resources where they are most needed. This enables more efficient utilization of limited resources and enhances the overall effectiveness of peacekeeping operations.
- d) **Decision Support Systems:** AI can assist peacekeeping commanders and decision-makers by providing data-driven insights and recommendations. AI-powered decision support systems can process information, generate scenarios, and simulate the potential outcomes of different actions (Jensen and Others, 2019). This helps in making informed decisions regarding troop deployment, resource allocation, and operational strategies.
- e) **Remote Sensing and Image Analysis:** AI can analyze satellite imagery, aerial photographs, and other remote sensing data to monitor and analyze conflict zones (Rothe and Shim, 2018). It can help identify movements of troops, changes in infrastructure, or damage assessment. AI-powered image analysis can provide valuable information for situational awareness, verification of compliance with peace agreements, and planning of response actions.
- f) **Communication and Translation:** Language barriers often pose challenges in peacekeeping missions. AI-powered language translation tools can assist peacekeepers in communicating with local populations, gathering information, and promoting dialogue. Real-time translation systems can facilitate better understanding and cooperation between peacekeepers and local communities, contributing to effective engagement and conflict resolution.

It is crucial to note that AI should augment and support human decision-making rather than replace it. Humans still possess the contextual understanding and moral reasoning necessary to navigate complex conflicts. Therefore, the responsible and ethical use of AI in peacekeeping operations is of utmost importance, ensuring transparency, accountability, and respect for human rights. Overall, AI has the potential to revolutionize peacekeeping efforts by providing valuable insights, improving situational awareness, and enhancing decision-making processes. Utilizing AI technologies effectively can contribute to more effective and efficient peacekeeping operations, ultimately promoting stability and peace in conflict-affected regions.

6-1-5.AI, Future of Work and Social and Political Instabilities

AI continues to transform the landscape of work, presenting myriad opportunities and challenges that influence the social and political fabric of society. As AI technologies become increasingly integrated into various industries, their impact on employment, social structures, and political dynamics is becoming more pronounced.

AI's potential to automate routine tasks and augment human capabilities is reshaping the nature of employment. According to Brynjolfsson and McAfee (2014), AI technologies have the capacity to optimize production processes, streamline operational tasks, and enhance productivity, contributing to the creation of new job categories while also reshaping existing roles. As AI increasingly augments human labor, it necessitates a shift in workforce skills, emphasizing the demand for advanced technical competencies, problem-solving abilities, and adaptability (Arntz and Others, 2016).

The widespread adoption of AI in the workplace has spurred debates concerning its impact on societal disparities, income inequality, and political stability. The possibility of job displacement due to automation has prompted discussions on social and economic inequalities, as individuals in certain job sectors face greater risks of unemployment or underemployment (Ford, 2015). The ramifications of such shifts reach beyond individual livelihoods, influencing broader sociopolitical structures and welfare systems.

AI's impact on political stability is multifaceted, intertwining with issues of social equity, labor policy, and economic conditions. It prompts discussions on the future of social safety nets, workforce retraining initiatives, and

government policies aimed at addressing potential job displacement and inequality. These discussions are integral to ensuring that the benefits of AI are distributed equitably and that the potential disruptions align with broader societal goals and values (Manyika and Others,2017).

Ensuring ethical AI integration amid these shifts is essential. The responsible development and deployment of AI systems require robust regulatory frameworks, ethical standards, and inclusive decision-making processes. The impact of AI on work, social structures, and political dynamics underscores the importance of proactive engagement by policymakers, industry leaders, and civil society to safeguard against potential inequalities and instabilities resulting from AI-driven changes in the workplace (Stiglitz,2018).

6-2.The US and China's AI Strategies

Addressing the challenges of the US and China's AI strategies requires a review of both countries' approaches to AI strategies. The following section will outline the US and China's AI strategies.

6-2-1.The US AI Strategy

The U.S has recognized the inextricable link between AI, national security, and defense, leading to the formulation of a strategic framework that aims to harness the potential of AI while addressing its associated challenges. This strategy encompasses targeted investments, ethical guidelines, and regulatory mechanisms to fortify the U.S AI capabilities. This section explores the significance of AI for U.S. national security and defense, delve into the existing regulations and guidelines governing AI, and analyze the ongoing strategic focus on leveraging AI for military and security purposes.

Importance of AI for U.S. National Security and Defense can be discussed in following areas: a) enhancing military capabilities: AI has emerged as a critical force multiplier, augmenting the capabilities of the U.S. military across various domains, including intelligence, surveillance, and reconnaissance (ISR), autonomous systems, and information warfare. The U.S. Department of Defense (DoD) has been actively leveraging AI to be able to strengthen its command and control systems, optimize logistical operations, and bolster its cyber defense capabilities (Bowen,2021); b) innovation and technological superiority: AI is pivotal for maintaining the U.S. technological edge and innovation leadership in the global security arena. Investments in cutting-edge AI technologies are seen as crucial for

ensuring that the U.S. military remains at the forefront of technological developments, positioning the country as a leader in critical defense applications, such as autonomous vehicles, swarming drones, and predictive maintenance for advanced weapon systems (National Security Commission on Artificial Intelligence,2021); c) cybersecurity and threat mitigation: AI plays a fundamental role in fortifying the U.S. cybersecurity measures. By analyzing vast datasets and network traffic patterns, AI enables the timely detection and response to cyber threats, thereby bolstering the resilience of critical infrastructure, government systems, and defense networks. AI-driven cybersecurity solutions have become indispensable in combatting sophisticated cyber adversaries (National Institute of Standards and Technology,2020).

The U.S. government unveiled the National Strategy for AI in 2019, outlining a cohesive plan to propel American leadership in AI, emphasizing strategic investments, technological innovation, and AI-driven national security advancements. The strategy positions AI as a critical component of U.S. economic competitiveness, addressing societal challenges, and enhancing defense and security capabilities (The White House,2019). Also, the U.S. DoD has emphasized its commitment to AI-driven defense innovation through initiatives such as the Joint Artificial Intelligence Center (JAIC) and the Defense Innovation Unit (DIU). These entities focus on fostering collaboration with the private sector, facilitating the rapid adoption of emerging AI technologies, and ensuring their seamless integration into military operations while adhering to ethical and legal imperatives (The U.S. Department of Defense,2021).

The U.S. has been proactive in advocating for the ethical and responsible use of AI. This has culminated in the development of guidelines and ethical frameworks to steer the development and deployment of AI technologies. Government agencies, including the DoD and the National Security Commission on Artificial Intelligence, have advocated for transparent and accountable AI systems to navigate potential ethical and security challenges (National Security Commission on Artificial Intelligence,2021).

Regulations concerning AI encompass export control mechanisms aimed at preventing sensitive AI technologies from falling into the wrong hands. Efforts to collaborate with like-minded nations have sought to establish international norms and standards for the ethical and responsible use of AI in strategic and security domains. These measures are aimed at preventing

the misuse of AI for malicious purposes and enhancing global security cooperation (The U.S. Department of Commerce,2020).

In sum, the U.S. AI strategy underscores the critical importance of AI for national security and defense, emphasizing its role in enhancing military capabilities, fortifying cybersecurity, and maintaining innovation leadership. Alongside these efforts, the U.S. has enacted regulatory mechanisms to ensure the responsible and ethical integration of AI, prevent unauthorized proliferation, and foster international collaboration on AI norms and guidelines. The ongoing commitment to AI-driven strategic initiatives and regulatory frameworks reflects the U.S dedication to leveraging AI for national security and defense while adhering to ethical and legal imperatives.

6-2-2.China's AI Strategy

In July 2017, China's State Council released the New Generation Artificial Intelligence Development Plan (AIDP), which, along with Made in China 2025, forms the cornerstone of China's AI strategy. Both documents, as well as the broader issue of AI, have garnered sustained attention from China's highest authorities, including Xi Jinping. In October 2018, Xi Jinping personally led a Politburo study session specifically focused on AI. During this session, Xi emphasized China's need to lead in theoretical research and possess core AI technologies, placing the country at the forefront. He stressed the importance of addressing China's deficiencies and ensuring a firm grasp on critical AI technologies. Xi's statements affirm China's commitment to the key tenets outlined in the AIDP and Made in China 2025, advocating for global leadership and self-reliance in AI technology (Allen,2019:3-4).

The AI industry in China possibly has fewer barriers to commercial and military cooperation. The Chinese military's advancement in AI is substantially influenced by its observation of the U.S. defense innovation plans and concerns about a potential "generational gap" compared to the U.S. military. A primary focus of Chinese AI development is to bolster battlefield decision-making through the strategic utilization of AI. Similar to the U.S. military objectives, China aims to harness AI for processing large volumes of intelligence data to gain a comprehensive understanding of the battlefield and to offer actionable recommendations to military decision-makers (Hoadley and Lucas,2018).

Additionally, China is actively researching various types of autonomous vehicles for air, land, sea, and submersible operations. Notably, a Chinese university with affiliations to the military showcased an AI-powered swarm of 1,000 unmanned aerial vehicles (UAVs) at an airshow in 2017. Subsequently, a media report unveiled a computer simulation demonstrating a comparable swarm effectively identifying and neutralizing a missile launcher. Publicly available sources also indicate that China is developing a suite of AI tools for cyber-defense and offensive cyber operations. The remarkable similarities between the U.S. and Chinese AI development have raised concerns among some leaders in the DoD about the potential for achieving a distinct and enduring advantage on the battlefield, as envisioned in current defense innovation guidelines (Hoadley and Lucas,2018).

Despite China's formidable strength in AI research and commercial applications, its leadership perceives substantial weaknesses relative to the U.S in top talent, technical standards, software platforms, and semiconductor technologies. While most within China's leadership concur that China is one of the two global "giants" in AI, there is widespread recognition that China is not equally strong across all domains. China's "White Paper on Artificial Intelligence Standardization" released in January 2018 underscores that China's AI ecosystem lags in several critical domains:

Although China has a good foundation in the field of AI, even as core technologies such as speech recognition, visual recognition, and Chinese language information processing have achieved breakthroughs and possessed huge market environments for applications, the overall level of development still lags behind that of developed countries (Allen,2019:10).

But, as Allen (2019) interviews with China's officials show, China's notable success in the commercial AI and semiconductor markets directly impacts the country's geopolitical power, as well as its military and espionage AI capabilities. The flourishing commercial market in China holds strategic importance for the nation's national security, primarily by reducing the capacity of the U.S government to exert diplomatic and economic pressure on China. Furthermore, this success augments the technological prowess accessible to China's military and intelligence community. Notably, practically all major technology firms in China extensively collaborate with the country's military and state security services, in many cases under legal obligation to do so.

6-3.The U.S and China's Competition in the Realm of AI

The competition between the US and China as two giant AI powers has significant ramifications for global security (Saniabadi,2019). This multifaceted competition casts a profound shadow over the contemporary international landscape and necessitates a nuanced understanding of its consequences. Competition between the US and China for AI Supremacy can be investigated in following areas:

a) Technological innovation and economic significance: the escalating competition between China and the U.S for AI supremacy underscores the pivotal role of cutting-edge technologies in shaping economic and strategic ascendancy. "Internet + Production" seeks to use Internet of Things and big data to enable the real economy to drive development in the digital economy and accelerate intelligent manufacturing adaptation. Both countries have made substantial investments in AI research and development, competing for technological breakthroughs, patents, and commercial applications. Especially, by proposing the idea of economic decoupling from China in 2020, the importance of AI-based technologies to foster economic and strategic ascendancy has become clearer for the U.S. AI has brought undeniable economic benefits but the competition with China extends beyond just increasing GDP. It is also about the spread of Chinese values norms and standards for using AI worldwide. This competition is not just about who has the most advanced technology but also about who can influence how AI is used and perceived on a global scale (Sullivan,2021);

b) military and defense applications: the competition extends to military and defense arenas, where AI technologies are becoming increasingly intertwined with national security strategies. Both countries strive to leverage AI for intelligence gathering, surveillance, cyber defense, autonomous weapons systems, and information warfare, iterating technological developments to attain military dominance and strategic advantage (Council on Foreign Relations,2021); For example, at the Beijing Xiangshan Forum on October 24, 2018, Major General Ding Xiangrong, Deputy Director of the General Office of China's Central Military Commission, gave a major speech in which he defined China's military goals to "narrow the gap between the Chinese military and global advanced powers" by taking advantage of the "ongoing military revolution ... centered on information technology and intelligent technology" (Allen,2019:5);

c) geopolitical implications: the intensifying competition between China and the U.S for AI leadership is inseparable from broader geopolitical dynamics. The repercussions of this rivalry are felt across international relations, shaping alliances, trade relations, and global security paradigms (Singer,2018). Forming partnerships with “like-minded” nations based on democratic values is simple, but maintaining these alliances in the face of China’s pressure is a real challenge. Sun Tzu's quote "Victory can be anticipated, but it cannot be forced" highlights this. As alliances expand geographically, conflicting interests and values may arise, pushing leaders to compromise and focus on common goals. A single alliance will not cover all aspects of competition with China, as different countries have different concerns. A values-based alliance can help counter China's economic coercion and illiberal practices. However, excluding China from organizations like the “Clean Network” could deter nations seeking competition without conflict but still desiring a relationship with China. The shift towards AI multipolarity and an open structure presents opportunities for the U. S. if it can rally its allies towards a common strategy. Middle powers like European and Asian allies as well as traditionally nonaligned powers such as India and Vietnam will play a crucial role in determining power balances. Competition in economic technological and political realms will be a key with China preferring partnerships over formal alliances. The world's geopolitical landscape is unlikely to support blocs along neat ideological lines making case-by-case coalitions more diplomatically challenging. Bilateral and multilateral engagements will shape AI competition and may lead to changes in the international structure to accommodate the rise of middle powers (Sullivan,2021).

The increasing prominence of AI will reshape the global landscape, leading to the emergence of two distinct blocs of nations. The first bloc will be centered around the United States and its allies, who will adhere to Western values and incorporate advanced technologies. The second bloc will be led by China and will embrace its political model and technological solutions. The remaining countries of the world will be subjected to constant pressure from both blocs. Nations that successfully implement AI will witness substantial economic growth, but the disparity between developed and developing countries will amplify at an unprecedented rate (Sajduk,2019: 175).

The escalating competition between China and the U.S in the arena of AI technologies has engendered concerns regarding technological proliferation and the potential for an arms race in AI-powered military systems. The quest for dominance in AI technologies has the potential to fuel a spiral of competition, necessitating vigilance in arms control and regulatory mechanisms (Weiss,2021). The competition poses critical challenges for international norms and governance in the domain of AI. As China and the U.S seek to assert their technological leadership, the development and deployment of AI technologies are increasingly intertwined with questions of standards, ethical considerations, and normative frameworks governing AI's role in global security and stability (Lee,2020).

7. Discussion

AI's impact on global security is undeniable, with both positive and negative implications. While AI has the potential to revolutionize military capabilities, strengthen cybersecurity, and improve surveillance and peacemaking, also the integration of AI into global security poses several challenges that need careful consideration. Here are some key challenges: a) bias and discrimination: AI algorithms are trained on existing data, and if this data contains biases or discriminatory patterns, it can lead to biased outcomes. In the context of global security, biased AI systems could result in unfair treatment or profiling of certain individuals or groups. It is crucial to ensure that AI systems are trained on diverse and representative data sets, and regular audits are conducted to identify and address biases; B) privacy concerns: AI-based surveillance systems, including facial recognition technology, raise concerns about individuals' privacy rights. The collection, storage, and analysis of vast amounts of personal data can potentially infringe on privacy rights if not properly regulated. It is important to establish clear guidelines and regulations on data collection, retention, and usage to strike a balance between security needs and individual privacy; c) cybersecurity risks: AI systems are vulnerable to cyberattacks, and exploiting these vulnerabilities could have severe consequences for global security. Malicious actors could manipulate AI algorithms, gain unauthorized access to surveillance systems, or use AI to spread disinformation or launch cyber-attacks. Protecting AI systems against cyber threats necessitates robust security measures, regular updates, and adherence to industry best practices; d) ethical implications: The use of AI in global security raises ethical questions regarding the proportionality and necessity

of surveillance measures. Striking the right balance between national security interests and individual rights is critical. Decision-making algorithms used in autonomous weapons systems also raise ethical concerns, as they could carry out actions with potentially dire consequences without human oversight. Establishing ethical frameworks and guidelines for the development and deployment of AI in security is crucial; e) policy and regulation: the rapid advancement of AI technology poses challenges for policy and regulation to keep pace. International cooperation is required to formulate policies and regulations that address the global implications of AI in security.

The competition between the US and China as two giant AI powers bold the importance of these challenges. This competition has significant ramifications for global security, with implications spanning economic, military, and geopolitical spheres. This multifaceted competition casts a profound shadow over the contemporary international landscape and necessitates a nuanced understanding of its consequences. As this rivalry extends influence across economic, military, and geopolitical realms, it necessitates careful deliberation, international cooperation, and strategic foresight to navigate the potential impact of AI in shaping a more secure and stable global order.

8. Some Policy Recommendations

Addressing the challenges of AI development for global security requires a multifaceted approach encompassing ethical, regulatory, and collaborative initiatives. Here are some policy recommendations to navigate the complexities and ensure responsible integration of AI in the context of global security.

- Developing ethical guidelines for AI in global security is crucial. Policies must focus on transparency, accountability, and ethical use to prevent misuse and protect against harm. Collaboration among governments, organizations, and tech leaders is essential to create universal standards.
- Developing regulatory standards and norms specific to AI in global security is essential to ensure compliance with ethical principles and mitigate risks. Policymakers and governing bodies should strive to create clear regulations addressing AI in surveillance, cyber defense, military applications, and international cooperation. This includes defining legal boundaries, data privacy and protection, prohibitions on

autonomous lethal weapons, and guidelines for the use of AI in peacekeeping and conflict resolution.

- International collaboration and information sharing are vital for understanding AI's global security impact. Governments and organizations should promote dialogue and knowledge exchange to enhance preparedness in handling AI-related security challenges through collaborative platforms and joint initiatives.
- Investing in capacity building and training programs geared towards AI in global security is essential. Governments and international bodies should allocate resources for specialized education, training, and skill development in AI for security professionals, policymakers, and decision-makers.
- Strategic risk assessments for AI are crucial for policymakers to anticipate security threats. Evaluations help understand real-world implications, guiding policy adaptations to address emerging challenges and opportunities in AI integration.
- Promoting transparency and engagement in AI for global security is essential. Public awareness, access to information, and mechanisms to address concerns should be prioritized. Open discussions and citizen involvement can improve trust and accountability in AI governance.
- Governments and international organizations must collaborate with AI industry and research communities to align AI development with security priorities.

9. Conclusions

The intersection of AI and global security presents a fascinating, albeit complex, landscape. As AI technologies continue to advance, they are increasingly integrated into various aspects of military and security operations, raising critical questions about the implications for global stability. Furthermore, the dynamics of competition and collaboration between the US and China in this domain significantly shape the future trajectory of global security.

It is essential to recognize that AI has the potential to revolutionize warfare and defense. From autonomous weapon systems to cyber operations and surveillance, AI technologies offer capabilities that can enhance military effectiveness and strategic decision-making. While these advancements hold promise for improving security, they also bring forth unique challenges,

such as the ethical use of AI in military applications and the potential for arms races driven by AI-powered capabilities.

The US and China stand at the forefront of AI development and application, positioning themselves as key players in the evolving landscape of global security. Both countries have invested substantially in AI research and development, leveraging these technologies to bolster their military capabilities and national security infrastructure. This competition extends beyond conventional military domains and encompasses cyber warfare, information operations, and the race for AI dominance in critical sectors such as quantum computing and strategic autonomy.

The implications of this competition are far-reaching. The pursuit of AI superiority has the potential to fundamentally reshape the geopolitical landscape, impacting alliances, defense strategies, and the ethical frameworks underpinning global security. One significant concern is the risk of an escalating AI arms race, as nations seek to outpace each other in weaponizing AI technologies, which could heighten the potential for miscalculation and unintended conflict.

In navigating this landscape, it becomes crucial for nations to engage in transparent dialogue and establish norms and regulations governing the responsible use of AI in security contexts. International cooperation, diplomacy, and multilateral agreements are essential for managing the risks associated with the proliferation of AI in global security and mitigating the potential for destabilizing effects.

In conclusion, the evolving interplay between AI, global security, and the competition between the US and China yields a complex landscape with profound implications for international relations and strategic stability. Navigating this terrain necessitates a balanced approach that acknowledges the transformative potential of AI while proactively addressing the associated challenges through collaboration, dialogue, and ethical frameworks.

10. Acknowledgement

The author would like to express his appreciation to the Research Deputy of the Institute for Humanities and Cultural Studies for providing the possibility of doing this research.

References

1. Allen, G.C. (2019). Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security.
2. Arntz, M; Gregory, T; Zierahn, U. (2016). The risk of automation for jobs in OECD countries: A comparative analysis. OECD Social, Employment and Migration Working Papers, No. 189. Paris: OECD Publishing.
3. Baczyk, M and Others. (2019). Artificial intelligence and machine learning in cybersecurity. In 2019 International Interdisciplinary PhD Workshop (IIPhDW). IEEE.
4. Bowen, J. (2021). Artificial intelligence in national defense: Comparisons of strategic plans in the U.S. and China. *Journal of Strategic Security*, 14(1), 1-23.
5. Brynjolfsson, E; McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. New York, NY: W. W. Norton & Company.
6. Christopher Cullen, Sam Tyner-Monroe; Samp, Tony; Borden, Bennett; Tobey, Danny; Darling, Coran. (2023). *The US National AI R&D Strategic Plan 2023: A comprehensive look into the future of AI*. Retrieved from <https://www.dlapiper.com/en/insights/publications/ai-outlook/2023/the-us-national-ai-rd-strategic-plan-2023>.
7. Council on Foreign Relations. (2021). *Artificial Intelligence*. Council on Foreign Relations.
8. Dehghani Firoozabadi, S.J; Chehrazad, S. (2022). Geopolitics of artificial intelligence; Theoretical roadmap for algorithmic competitions of world actors. *Geopolitics Quarterly*, Vol. 0, No.0. **[In Persian]**
9. Dehghani Firoozabadi, S.J; Chehrazad, S. (2023). Revising International Relations Theories in the Era of Artificial Intelligence (AI). *Strategic Studies Quarterly*, 26(100), 83-107. **[In Persian]**
10. Feldstein, S. (2019). *The global expansion of AI surveillance (Vol. 17)*. Washington, DC: Carnegie Endowment for International Peace.
11. Fischer, S.C; Wenger, A. (2021). Artificial intelligence, forward-looking governance and the future of security. *Swiss Political Science Review*, 27(1), 170-179.
12. Floridi, L; Taddeo, M. (2018). What is data ethics? *Philosophical Transactions of the Royal Society A*, 376(2128), 20180081.
13. Ford, M. (2015). *Rise of the robots: Technology and the threat of mass unemployment*. New York, NY: Basic Books.
14. Gunasekaran, M; Madanian, S; Awajan, A; Rahman, M; Shuaib, K. (2020). Artificial intelligence in cybersecurity: A review. *Computers & Security*, 88, 101639.
15. Hoadley, D.S; Lucas, N.J. (2018). *Artificial intelligence and national security*. Congressional Research Service.
16. Janiesch, C; Zschech, P; Heinrich, K. (2021). *Machine learning and deep*

- learning. *Electronic Markets*, 31(3), 685-695.
17. Jensen, O.D; Heinrich, F; Jegstad, J. (2019). Social media analytics and conflict prediction: Challenges and limitations. *International Studies Review*, 21(3), 390-409.
 18. Jones, R; Bavisi, A; Iyengar, S.S; Ahmed, A. (2021). A survey on machine learning techniques for cybersecurity. *Journal of Cybersecurity and Privacy*, 2(2), 120-142.
 19. Jurafsky, D; Martin, J.H. (2019). *Speech and language processing* (3rd ed.). Pearson.
 20. Kreps, S.E. (2020). The next phase in the AI arms race. *Survival*, 62(5), 79-104.
 21. Lazaro, C; Rizzi, M. (2023). Predictive analytics and governance: a new sociotechnical imaginary for uncertain futures. *International Journal of Law in Context*, 19(1), 70-90.
 22. LeCun, Y; Bengio, Y; Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444.
 23. Lee, C. (2020). The global competition in artificial intelligence. Center for Security and Emerging Technology.
 24. Lewis, J.A. (2019). The cyber weapons of mass disruption. *Survival*, 61(1), 7-28.
 25. Lin, H; Singer, P.W. (2014). *Cybersecurity and cyberwar: What everyone needs to know?* Oxford University Press.
 26. Mousavi Zare, S.J; Zarghani, S.H; Azami, H. (2017). Analysis of the position of science and technology in the realm of hard, soft and smart power. *Geopolitics Quarterly*, 13(47), 103-138. **[In Persian]**
 27. Manyika, J; Lund, S; Chui, M; Bughin, J; Woetzel, J; Batra, P; Ko, R; Sanghvi, S. (2017). *Jobs lost, jobs gained: Workforce transitions in a time of automation.* McKinsey Global Institute.
 28. Malek Mohammadi, H. (2014). Techno-Geopolitics; a pro classical geopolitics challenging critical approach. *Geopolitics Quarterly*, 10(36), 109-121.
 29. National Institute of Standards and Technology. (2020). *AI Standards for Federal Agencies.* Retrieved from <https://www.nist.gov/itl/applied-cybersecurity/ai-standards-federal-agencies>.
 30. National Security Commission on Artificial Intelligence. (2021). *Final Report.* Retrieved from <https://www.nsc.ai.gov/final-report>.
 31. Rayhan, A; Rayhan, S. (2023). *AI and Global Security: Navigating the Risks and Opportunities.*
 32. Rothe, D; Shim, D. (2018). Sensing the ground: On the global politics of satellite-based activism. *Review of International Studies*, 44(3), 414-437.
 33. Russell, S; Norvig, P. (2021). *Artificial intelligence: A Modern Approach.* Pearson.
 34. Sajduk, B. (2019). Theoretical premises of the impact of artificial intelligence on the international relations and security. *The Copernicus Journal of Political Studies*, (2), 157-180.
 35. Saniabadi, E.R. (2019). Comparative analysis of US 2017 national security

- strategy document towards China and Iran. *Geopolitics Quarterly*, 14(4), 188-208.
36. Schmidhuber, J. (2015). Deep learning in neural networks: An overview. *Neural Networks*, 61, 85-117.
 37. Shook, J.R; Solymosi, T; Giordano, J. (2020). Ethical constraints and contexts of artificial intelligent systems in national security, intelligence, and defense/military operations. In *Artificial Intelligence and Global Security: Future Trends, Threats and Considerations* (pp. 137-152). Emerald Publishing Limited.
 38. Singer, P. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt.
 39. Smith, N; Li, Y; Alajaji, I. (2019). Deep learning for video surveillance: A review. *Neurocomputing*, 335, 12-24.
 40. Stiglitz, J.E. (2018). *Towards a progressive capitalism: U.S. foreign policy, international institutions, and global social democracy*. Geneva: United Nations Research Institute for Social Development.
 41. Sullivan, R. (2021). *The US, China, and artificial intelligence competition factors*. China Aerospace Studies Institute.
 42. Sutton, R.S; Barto, A.G. (2018). *Reinforcement learning: An introduction*. MIT press.
 43. The White House. (2019). Executive Order on Maintaining American Leadership in Artificial Intelligence. Retrieved from <https://www.whitehouse.gov/presidential-actions/>.
 44. U.S. Department of Commerce. (2020). Update on Export Control Reform Initiative. Retrieved from <https://www.commerce.gov/>.
 45. U.S. Department of Defense. (2021). Ethics Principles for Artificial Intelligence. Retrieved from <https://www.ai.gov/ethics-principles-artificial-intelligence>.
 46. Weiss, M. (2021). *Artificial intelligence, global security, and strategic stability*. Joint Special Operations University.
 47. Zhao, Q; Zhang, Y; Gyampah, K.K; Bélanger, F. (2022). Artificial intelligence in information security: A systematic review and research agenda. *Information & Management*, 59(1), 103439.

COPYRIGHTS

©2023 by the authors. Published by the Iranian Association of Geopolitics. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY 4.0) <https://creativecommons.org/licenses/by/4.0>

