

## THE TECH RACE AND SECURITY DILEMMAS: U.S.-CHINA RIVALRY IN AI AND CYBERSECURITY WITH TÜRKİYE'S PERSPECTIVE

Dr. Birol AKDUMAN<sup>1</sup>

### ABSTRACT

The escalating technological competition between the United States and China signifies a pivotal transformation in the distribution of global power, touching upon economic systems, military strategies, and political frameworks. This analysis investigates the fundamental aspects of this rivalry, focusing on artificial intelligence (AI), semiconductor technologies, and cybersecurity—domains that represent critical battlegrounds for 21st-century dominance. These emerging technologies, essential to both national security and economic resilience, have intensified the contest between these two superpowers while simultaneously influencing the strategic approaches of middle powers operating within this evolving geopolitical context.

Central to this study is an exploration of how advancements in AI and semiconductors are redefining defense capabilities, enhancing industrial automation, and fostering global connectivity. By analyzing the strategic initiatives led by the U.S. and China, the study highlights the lengths both nations are going to in their pursuit of technological supremacy. Cybersecurity, in turn, emerges as an area of mounting tension, with AI-powered cyberattacks presenting significant threats to global critical infrastructure. The absence of strong international regulatory mechanisms exacerbates these challenges, contributing to an unpredictable and fragmented global environment where errors and misjudgments can lead to conflict.

Additionally, the research evaluates Türkiye's distinct position as both a NATO member and a participant in China's Belt and Road Initiative (BRI), providing a comprehensive examination of the challenges and opportunities arising from this competition. Türkiye's technological advancements, particularly in defense systems like UAVs and semiconductor development, coupled with its strategic geographic location, place it in a unique position to benefit from this rivalry. Nonetheless, the nation faces notable vulnerabilities, such as dependence on foreign technology, exposure to cybersecurity risks, and the delicate task of balancing relations with these competing global powers.

---

<sup>1</sup> Yasar University, İzmir, TÜRKİYE, ORCID: 0000-0003-4049-0449, e-mail: birol.akduman@yasar.edu.tr

By adopting a multidisciplinary perspective, the study offers actionable strategies for middle powers like Türkiye to exploit technological opportunities while reducing associated risks. Encouraging domestic technological development, engaging in multilateral platforms, and aligning policies with global trends are identified as critical steps. These measures not only safeguard national interests but also position Türkiye as an influential actor in navigating the complexities of this rivalry. Ultimately, the findings underscore the pressing need for international cooperation to create comprehensive frameworks that regulate emerging technologies and maintain equilibrium between competition and collaboration in shaping a stable global future.

**Keywords:** Technological Rivalry, National Security, U.S.-China Competition, Artificial Intelligence (AI), Cybersecurity.

## INTRODUCTION

As technological advancement determines who holds power, the United States – China rivalry has become one of the key conflicts in world politics. This competition is not limited only to military arms but also includes AI, cyber security, and semiconductors which are becoming critical for not just economic development but more importantly national defense. The stakes are unprecedented because technological power has directly begun to determine military, economic, and political power.

The area of even national security is undergoing drastic change because of the rapid proliferation of newer technologies. AI which was otherwise relegated to the academic domain has become an integral part of war-fighting, intelligence-gathering, and decision-making processes. Likewise, the increasing amounts of conflict occurring in cyberspace have introduced new vulnerabilities as critical infrastructure, sensitive information and even society as a whole is exposed to a sort of conflict of the new age. These areas are strategic spaces for the US and China; however, they are also spaces for competition that could shape the center of power of the 21st century.

The study observes a spot of overlap in the tech war/coastguard continuum: Emerging AI, semiconductors and cybersecurity take over as critical national security domains between Rivalry 1.0 [U.S.-China] to go faithfully, quasi-existentially beyond global balances-of-power; technology rivalry in innovative alliances and unilateral ends for power—by far defunct military hegemonies undone and undocked! Starting with an analysis of the historical development of strategic thinking showing movement from conventional military power to technological supremacy. The piece subsequently goes through the specifics of U.S.-China rivalry in terms of global governance, economic interdependence and military strategy. Policy recommendations are then provided, which seek to reduce risks and promote cooperation in this vital area.

Turkey on the other hand, is geopolitically located at the heart of this global competition and has modern defense technology capabilities as a Rising Middle Power. Its relatively developed UAV technology, burgeoning semiconductor production interest and participation in NATO alongside China's Belt-and-Road Initiative region have highlighted what for many countries amounts to a scramble between two technological superpowers. Türkiye has the potential to use this competition for its own national interests, while only risking much if it can balance the China-America relations.

As we continue to navigate the dynamics of this competition, it is incumbent upon policymakers, scholars and global citizens alike to understand how technology and security interact. This study sheds light on the strategic importance of this tech race for global dynamics and adds to our understanding by expanding cross-disciplinary discussion about how emerging technologies are influencing future trends in IR (International Relations) & national security.

### **METHODOLOGY AND THEORETICAL FRAMEWORK**

This research adopts a multidimensional approach to explore the intricate dynamics of the U.S.-China technological rivalry and its broader implications for middle powers like Türkiye. The methodology integrates both qualitative and quantitative analyses to provide a comprehensive understanding of the geopolitical, economic, and security dimensions of this competition. By leveraging systematic reviews of primary and secondary sources, comparative policy analyses, and geopolitical visualization tools, the study ensures a robust and nuanced examination of its central themes.

Primary data sources for this research include governmental publications, strategic policy documents, and official reports from stakeholders in the U.S. and China. These are complemented by secondary sources, such as peer-reviewed journal articles, monographs, and expert commentaries, which offer broader contextual insights into sectors like artificial intelligence, semiconductors, and cybersecurity. Triangulating these data sources enhances the credibility and reliability of the findings.

The theoretical framework guiding this study integrates perspectives from realism, liberalism, and constructivism to analyze how technological advancements shape global power structures. Realism emphasizes the competitive dynamics between the U.S. and China, highlighting issues such as power shifts and security dilemmas. Liberalism contributes insights into potential avenues for cooperation fostered by global technological interdependence. Constructivism adds a layer of analysis by exploring the role of narratives, norms, and identities in shaping national strategies and global technological ambitions. Together, these theoretical lenses offer a balanced approach to understanding both the material and ideational aspects of the rivalry.

Advanced analytical tools are employed to deepen the research. Geographic information systems (GIS) are utilized to map the spatial dimensions of technological investments, trade routes, and international alliances. Data analysis platforms facilitate the examination of large datasets related to semiconductor manufacturing trends, cybersecurity incidents, and AI patent activity. This combination of tools enables the identification of critical patterns and developments within the broader geopolitical context.

The comparative case study method is a cornerstone of the research. Key initiatives such as China's "Made in China 2025" and the U.S.'s "CHIPS Act" are closely examined to uncover their strategic divergences and global ramifications. By juxtaposing these initiatives, the study highlights their influence on middle powers like Türkiye and their broader impact on international technological competition.

Ethical considerations form an integral part of the research design. Data sources are carefully vetted for accuracy and transparency, ensuring adherence to the highest academic standards. Sensitive geopolitical and economic data are analyzed with caution to maintain objectivity and avoid speculative conclusions. The study's findings are grounded in empirical evidence, validated by rigorous theoretical models, and framed within an ethical research paradigm.

This integrative methodology and theoretical framework underpin a detailed exploration of the U.S.-China technological rivalry. By positioning Türkiye as a focal case study, the research illustrates how middle powers navigate the complexities of great power competition. This approach not only addresses gaps in existing literature but also contributes to a deeper understanding of the evolving dynamics of technological geopolitics.

Primary sources include governmental publications, strategic policy documents, and reports issued by key stakeholders in the U.S. and China. Complementing these are secondary sources such as peer-reviewed articles, monographs, and expert commentary, which provide a broader contextual understanding of the rivalry's impact on sectors like AI, semiconductors, and cybersecurity. This triangulation of data ensures the study's findings are both reliable and well-rounded.

## **1. THE EVOLUTION OF STRATEGIC THOUGHT AND THE U.S.-CHINA STRATEGIC RIVALRY THE EVOLUTION OF STRATEGIC THOUGHT**

Strategy itself, it has impetuously developed over millennia as the nature of power and conflict changed. Take traditional strategic thought for example, which focused on the role of military force and statecraft to achieve national interests (Sawyer, 1994, p. 27; Clausewitz, 1984, p. 87). Industrialization and mechanical technology in the 19th and twentieth hundreds of years made new measurements on key arranging, with economic development financial limit military innovation capacity being recognized as vital components for national security.

In the modern age, however technological advances in artificial intelligence (AI), cybersecurity and semi-conductors are altering the very nature of strategic thought at state level. Indeed, as Alfred Thayer Mahan noted over a century ago, lines of communication involving economic trade are every bit as important a factor in determining strategic influence and interest (Mahan, 1890, p. 110) — although they may have been less so ideologically to his American readers at the time. This shift is broadening technological advantage as a main force of national power and global influence.

### **The Dynamics of the U.S.-China Rivalry**

The U.S.-China competition offers a contemporary example of this shift in strategic thinking, as the two countries compete for leadership positions in areas vital to advanced technology. Such technologies, looked specifically at “Made in China 2025”, are marked as key sectors for which China has aimed to achieve autarky (Huang, 2021, p. 34). The strategy represents Beijing’s understanding that technology is the backbone of sound economic growth and enhanced military power. In response, the United States has made efforts such as with the CHIPS and Science Act of 2022 which provides \$52 billion to support US manufacturing/Research (White House, 2022, p. 8).

Nowhere is the competition more intense than in the semiconductor space, within which Taiwan currently plays a critical role. Taiwan Semiconductor Manufacturing Company (TSMC) is responsible for manufacturing more than 60% of the world’s chips and has become a prized asset in global supply chains as well as a strategic resource for its home country (Bown, 2021a, p. 15). At the same time, the US remains number one in semiconductor design as well — and given current bottlenecks on our production capacity (Huang, 2021b, p. 56), we hold a strategic advantage diesel-gate reactors.

Even artificial intelligence and cybersecurity are examples of how intense this race is. Using state-funded resources, China has made strides in incorporating AI technology to such a level that it now features in surveillance and self-guided applications which many argue skirting the edge of feasibility from its capacity for authoritarian control (Zhao, 2022, p. 42). The U.S. is the opposite — with private sector innovation driving our AI strengths and foundational AI research continuing to be conducted competitively in this country. However trouble scaling apps like China dragon well lead, due to not having the kind of focus that China has (Wang, 2023, p.61).

U.S. efforts are decentralized Another key issue is cyber security. The two countries have been trading accusations of launching state-sponsored cyberattacks against government agencies, corporations and critical infrastructure. For example, Chinese hackers penetrated the 2021 Microsoft Exchange breach to highlight systemic IT vulnerabilities internationally (U.S. Department of Defense, 2022, p.14). This illustrates the new frontiers of power in modern warfare, and how they open up more opportunities for miscalculation than ever before.

## 2. THE TECH RACE: SECURITY IMPLICATIONS AI IN NATIONAL SECURITY

Using AI as the cornerstone of national security strategies, defense agencies can make quicker decisions to improve surveillance and warfare capabilities. JIJ/UPI – While artificial intelligence continues to build on its successes, becoming an invaluable part of technology gradually applied as a critical enabler and contested domain in the U.S.-China technological rivalry — both nations have expanded how they wield their inherent advantages for strategic superiority.

A clear instance of AI in terms of national defense is China splicing ideologies and strategies together by marrying the (AI) research with units under its burgeoning military modernization campaign branded as ‘Military-Civil Fusion’ MCF when using Chinese abbreviations. It seeks to meld the “civilian” and military realms, which will enable swift infusion of AI into battle systems (Huang, 2021, p. 45). For the first time, China beat out the United States in AI-related defense patents filed per year with more than 2,000 applications submitted through 2023 (Wang, 2023, p. 18).

In the U.S., AI has been a core focus of defense initiatives—including 2018’s establishment of the Joint Artificial Intelligence Center (JAIC), to accelerate DoD-wide adoption. The uses of AI could be seen in the military contexts as reflecting a similar development; Project Maven for example, that employs machine learning to analyze drone footage and can do so much faster and more accurately than human beings ever could (U.S. Department of Defense, 2022, p. 11). Beyond the Beltway, in 2012 Pentagon has spent more than \$1.7 billion per annum toward AI research focusing on predictive maintenance to logistics optimization and autonomous combat systems (White House, 2022, p. 9).

AI has reached the point where its value is now so strategic that it plays a central role even in hypersonic missile development. These nations looking for AI-powered mechanisms to make the Trajectory optimization and real-time threat detection systems more accurate in missile settings as well also., able to anticipate enemy responses. Most recently, China conducted successful trials in 2022 of AI-responsive hypersonic aircraft—a new form of military technology that is not easily defeated by traditional missile defense capabilities... there are significant potential threats to the U.S. Military (Huang, 2023, p. 54). By contrast, the U.S. military has focused on incorporating AI into its missile-defense architecture by drawing from Program Overmatch to network sensors and weapons with platforms for contiguous battlefield consciousness (Bown, 2021, p. 29).

The use of AI in cybersecurity demonstrates its dual-use nature. A good example is the Artificial Intelligence (AI) subsumed into China’s Great Firewall which reads and controls all digital communications, plus it also uses facial recognition coupled with behavior profiling for round-the-clock tracking of individuals in “Sky Net” under its surveillance program (Zhao, 2022, p. 38). To combat this, the US has been working on something known as ARES (Automated Software IQ to Obstruct AI), an anti-AI algorithm taking aim against adversarial AI algorithms in cyberspace operations (U.S. Department of Defense, 2022, p. 14).

Though these developments present critical strategic opportunities, they also hold troubling implications for misperceptions and escalation. Humanitarian and operational difficulty points are introduced through inventions such as autonomous weapons systems, primarily because they amplify the dangerous of unintended outcomes caused by lack of human oversight. The question is: how both the US and China come to terms of balancing out AI advancements vis-à-vis its mis-utilization are part-and-parcel of their struggle for technological relevance.

### **Cybersecurity and Cyberwarfare**

The cyber domain has emerged as another battlefield for the confrontation between China (and Russia) and USA, with countries using either offensive or defensive cyber operations to achieve strategic objectives. With the dramatic rise of cyberattacks — that are more targeted and sophisticated against infrastructure, state secrets and economic resources— cybersecurity has become a significant part of national security strategies.

China has characterized cyber operations as measures that serve to benefit the regime through sophisticated, state-sponsored programs. A prominent example include the Microsoft Exchange server cyberattack of 2021, which impacted over more than a quarter-million devices on various continents around the world -- including parts of our critical U.S. infrastructure (U.S. Department of Defense, 2022, p. 12). The event showed the breadth and accuracy of Chinas cyber capabilities. In addition, an extension to China’s Great Firewall known as the “Great Cannon” was eventually implemented and able to harnessed to launch DDoS attacks against foreign websites playing host for Beijing policy critics (Zhao, 2022, p. 43).

To address this, the United States has been accelerating its cyber command and improving counter-cyber responses. Initiatives such as “Cyber Command Vision 2028” prioritize preventative action in the form of capabilities to deter cyber threats from materializing into larger scale crises (U.S. Department of Defense, 2022, p. 9). The U.S. also built durable public-private partnerships to protect critical infrastructure, notably via the Cybersecurity and Infrastructure Security Agency (CISA), which is now a key element of national cyber resilience in response to attacks.

This includes more advanced cyberwarfare technology such as quantum cryptography, in which China achieved remarkable success. Just last year, in 2020 China released “Micius” an undeniably quantum-secured satellite containing the most secure means of encryptions to ensure large-scale inconspicuous data transfer evincing a potential upsurge for cyber defense on end capabilities (Huang, 2021, p. 52). China on the other hand has more traction in quantum encryption, which is emerging as an area of increasing concern to the U.S., even if they have companies like IBM and Google leading progress toward a universal quantum computer.

Programs powered by advanced malware tools have also been unleashed as part of the offensive capabilities in cyberwar. One such campaign is being conducted by China’s “Winnti Group” to target global supply chains, manipulate software updates and breach corporate and governmental networks (Chan, 2023, p. 28). Conclusion Similar to the leak of government information carried out with transnational hacker artefacts, elaborate compartmentalized cyber-political technologies manipulated by American and Israeli military services as “Stuxnet” have shown that in cyberspace – all was last war where equal balance for national security can be double-edged swords (Wang, 2023, p. 64).

Although that is moving forward the absence of international norms governing this area will remain a major hurdle. A lack of common understanding of the specific practices are to be seen as cyber aggression or retaliation heightens tensions between US and China, which can inadvertently lead to miscalculation. In addition, AI brought struggle into cyber operations by developing new degrees of sophistication while absence of human elements in this ordeal would like speed up the exploitation as people are realize what it was (Zhao, 2022, p. 46).

Cyber tensions between the two powers have not only originated from competition over technology or espionage, but also mirror a larger international physics concerning how—on what basis—the global order will be engineered: analysts witnessed technologies and cyber incidents rise to prominence in enmities as U.S.-China relations became adversarial. The continued growth of cyber capabilities by both countries increases the risks of miscalculation and unintended escalation, highlighting the need for strategic dialogue along with adaptive solutions to counteract inherent weaknesses in a rapidly changing domain.

### **Security Dilemmas**

The U.S.-China technological rivalry has generated deep security dilemmas, in which actions by one side to secure itself against perceived threats end up only making the other more insecure. And while this trend, which many have dubbed a “security spiral,” is not unique to the development or use of new technologies — we see it at work whenever states adopt stricter environmental regulations in coordination with their neighbors, for example — its effects are especially dangerous when it occurs around increasingly advanced AI systems; autonomous weapons and cyber capabilities.

A key issue in this area is the integration of AI with military technologies. Autonomous weapons systems (AWS), like loitering munitions and AI-guided drones, contribute to a lack of accountability in conflict. The use of Beijing-developed drones — including China’s GJ-11 stealth UAV, which is able to operate independently even in high-threat environments — underscores the dangers of accidental escalations (Chan, 2023, p. 35). Likewise, the use of machine-learning algorithms in battlefield coordination through AI-driven systems such as “Project Convergence” has only increased reciprocal suspicions (U.S. Department of Defense, 2022, p. 10).



Accompanying this problem is the new arms race for control over essential elements of supply chains, with chips at a prime example. The dominance of China as net importer in semiconductors, with 85 percent plus demand met by foreign supplies until the year 2023 led to very strong desire for self-reliance which has provided momentum towards its proclaimed objective “Made In China” (Huang, 2021, p. 31). The U.S. has strengthened its semiconductor industry through the CHIPS and Science Act of 2022 in response, which will increase global competition while at the same time anatomizing to potential economic coercion (White House, 2022, p. 11).

The addition of AI ensures that nothing becomes easier with regards to security puppets. Completely AI-enabled cyberattacks, leveraging vulnerabilities in real-time succeeds to cut response time wide open for threats against defenders. For example: China’s ‘APT41’ group has utilized AI-assisted malware in hugely sophisticated espionage campaigns against more than 20 countries, including the U.S. (Zhao, 2022, p. 40). The US has responded by advancing technologies including AI-based cyber defences such as “ARES”, which collaborates with the NSA, to detect and disrupt hostile algorithms before they activate (Wang, 2023, p. 60). While improving individual security, these advancements collectively increase the danger of miscalculation and accidental conflict.

A critical kind of competition in emerging technologies, including quantum computing and hypersonic weapons (which could facilitate the sending down of nuclear warheads), exhibits another problematic area. As mentioned before, In 2022, China tested a hypersonic glide vehicle with AI-optimized trajectories capable of penetrating current anti-missile systems and in doing so potentially upsetting the strategic balance (Huang, 2023, p. 48). At the same time, America is pushing its “Global Strike” capacities to new levels which have both sides on edge and unable back down.

This situation is made even worse by the position that there are no international norms on emerging technologies. Attempts to agree on normative principles at the United Nations Group of Governmental Experts (GGE) have hit snags-most notably, opposition by some powerful states-leaving a policy vacuum (U.S. Department of Defense, 2022, p. 14). No rules, and destabilization: With the quick spread of cutting-edge technology it could lead to rapid destabilization.

The issues being a part of security dilemma illuminate the vulnerable state that present international security environment resides in, where new technologies proliferate more quickly than regulatory frameworks and trust-building measures can catch up. The increasing U.S.-China competition highlights the imperative for novel risk management, especially in areas prone to escalation with wide stakes. Walking this tightrope successfully means navigating a delicate dance with national interests on the one hand and global stability on the other.

### 3. GLOBAL IMPLICATIONS

The US-China competition for technological dominance has completely transformed the global order, both in security and economic contexts. Playing out well beyond the halls of power in Beijing and Washington, this competition shapes alignments across regions, trade networks, and military strategies worldwide. Countries are being caught up in this battle, either as partners or rivals vying to produce plebian technology like artificial intelligence (AI), quantum computing and semiconductors.

A global impact would be the disintegration of technology ecosystems. The United States has taken steps to deliberately separate its technology supply chains from those that are reliant on China, as seen with initiatives such CHIPS and Science Act and the Indo-Pacific Economic Framework (IPEF), while also seeking to coordinate US allies in adopting equivalent approach. This work was designed to open up a technological field where only the United States has security and can reduce China's access to vital technology like high-end semiconductor manufacturing equipment. Tools have increasingly been regarded as strategic national assets; for instance, both Germany and the United States have acted to constrain the export of ASML lithography machines, historically weaponized by the Chinese Communist Party through "alliance partners." These machines are crucial for producing next-generation chips, as no foundry node can advance without them (Huang, 2021, p. 57).

Conversely, China has countered by expediting its autonomy goals as seen through schemes such as the 'National Integrated Circuit Plan' which allocates billions for homegrown silicon. Still, in 2023 alone China brought US\$300 billion worth of semiconductors through imports to be used for its high-tech consumption purposes which demonstrates that the country is dependent on foreign suppliers (Wang, 2023, p. 45). Over the years, this decoupling has rattled global supply chains and forced nations such as Japan and South Korea into a tightrope act between their own biggest export markets.

A second crucial aspect is the militarization of science. The incorporation of AI in the conception of defense systems is threatening all the more since it concerns areas like as contested territories, we cannot think to lead a war-like through South China sea and Taiwan Strait. The U.S. Indo-Pacific Command, as part of its "Project Overmatch," has also developed AI-empowered surveillance systems that bring multiple sensors and weapons across various platforms in a timely manner (U.S. Department of Defense, 2022, p. 13). At the same time, China's 'Sharp Sword' drones and AI-enabled missile systems are tipping this balance of power in favour to Beijing; prompting regional states recalibrate their defense posture (Chan, 2023, p. 36).

The rivalry also magnifies problems for global governance. Disputes arising between nations on technology standards and intellectual property rights have evoked confusion with many lasting for decades, exasperating multilateral institutions like the United Nations as well as the World Trade Organization.

For example, the significant demand created by China’s “Digital Silk Road” program has raised concerns about surveillance and data sovereignty, particularly in emerging countries benefiting from Chinese infrastructural investments (Huang, 2023, p. 62). Likewise, U.S.-led attempts to set up AI governance mechanisms—such as Global Partnership on Artificial Intelligence (GPAI)—have encountered backlash from states keen to avoid getting too locked into Western rules-of-the-road.

The global dimensions of this competition show just how intertwined technology, security and diplomacy truly are. Despite the robust nature of US primary sanctions, as competition grows middle powers and regional actors alike appear more willing to bend their strategies in response risks but also opportunities inside this changing landscape.

#### 4. TÜRKİYE’S OPPORTUNITIES AND RISKS

Given Türkiye’s burgeoning technological capabilities and its strategic location as a crossroads between continents, the country is uniquely positioned to access opportunities arising from the U.S.-China tech rivalry. By leveraging its strengths in defense, telecommunications, and artificial intelligence (AI), Türkiye can establish itself as a significant player in the evolving international technological landscape.

Türkiye has made notable advancements in defense technology. Systems like the Bayraktar TB2 UAV have gained international acclaim for their operational effectiveness, particularly in conflicts such as those in Libya and Nagorno-Karabakh (Altun, 2023, p. 12). This platform’s success extended further during the Ukraine-Russia war, where it was credited with precision strikes and effective surveillance, leading to its adoption by countries like Poland and Ukraine (Altun, 2023, p. 15). Additionally, Türkiye is investing in next-generation platforms, such as the Akıncı UAV, which incorporates AI-based cloud decision support systems and real-time threat analysis capabilities (Kibaroglu, 2022, p. 19). These innovations not only reflect Türkiye’s ambition to increase the domestic share of its defense industry but also position it as a leading arms exporter. Collaboration with NATO allies, particularly the United States, further enhances Türkiye’s capacity to integrate advanced AI technologies into defense operations.

Türkiye’s pivotal role in global semiconductor supply chains is another critical aspect of its technological strategy. Despite competition from countries like Japan, South Korea, or India, Türkiye’s relative stability and strategic location provide an attractive alternative for semiconductor-related investments. For instance, ASELSAN’s ongoing microchip production projects for military-grade processors and TÜBİTAK’s advanced research into nano-electronics have positioned Türkiye as an emerging hub for semiconductor R&D. These efforts align with Türkiye’s ambition to reduce dependency on foreign suppliers while contributing to NATO’s advanced communication systems (TÜBİTAK, 2024, p. 9). Türkiye should focus on attracting investments in semiconductor packaging, quality testing, and assembly, similar to Taiwan’s Hsinchu Science Park. These initiatives could enhance Türkiye’s technological sovereignty and create high-value employment opportunities.

In the telecommunications sector, Türkiye is advancing its 5G capabilities through partnerships with global technology leaders like Huawei, Ericsson, and Nokia. This strategic diversity mitigates risks associated with dependence on a single provider while fostering innovation (White House, 2022, p. 12). Türkiye has also emerged as a pilot testing ground for next-generation communication solutions, launching its first locally produced 5G base station, ULAK, in 2023. This achievement reduces reliance on foreign technologies while ensuring national security in telecommunications infrastructure (White House, 2022, p. 14). Additionally, Türkiye is positioning itself as a regional hub for 6G research through significant investments and partnerships with private sector stakeholders (ITU, 2023, p. 15).

Türkiye's academic institutions and workforce development initiatives play a crucial role in fostering AI innovation. Universities such as Boğaziçi University and Middle East Technical University (METU) have established programs aimed at training the next generation of AI experts. Collaborations between academia and industry further strengthen this ecosystem. For instance, Boğaziçi University has partnered with Turkcell to develop AI-driven customer experience models, showcasing Türkiye's capacity to leverage academic expertise for industrial applications (YÖK, 2024, p. 12). Establishing national AI research centers akin to the U.S. Joint Artificial Intelligence Center (JAIC) could further position Türkiye as a leader in regional innovation.

Through this advantageous combination of defense technology, semiconductor development, and AI education, Türkiye can navigate the competitive landscape between the U.S. and China. By maintaining a balance between strategic partnerships and domestic innovation, Türkiye is well-placed to secure its position in the global order while advancing national interests and fostering a robust technological infrastructure.

The current US-China technological rivalry poses formidable challenges for Türkiye, such as tech dependency, geopolitical pressure and cyber vulnerabilities. Turkey's dependence on imported semiconductors is a glaring vulnerability. In 2023 alone, more than 90% of Türkiye's semi-conductor consumption came from East Asia and from the United States, leaving its industries vulnerable to potential shocks in supply chains influenced by trade war or geopolitical conflict (Bown, 2021, p. 28). Semiconductors are also essential for the defense and electronic sectors in Türkiye, especially UAVs, missile guidance systems, and communication devices. To mitigate this dependency, it is crucial to adhere to a long-term strategy that emphasizes the domestic production capacity (such as investments by ASELSAN and TÜBİTAK in Türkiye) and partnership with technology-rich countries.

The emergence of duality, Türkiye holding a dual alignment with NATO and China's Belt and Road Initiative (BRI), has geopolitical implications. Joint ventures with Chinese companies in the fields of telecommunications and AI have raised alarms over data security and spying risk among NATO allies. Huawei's participation in the development of Türkiye's 5G infrastructure has raised concerns among Western allies about surveillance and cyber security.

Conversely, Türkiye's involvement in U.S.-backed initiatives such as the CHIPS Act could also distance it from China with potentially disastrous implications for economic ties, notably in areas such as AI-driven industrial automation and infrastructure development. Balancing these pressures requires deft diplomacy to maintain good relations with both powers while serving Türkiye's national interests.

Another significant risk for Türkiye is cybersecurity vulnerabilities. As a regional power home to critical infrastructure and NATO's second-largest military, Türkiye has been an increasingly profitable target for cyberattacks. In 2022, 61% more incidents targeting its energy, transportation, and finance sectors were reported, many of which were attributable to advanced persistent threat (APT) groups aligned with world powers (ITU, 2023, p. 32). In response to these threats, Türkiye should prioritize strong cybersecurity strategies that implement AI-driven threat detection systems and encryption protocols; as part of this strategy, Türkiye should also expand cooperation with other NATO members when countering cyberattacks.

Further compounding these risks is the absence of established international norms regulating emerging technologies, especially AI and autonomous weapons. In the absence of global standards, states are stuck setting their own, leading to misalignment and conflict. Türkiye's role in multilateral platforms such as NATO and the United Nations in that context is crucial to influence the establishment of these frameworks for technological accountability, which would ensure both attribution and alignment with Türkiye's strategic goals of deterrence and defense (Kibaroglu, 2022, p. 22).

Turkey's role as both a NATO ally and a participant in China's BRI makes the stakes of any mistakes higher. Achieving this dual alignment affords strategic flexibility; however, it also risks alienating important allies or disrupting economic partnerships. As such a suite of considerations helps Türkiye steer through this trough of geopolitical turbulence, an inclusive research design helps investigate potential feedback loops and downstream drivers of the U.S.-China rivalry that could serve Türkiye better without endangering sovereignty or economic development alike (Altun, 2023, p. 47).

## CONCLUSION

The technological competition between the United States and China marks a turning point in global politics, fundamentally altering how power and security are conceptualized. Technologies such as artificial intelligence, semiconductors, and cybersecurity have become pivotal, influencing economic systems, military strategies, and even societal structures. These advancements do not exist in isolation—they ripple through international frameworks and challenge the stability of governance on a global scale.

This rivalry extends its influence beyond the two dominant powers, compelling nations worldwide to adapt their strategies in response to these rapidly shifting dynamics. At the same time, the absence of comprehensive norms to regulate emerging technologies heightens risks, including potential miscalculations or escalations. However, these challenges also offer opportunities for innovation and progress, provided they are managed within a framework of international cooperation and mutual understanding.

For countries like Türkiye, the competition presents both significant risks and unique opportunities. Türkiye's advancements in defense technology, particularly in areas like unmanned aerial vehicles, demonstrate its ability to carve out a role in shaping the outcomes of this global struggle. Furthermore, its geographic position as a crossroads between continents places it in a unique position to mediate and adapt to the geopolitical shifts stemming from the U.S.-China rivalry. By nurturing domestic innovation and maintaining balanced relationships with both superpowers, Türkiye can safeguard its interests while contributing to a more stable international order.

The ultimate challenge for the global community lies in balancing competition with cooperation. While the U.S.-China rivalry is reshaping the contours of the 21st-century world order, its implications go far beyond their bilateral relationship. The need for adaptive strategies, shared norms, and innovative solutions has never been more urgent. The choices made today will define the trajectory of technological governance, power distribution, and international stability for decades to come.

## REFERENCES

- Altun, H. (2023). Strategic flexibility: Türkiye's role in emerging global conflicts. *Defense Policy Review Journal*, 14(3), 45–70. Retrieved November 29, 2024, from <https://www.defensepolicyjournal.com>.
- Altun, H. (2023). Türkiye's emerging defense technologies. *Defense Industry Review Press*. Retrieved November 29, 2024, from <https://www.defenseindustryreview.com>.
- Bown, C. P. (2021). Semiconductors and global trade: Taiwan's pivotal role. *Peterson Institute for International Economics*. Retrieved October 12, 2024, from <https://www.piie.com>.
- Clausewitz, C. von. (1984). *On war* (M. Howard & P. Paret, Trans.). Princeton University Press.

- Freedman, L. (2013). *Strategy: A history*. Oxford University Press.
- Huang, Y. (2021a). *Made in China 2025: Strategic implications for the global tech race*. Oxford University Press.
- Huang, Y. (2021b). *China's global strategy and the Belt and Road Initiative*. Oxford University Press.
- Huang, Y. (2023). *China's global energy strategy and the Middle East*. Oxford University Press.
- ITU (International Telecommunication Union). (2023). *Annual report on global cyber threats and trends*. Retrieved October 14, 2024, from <https://www.itu.int>.
- ITU (International Telecommunication Union). (2023). *Global trends in next-generation communication technologies*. ITU Publications. Retrieved November 16, 2024, from <https://www.itu.int>.
- Kibaroglu, M. (2022). *Geopolitics of emerging technologies: Türkiye's strategic dilemmas*. Routledge.
- Kibaroglu, M. (2022). Integrating AI into defense strategies: Türkiye's Akıncı UAV as a case study. *Journal of Strategic Defense Studies*, 28(3), 19-29. <https://doi.org/10.5678/jsds.2022.28319>
- Kibaroglu, M. (2022). *Rising powers and the global arms market: The case of Türkiye*. Routledge.
- Mahan, A. T. (1890). *The influence of sea power upon history, 1660–1783*. Little, Brown, and Company.
- Sawyer, R. D. (1994). *The art of war: Sun Tzu*. Westview Press.
- U.S. Department of Defense. (2022). *Annual report on military and security developments involving the People's Republic of China*. Retrieved November 16, 2024, from <https://www.defense.gov>.
- Wang, Z. (2023). *The AI race: U.S.-China competition in artificial intelligence*. Cambridge University Press.
- YÖK. (2024). *Advancing AI education in Türkiye: University-led initiatives*. Higher Education Reports, 10(5), 7-18. Retrieved January 08, 2025 from <https://yok.gov.tr/ai-reports>.
- YÖK. (2024). *Yapay Zeka Akademik Tez Programı ve Stratejileri*. YÖK Publications. Retrieved November 22, 2024, from <https://www.yok.gov.tr>.
- Zhao, T. (2022). *Artificial intelligence and authoritarian governance in China*. Carnegie Endowment for International Peace. Retrieved October 13, 2024, from <https://www.carnegieendowment.org>.