EMERGING MILITARY TECHNOLOGIES AND SHIFTING GLOBAL BALANCE OF POWER: A REALIST PERSPECTIVE

CÔNG NGHỆ QUÂN SỰ MỚI NỔI VÀ SỰ THAY ĐỔI CÁN CÂN QUYỀN LỰC TOÀN CẦU: PHÂN TÍCH TỪ GÓC ĐỘ CHỦ NGHĨA HIỆN THỰC

Nguyen Thi My Hau, Le Thi Phuong Loan*

The University of Danang - University of Foreign Language Studies, Vietnam

*Corresponding author: ltploan@ufl.udn.vn

(Received: March 01, 2026; Revised: March 27, 2026; Accepted: April 10, 2026)

DOI: 10.31130/ud-jst.2026.24(5C).295

Abstract - This paper analyzes impacts of emerging military technologies such as Artificial Intelligence (AI), autonomous weapons, and hypersonic weapons on global power shifts. Grounded in the Realist framework with case study and forecast methods, the paper examines how the technological race is reshaping national power and changing the global balance of power. The research findings indicate that breakthroughs in emerging military technologies are eroding traditional deterrence doctrines and intensifying security dilemmas, thereby, making the global balance of power more dynamic and unpredictable. National power, as a result, depends heavily on mastering core technologies rather than relying solely on tangible military assets. In this context, from a Realist perspective, Vietnam needs to prioritize the development of core technologies, while implementing flexible technology diplomacy to enhance its self-help capacity and promote strategic position in a volatile international environment.

Key words - Emerging military technologies; global power structures; balance of power; realism; technology diplomacy.

Tóm tắt - Bài báo phân tích tác động của công nghệ quân sự mới nổi (EMTs) như trí tuệ nhân tạo, vũ khí tự hành và siêu vượt âm đến sự dịch chuyển quyền lực toàn cầu. Sử dụng phương pháp nghiên cứu tình huống và dự báo cùng lăng kính Chủ nghĩa hiện thực, bài báo làm rõ cách thức cuộc đua công nghệ tái định hình sức mạnh quốc gia và thay đổi cán cân quyền lực toàn cầu. Kết quả nghiên cứu cho thấy những đột phá về EMTs làm xói mòn học thuyết răn đe truyền thống và làm trầm trọng thêm thế lưỡng nan an ninh, khiến cán cân quyền lực toàn cầu trở nên năng động và khó dự đoán hơn. Sức mạnh quốc gia ngày càng phụ thuộc vào khả năng làm chủ công nghệ cốt lõi, thay vì chỉ dựa vào khí tài quân sự hữu hình. Theo đó, Việt Nam cần tập trung phát triển công nghệ cốt lõi và triển khai ngoại giao công nghệ nhằm tăng cường năng lực tự cứu (self-help) và củng cố vị thế chiến lược trong môi trường quốc tế đầy biến động.

Từ khóa - Công nghệ quân sự mới nổi; cấu trúc quyền lực toàn cầu; cán cân quyền lực; chủ nghĩa hiện thực; ngoại giao công nghệ.

1. Introduction

In the geopolitical landscape of the 21st century, the world is witnessing a significant power shift from West to East, driven by remarkable economic growth and rising powers in Asia such as China. This transition has challenged the US global dominance and traditional Western-dominated world order. From a Realist perspective, military power determines national standing. In the 21st century, emerging military technologies (EMTs) such Artificial Intelligence (AI), hypersonic weapons, and cyber warfare have enabled emerging powers to close the gap and disrupt the traditional military advantage of the West, creating a volatile international environment and reshaping the global balance of power. In this sense, this study analyzes the impact of EMTs on the shifting international balance of power from a Realist perspective. Accordingly, foreign policy recommendations are proposed to help Vietnam proactively adopt advanced EMTs, enhance a self-reliant, self-sufficient, and flexible foreign policy to maximize national interests in a reshaping world order.

2. Overview of Realism in International Relations

Realism is a long-standing International Relations theory, positing that in an anarchic international environment, states always strive for survival. This school of thought is characterized by the emphasis of state-centric power and security. In this study, the two strands of Defensive Realism and Offensive Realism are employed to analyze EMTs development and implications for the transition of global power. From a Realist lens, in a self-help system, survival and national security are the primary goals of all states. Accordingly, power is the most reliable means to secure survival [1]. While Defensive Realists believe that states seek to accumulate power only to ensure survival, not to change the system structure or intensify confrontations [2], Offensive Realists argue that states must assume the worst about other states' intention, thus, always pursue hegemony in an anarchic system [3]. Therefore, to ensure security, states must maximize their relative gains while limiting the power of others in an anarchic international environment from a Realist lens [2].

3. A Realist perspective on impacts of EMTs on the global power balance and security dynamics

3.1. Changing perceptions of power and approaches to power balancing

From a Realist perspective, Kenneth N. Waltz relates a state's power to its material factors such as population, territory, economic capability, and military strength [1]. However, in the digital age, EMTs are redefining material factor superiority: military power, often considered the final arbiter of security or conflict settlement, and the core

component of state power in Offensive Realist school [2] [3], is now measured not only by the quantity of modern equipment but also by the speed of information obtaining, processing, and integration of combat weapons to enhance operational capabilities. This reality leads to a paradox: states with vast territories possessing expensive, advanced weapons become more vulnerable to asymmetrical attacks using inexpensive drones from smaller states. A geographically small state that masters AI algorithms in controlling swarms of unmanned aerial vehicles (UAVs) can completely neutralize the modern military platforms of a superpower. For example, in June 2019, Iran shot down a US drone (RQ-4A Global Hawk/MQ-4C Triton) worth approximately $220 million over the Strait of Hormuz using its domestically produced 3-Khordad air defense missile system [6]. A drone, a massive investment costing twice as much as an F-35 fighter jet, was destroyed by an air defense system costing dozens of times less. This demonstrates that massive military platforms are no longer "invincible". The US is also facing an unprecedented economic war of attrition against inexpensive drone technologies. Specifically, US Navy warships had to resort to SM-2 interceptor missiles, costing $2.1 million each or ESSM missiles costing $1 million each, to shoot down Houthi suicide drones costing only $2,000. Furthermore, the Houthi have trained their proxy forces in launching mass (saturation attacks) of inexpensive drones. The use of low-cost drones in large-scale attacks creates a clear cost difference, where the defender must spend much more to respond. This situation can be seen as a form of economic pressure over time. As a result, it may increase the defense budget and force the country to make trade-offs in spending. In the long run, this may also affect its overall production capacity (PPF). It is estimated that launching 50 drones worth $100,000 would require the US to spend at least $100 million on missiles for defense [7]. This is how a smaller state compromises the financial capacity and military presence of a superpower. In addition, cyber power allows weaker states to achieve strategic goals without military confrontations. Specifically, the Stuxnet malware campaign (2010) carried out by Israel to infiltrate the industrial control systems of the Natanz nuclear facility (Iran) caused over 1,000 nuclear centrifuges to self-destruct. This slowed Iran's nuclear program by several years. Cyber power helped Israel achieve its ultimate security goal without firing a single shot [8]. In this sense, EMTs breakthroughs are gradually blurring the traditional concept of power and redefining the nature of power in an anarchic international system.

Realists assume that in an anarchic international environment, states typically balance power through two key strategies: internal balancing and external balancing. Yet, the rapid development of EMTs has forced state leaders to reassess the costs and benefits of these two approaches. Traditionally, internal balancing model relied on increasing tangible hard power such as the quantity of military manpower, weapons, and defense budget. Furthermore, in the past, technologically backward states could copy military breakthroughs from larger powers to mitigate research risks and costs [9]. However, rapid advancements in science and technology have now transformed the nature of power, shifting it from tangible to intangible, integrated systems. In this era, a smaller, technologically sophisticated military force with data dominance and automation can outperform massive, conventional armies. For example, in the Russia - Ukraine conflict, Russia has increasingly deployed Lancet loitering munitions - AI-integrated drones costing approximately $35,000 - to destroy modern, advanced military equipment supplied to Ukraine by the West, such as German Leopard 2 tanks and US Bradley fighting vehicles - each worths millions of dollars [10]. This reality shows that the old-style, "massive steel" armies are becoming extremely vulnerable to an efficient force with superior algorithms. These profound changes have prompted a restructure of defense spending priorities. States are now investing not only in military equipment but also in research and development (R&D). In recent fiscal years, the US Department of War (then Department of Defense) has repeatedly requested unprecedentedly record budgets for Research, Development, Testing, and Evaluation (RDT&E) - *i.e.* exceeding $130 billion in 2023 - allocating on basic science, semiconductor, AI, and directed-energy weapons rather than conventional arms production [11]. Major powers have increasingly focused on mastering EMTs such as AI, hypersonic weapons, often applied in operations including cyber warfare. Therefore, EMTs have been developed based on complex software algorithms and ultra-small semiconductor chip systems, making them very difficult to replicate without sufficiently advanced industrial infrastructure. Indeed, military technology is now tacit knowledge and closely tied to an organization, making it resistant to imitation or espionage [12]. Therefore, states are forced to invest enormously on R&D to ensure strategic self-reliance. This shift also generates a new form of internal balancing: the integration of civilian and military capabilities. In the era of EMTs, boundaries between civilian and military technologies are blurring due to the duality of new breakthroughs. With foundational technologies like AI and data infrastructure often led by private technology corporations, states tend to integrate technologies primarily developed in universities, startups, and civilian innovation ecosystems into their defense capabilities. Such an integration optimizes national resources, allowing smaller states or emerging powers to avoid dead-end research and compensate for traditional military budget shortfalls, thereby creating leaps in combat capabilities. A prime example is China's military-civilian integration strategy, mobilizing technology corporations like Baidu and Huawei to develop AI and 5G for national defense. Accordingly, the power race is no longer simply about arms purchases, but a race for innovative capabilities [13].

Regarding external balancing, the stringent infrastructure and transnational supply chain requirements of EMTs have driven states to seek security through international cooperation. For example, Ukraine has promoted the formation of the Drone Coalition since early 2024, led by the United Kingdom and Latvia, aiming to provide Ukraine with one million reconnaissance-strike drones, and various anti-UAV systems [14]. Similarly, Sweden's official accession to NATO in 2024 marked a

strategic shift in security mindset: from neutrality to alliance to ensure collective security from a high-tech ecosystem [15]. The nature of cooperation also changed, shifting from traditional mass mobilization to network-centric capabilities such as levels of technological compatibility or shared data structure. A prime example is the trilateral security partnership of AUKUS, in which the US and the United Kingdom committed to transferring submarine technology and providing Australia with nuclear energy in the near future [13]. This is a rare move in international relations regarding the sharing of sensitive technologies, signaling a strategic shift in external balancing strategy of the US: instead of simply providing security protection, the US is striving to enhance the self-defense capabilities of allies through the acquisition of advanced military technology and demanding greater investment from allies [16]. In this sense, alliances are no longer formed solely to balance material power but to build a collective shield against technological threats from adversaries.

3.2. Expanding the concept of national security and changing the relative status of states

The advancement of EMTs has challenged the conventional definition of national security. In previous centuries, national security encompassed constituent material factors such as military strength and territorial integrity [1]. However, the explosion of AI, cyberspace, and autonomous weapons has created a new strategic reality: a state can attack another state's power grid without crossing geographical borders, with massive destructive power equivalent to a traditional military operation. For example, in 2020, in response to Iran's attack on the water system in rural Israel, the Israeli government launched a non-volatile cyberattack on Shahid Rajaee port in Bandar Abbas - Iran's most strategically important seaport. The attack completely disrupted Iran's computer systems coordinating water and land traffic networks [17]. Such incidents redefined the concept of national security, shifting from a "protection of geographical borders" mindset to a "protection of multidimensional systems" mindset. From a Realist perspective, national security today is a vast, dynamic, interconnected system encompassing six spaces namely artificial space, social space, biological space, information space, natural space, and outer space [18]. National security in the EMT era also means maintaining strategic autonomy [19]. This includes controlling key digital infrastructures and minimizing reliance on "technological bottlenecks" controlled by adversaries. The US has developed the Secure and Trusted Communications Network Reimbursement (Rip and Replace) program, allocating billions of dollars to support American companies to replace equipment from China's Huawei and ZTE, deemed national security threats, to secure reliable data flows and communication supply chains [20]. At the same time, China has mobilized massive capital to build a closed-loop technology supply chain [21]. Through the "Digital Silk Road" initiative, China has promoted the export of 5G infrastructure, data centers, and especially the BeiDou satellite navigation system, providing services to over 200 countries and territories, allowing the Chinese military and economy to operate independently of the US GPS system. Furthermore, China is also building a parallel global digital infrastructure to mitigate risks from Western-controlled systems [22]. In addition, national security is ensured through technological adoption capacity, measured by the ability to transform AI algorithms into a practical deterrent advantage to maintain strategic autonomy [23]. Overall, national security in the 21st century is a multi-dimensional defense, where the ultimate goal is not only to protect physical territorial integrity but also to control key digital infrastructure, enhance self-reliance in core technology supply chains, and transform algorithms into tangible deterrents to ensure survival in an anarchic international environment.

These developments not only reshape how national security is understood but also affect the relative position of states in the international system. States that can control critical digital infrastructure, dominate key technology supply chains, and apply EMTs effectively in their military strategies are more likely to improve their standing in the global power structure. In contrast, those that depend heavily on external technologies may become more vulnerable and gradually lose their relative influence [18].

3.3. Shifting warfare methods

The advancement of EMTs has expanded the concept of national security to a multi-spatial form, thereby shifting methods of conducting warfare. In the digital age, national power is tied to the ability to dominate data and master core technologies, leading to modern warfare: conflict taking place silently in cyberspace where strategic advantage belongs to the side that achieves information superiority.

Firstly, the rise of algorithmic warfare and pressure of preemptive strikes. The integration of AI into the entire kill chain - from target detection to strike decision-making - has compressed the time cycle from hours to milliseconds. A paradox of survival was developed by Michael C. Horowitz: in an anarchic environment, human intervention in AI-integrated military systems is gradually reduced to achieve machine speed [23]. The fear of instant defeat by an adversary using fully autonomous systems drives state leaders to prioritize instantaneous decisions and automation, even though this increases the risk of unintended conflict escalation. The methods of warfare have therefore evolved from slow human coordination to a drastic shortening of the OODA (Observe - Determine - Decide - Act) cycle. A prime example is Israel's deployment of the AI-powered targeting system called *The Gospel* in Gaza Strip military operations since 2023. Notably, this system has significantly revolutionized the speed and volume of target identification in Gaza, from 50 targets per year (by human spies) to 100 targets per day (by *The Gospel*) [24].

Secondly, the shift towards gray zone conflict and non-kinetic warfare, as conventional military confrontations become increasingly costly and risky, leads states to seek strategic advantages below the threshold of total war. Here, EMTs act as a lever enabling state actors to silently attack critical infrastructure such as power grids, transportation and financial systems of an adversary [25]. Importantly, these

attacks are not merely monetary gains, yet long-term advantages such as disrupting the victim state's defense capability, economic stability and public trust [26]. These gray-zone activities allow aggressor states to deeply interfere in the internal affairs of victim states without concern for direct military retaliation, thereby eroding the traditional deterrence model. Furthermore, the proliferation of UAVs has outpaced international law development regarding these devices, allowing states to use them for espionage and intrusion into foreign airspace while maintaining the ability to deny strategic responsibility [27]. For example, a joint investigation by Nordic countries including Denmark, Norway, Sweden, and Finland in 2023, uncovered a network of Russian vessels and autonomous vehicles operating under the guise of scientific research to survey critical infrastructure on the North Sea seabed. These vessels often disable automatic identification systems (AIS), making their journeys difficult to trace and creating a phenomenon of "ghost ships" [28]. Furthermore, this not only allows the attackers to continue denying responsibility but also transforms the ocean into a high-risk gray zone, where Nordic countries face serious security threats without a sufficiently efficient international legal mechanism to prevent them in a timely manner.

Third, modern gray-zone warfare marks the expansion of conflict into the cognitive domain, where combat targets are not limited to physical entities but the will, perceptions, and beliefs of an adversary. Particularly, aggressor state can manipulate how the victim state processes information and makes decisions. AI and social media are being weaponized to generate disinformation and spread deepfakes at breakneck speed to manipulate public perception and undermine social stability without the use of firepower [29]. A prime example is China's "Cognitive Warfare" doctrine, which is an expansion of the three-warfare strategy of public opinion, psychological, and legal warfare. By utilizing AI and Big Data, states can control the flow of information to defeat an adversary without fighting, transforming cost-benefit calculations in the gray zone into an optimal strategy to shift the relative balance of power without triggering all-out war [30]. The expansion of cognitive domain conflict is clearly demonstrated through Singapore's proactive defense efforts, recognizing AI and deepfake as potentially weaponized tools that spread disinformation, erode public trust, and destabilize society. In October 2024, Singapore Parliament passed a bill banning the use of AI-generated content to impersonate candidates in elections. By establishing legal barriers against AI-driven content, Singapore is pioneering the protection of "cognitive sovereignty" against modern non-kinetic warfare methods, where victory is no longer determined by firepower but the ability to control the information space [31].

Last but not least, the proliferation of EMTs has led to a shift in the character of war by fueling the rise of asymmetric warfare, creating a cost-effectiveness paradox where the advantage of traditional physical capabilities is reversed by the ability to effectively attrite at a lower cost. EMTs breakthroughs have invented small, smart, and inexpensive weapons, empowering weaker states to challenge massive, expensive platforms of stronger states such as warships or aircraft [13]. Furthermore, the mass production of inexpensive drones creates an economic asymmetry: the victim state is forced to spend millions of dollars on interceptor missiles to counter devices costing only a few thousand dollars, leading to financial exhaustion and a loss of sustained operational capability [32]. This paradox also evident in cyberspace: when a modernized state becomes dependent on multi-billion dollar digital infrastructure, it will become more vulnerable towards cheap yet strategically effective malware [33]. As illustrated earlier, in military confrontations in the Red Sea in 2023-2024, the US had to resort to SM-2 interceptor missiles, each costing over $2.1 million, to destroy swarms of Houthi suicide drones, which cost only about $2,000 to $20,000 - a difference of hundreds of times. Therefore, despite its military superiority, the US faces the risk of financial depletion against an adversary capable of mass-producing inexpensive equipment [7]. This demonstrates that EMTs diminish advantages of major powers with conventional warfare methods, forcing them to confront inexpensive yet highly dangerous threats from smaller states in a war environment of plausible deniability.

3.4. Developing new national security models in a reshaping global power structure

The shifts in security concept and warfare methods have compelled major powers to develop new national security models to adapt to the era of EMTs, thereby fundamentally restructuring global power. First and foremost is the formation of an integrated national security model. Current major powers have evolved from traditional boundaries between military, economic, and technological spheres toward a more holistic security model. For example, the US has developed an integrated deterrence strategy, combining conventional military power with technological capabilities and a close alliance system. The establishment of the US Space Force and Cyber Command is evidence of efforts to expand this security model into new multi-domain operations (*i.e.* land, air, sea, cyber, cognitive domains) [11]. Simultaneously, through AUKUS, the US has transformed the ally network into a constitutive part of its domestic security ecosystem, ensuring strategic autonomy and survival from a Realist perspective [34]. Conversely, China implements the "Military-Civil Fusion" strategy to incorporate technological breakthroughs from the private sector into advanced EMTs [30]. Through data security legal frameworks such as the Data Security Act and National Intelligence Act, China has utilized large technology corporations to directly serve critical military objectives such as intelligentized warfare (human-machine collaborative decision making). Furthermore, China massively invested in the semiconductor industry to promote technological self-reliance - considered a vital pillar of national security - to overcome technological blockade measures from the West [35].

Secondly, the emergence of "technological bottlenecks" has reshaped the distribution of power, in

which the ability to control these bottlenecks becomes a superior strategic advantage. The development of new technology-based security models does not lead to an even distribution of power but rather promotes the formation of monopolies at strategic bottlenecks [32]. While EMTs benefit weaker states with asymmetric warfare and gray zone activities, at the structural level, power tends to re-centralize in states dominating core technologies and high-tech value chains. A prime example is the semiconductor supply chain for AI components, which is highly concentrated in a few regions such as Taiwan (China) or Japan, generating coercive power, allowing states controlling key stages of the supply chain to use technology as a tool for strategic pressure. This phenomenon can be explained through the concept of "weaponized interdependence," whereby states exploit asymmetrical control over technological networks to exert strategic pressure [36]. A state holding the "choke point" can weaponize access to sever or manipulate an adversary's infrastructure, causing serious security damages without triggering armed conflict. In this context, from a Neorealist perspective, such dependence creates structural vulnerabilities, compelling states to minimize reliance in order to ensure security and maintain power [1].

Third, technology is no longer viewed as a neutral yet techno-nationalist commodity, where states prioritize self-reliance and control over core technologies. A prime example is the Dutch government's decision, under pressure from the US, to officially revoke export licenses, preventing ASML Holding from selling advanced lithography machines to China. This shows that lithography technology is no longer viewed as a neutral commercial commodity, rather, it has been weaponized as a national security asset to maintain strategic position. The Netherlands - a small state possessing core technological secrets - is willing to trade off economic profits for control of access to the global value chain. In the new power structure, the state that dominates the new industrial revolution and possesses core technologies will be a new global hegemony[37]. Power now lies not only in owning the final product, but the ability to control access to the global value chain [38].

4. Policy implications for Vietnam

Considering EMTs impacts on global power shift, Vietnam - a rising middle-power - is restructuring its national security approach to safeguard core interests in an anarchic international environment full of uncertainties. To navigate successfully in a volatile international environment, Vietnam needs to combine internal and external balancing solutions from a Realist lens.

The first recommendation is that Vietnam should consistently promote its internal balancing strategy by investing in asymmetric technologies to mitigate the risk of sanctions and armed races. Specifically, in an international system where technological superiority can neutralize traditional weapons [25], Vietnam needs to prioritize resources on specialized EMTs such as AI, swarm drone systems, and long-range precision-guided missiles - key to building effective asymmetric deterrence (A2/AD) capabilities. The goal of achieving self-reliance in defense technology needs to be concretized by increasing investment in R&D to translate intellectual capital into practical firepower.

Secondly, Vietnam needs to develop its domestic semiconductor chip and telecommunications equipment manufacturing capabilities, while creating a transparent mechanism for the private sector to deeply participate in the technological ecosystem, facilitating "dual-use technologies" for both civilian and security contexts. In this sense, Vietnam could reduce strategic dependence on foreign technology supply chains [26]. In fact, in the digital age and intensifying major power competitions, supply chains are increasingly politicized as tools for adjusting strategic power. From a Realist perspective, complete dependence on hardware or software from other major powers is an existential risk.

Thirdly, developing cognitive security and cyber warfare capabilities must be emphasized at the same level as protecting territorial integrity. As conflict shifts to the cognitive realm, the ability to combat disinformation and deepfakes is a prerequisite for maintaining political stability. Therefore, Vietnam needs to build sufficiently strong algorithmic shields to protect public digital trust and ensure the integrity of strategic decision-making processes.

Fourthly, Vietnam needs to develop a high-quality workforce that serves long-term technological strategies. In the context of rapidly developing EMTs, humans play a key role in mastering and effectively applying these technologies. Therefore, Vietnam should invest more in training human resources in important fields like AI, cybersecurity, and data science. It is also necessary to promote Public-Private Partnership, and Triple Helix of Three-Party Partnership (between the State – University - Enterprise) to transform knowledge into practice. In the long term, building a high-skilled workforce will help Vietnam enhance its technological capacity, reduce dependence, and achieve technological self-reliance.

Finally, regarding External balancing, Vietnam needs to uphold Bamboo diplomacy to implement a flexible soft balancing policy through technology diplomacy. Within a multipolar technology structure, Vietnam must diversify partnerships in EMTs technological transfers and research to avoid overreliance on any single technology ecosystem. Furthermore, proactively engaging in and contributing to the development of international standards on AI governance and cybersecurity at forums such as the United Nations High-level Advisory body on AI, Paris Peace Forum or Cyber ASEAN Pacific - Forum will help Vietnam enhance its national prestige and negotiating power with superpowers. This will secure Vietnam's independence and self-reliance, while leveraging the power of EMTs to maintain peace and a stable balance of power in the region.

5. Conclusion

EMTs and the shifting global balance of power, viewed from a Realist perspective, demonstrate that in an anarchic environment, technology is the tool of power, the material

energy in the digital age. Major powers like the US and China are investing heavily in EMTs to maximize their power, not for the common good [39]. Therefore, this process creates a technological race, where each technological breakthrough not only provides immediate strategic advantages but also potentially reshapes the global power structure, forcing other states to respond and accelerate competition. In addition, from a Realist lens, EMTs have replaced traditional military concept as a new measure of power, where the ability to dominate core technologies determines a state's strategic advantage. However, the shift towards a technologically multipolar order is blurring the lines between peace and conflict, creating a fragile security environment. In time of weaponizing global value chains and rising technological nationalism, the global power structure has become more fragmented than ever, posing a significant challenge to preventive diplomacy or building effective conflict control mechanisms in the future. As a result, the analysis of EMTs and their impacts on global power structure is not only theoretically significant but also has profound practical value. This research has provided an analysis of EMTs impacts on fundamental shift in global balance of power from a Realist perspective and proposed relevant policy implications for Vietnam to leverage its multilateral technology diplomacy while protecting its physical and digital sovereignty.

However, employing solely Realism to analyze EMTs' impacts does not fully reflect the complexity of their impacts on the power structure and state behaviors. Realism posits that the state is the most dominant actor in international relations; however, in the digital age, non-state actors like big Tech corporations possessing core technologies directly influence global security and power structures. In contrast, Liberalism offers a more multifaceted perspective, viewing these corporations not merely as tools of the state but as independent geopolitical actors capable of rule shaping through control of global data infrastructure and algorithms. Furthermore, Realism views each state as a homogeneous "black box," ignoring the role of internal variables. These approaches obscure the role of internal factors such as domestic politics, science - technology policies, and innovation ecosystems - factors that directly determine the speed and effectiveness of EMTs development. Conversely, Constructivism offers a more comprehensive perspective, viewing EMTs as discursive symbols of power, reflecting how states construct their identity and decision-making within the international order. For example, while the US links EMTs to the mission of maintaining global leadership and governance norms, Russia sees them as an asymmetrical means of adjusting its power status, and China integrates new technologies into its grand narrative of "national rejuvenation" and strategic autonomy. This theory helps explain the diversity in state behaviors beyond purely materialistic calculations. Future research should employ these theoretical lenses to provide a more comprehensive analysis of the diversity in EMT strategies of great powers and their impacts on global power structure.

REFERENCES

[1] K. N. Waltz, *Theory of International Politics*, Boston: McGraw-Hill, 1979.

[2] H. K. Nam, *Theories of International Relations,* Hanoi: National Political Publishing House, 2017.

[3] J. J. Mearsheimer, *The Tragedy of Great Power Politics*, New York: W. W. Norton & Company, 2001.

[4] R. O. Keohane and J. S. Nye Jr, *Power and Interdependence*. New York, United States: Longman, 2001.

[5] A. Wendt, *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999.

[6] L. Voytko-Best, "Trump: 'Hard To Believe' Iran Drone Downing 'Intentional,'" *Forbes*, June 20, 2019. [Online]. Available: https://www.forbes.com/sites/lisettevoytko/2019/06/20/iran-shoots-down-us-drone-escalating-tensions-and-increasing-oil-prices/ [Accessed February 23, 2026].

[7] L. Seligman and M. Berg, "A $2M missile vs. a $2,000 drone: Pentagon worried over cost of Houthi attacks," *Politico*, December 20, 2023. [Online]. Available: https://www.politico.com/news/2023/12/19/missile-drone-pentagon-houthi-attacks-iran-00132480 [Accessed February 24, 2026].

[8] E. Nakashima and J. Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say," *Washington Post*, June 02, 2012. [Online]. Available: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html [Accessed February 24, 2026].

[9] A. Gerschenkron, *Economic Backwardness in Historical Perspective: A Book of Essays*. Cambridge, MA: Harvard University Press, 1962.

[10] V. Thanh, "Reasons why tanks are losing their status as 'king of the battlefield'," *Tin Tuc News (Vietnam News Agency)*, Sep. 15, 2024. [Online]. Available: https://baotintuc.vn/quan-su/ly-do-xe-tang-dang-mat-dan-vi-the-vua-chien-truong-20240915052107366.htm [Accessed February 27, 2026].

[11] U.S. Department of Defense, "Fiscal year 2020 Budget Request Overview," *Washington, DC: U.S. Department of Defense*, 2019. [Online]. Available: https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2020/fy2020_Budget_Request_Overview_Book.pdf [Accessed January 31, 2026].

[12] A. Gilli and M. Gilli, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security*, vol. 43, no. 3, pp. 141–189, 2018.

[13] A. C. Dall'Agnol, "The Diffusion of Military Power: A Neoclassical Realist Analysis," *Master's thesis, Federal University of Rio Grande do Sul, Brazil,* 2023. [Online]. Available: https://hdl.handle.net/10183/263185 [Accessed January 29, 2026].

[14] UK Government, "Joint Statement by Defence Ministers of the Drone Coalition," *www.gov.uk,* July 10, 2024. [Online]. Available: https://www.gov.uk/government/news/joint-statement-by-defence-ministers-of-the-drone-coalition [Accessed February 25, 2026].

[15] NATO, "Sweden officially joins NATO," March 7, 2024. [Online]. Available: https://www.nato.int/en/news-and-events/articles/news/2024/03/07/sweden-officially-joins-nato [Accessed February 25, 2026].

[16] U.S. Department of Defense, "Fiscal Year 2026 Budget Request Overview Book," *Washington, DC: Office of the Secretary of Defense,* 2025. [Online]. Available: https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/FY2026_Budget_Request_Overview_Book.pdf [Accessed January 29, 2026].

[17] J. Warrick and E. Nakashima, "Israel linked to a disruptive cyberattack on Iranian port facility," *The Washington Post*, May 18, 2020. [Online]. Available: https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html [Accessed February 25, 2026].

[18] C. Wu, "Redefining concepts of nation and national security and establishing their models for the new era," *Journal of Safety and Sustainability*, vol. 2, March 1, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2949926724000

581?via%3Dihub [Accessed January 29, 2026].

[19] L. Weiss, "Re-emergence of Great Power Conflict and US Economic Statecraft," *World Trade Review*, vol. 20, no. 2, 2021. doi: 10.1017/S1474745620000567.

[20] Federal Communications Commission, "Secure and Trusted Communications Networks Reimbursement Program." *www.fcc.gov*, 2020. [Online]. Available: https://www.fcc.gov/supplychain/reimbursement [Accessed February 25, 2026].

[21] B. Thuan, "China pours massive investment into the semiconductor industry," *VOV Online Newspaper.* [Online]. Available: https://vov.vn/kinh-te/trung-quoc-dau-tu-khung-cho-nganh-ban-dan-post1097960.vov [Accessed February 27, 2026].

[22] State Council Information Office of the People's Republic of China, "Full Text: China's BeiDou Navigation Satellite System in the New Era." *english.www.gov.cn,* 2022. [Online]. Available: https://english.www.gov.cn/archive/whitepaper/202211/04/content_WS63647de9c6d0a757729e249d.html [Accessed February 25, 2026].

[23] M. C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review*, vol. 1, no. 3, pp. 36-57, May 2018, doi: 10.15781/T2639KP49.

[24] H. Davies, B. McKernan, and D. Sabbagh, "'The Gospel': how Israel uses AI to select bombing targets in Gaza," *The Guardian*, December 01, 2023. [Online]. Available: https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets [Accessed February 26, 2026].

[25] C. W. Kegley, Jr. and G. A. Raymond, "Realism in the Age of Cyber Warfare," *Ethics & International Affairs*, April 26, 2021. [Online]. Available: https://www.ethicsandinternationalaffairs.org/online-exclusives/realism-in-the-age-of-cyber-warfare [Accessed January 29, 2026].

[26] C. Braccia and D. T. V. Nguyen, "Vietnam - A Leading Strategic Partner in Cybersecurity," *www.authorea.com,* October 2025. [Online]. Available: https://www.authorea.com/users/951088/articles/1335860-việt-nam-đối-tác-chiến-lược-hàng-đầu-về-an-ninh-mạng [Accessed January 29, 2026].

[27] T. Ly, "Unmanned Vehicles: History, Strengths, and Gaps to Be Filled," *People's Army Newspaper*, October 05, 2025. [Online]. Available: https://www.qdnd.vn/quan-su-the-gioi/vu-khi-trang-bi/phuong-tien-khong-nguoi-lai-lich-su-suc-manh-va-nhung-khoang-trong-can-lap-day-849144 [Accessed January 31, 2026].

[28] H. Edwardes-Evans, S. Elliott, and A. Franke, "Russian vessels 'mapping Nordic subsea energy assets,'" *S&P Global Commodity Insights*, April 19, 2023. [Online]. Available: https://www.spglobal.com/energy/en/news-research/latest-news/electric-power/041923-russian-vessels-mapping-nordic-subsea-energy-assets [Accessed: February 27, 2026].

[29] E. B. Kimber, "National Security in the Digital Age: Leveraging America's Technical Advantage," *Two Six Technologies*, April 2025. [Online]. Available: https://twosixtech.com/wp-content/uploads/National-Security-Digital-Age-April-2025-1.pdf [Accessed January 31, 2026].

[30] U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China 2024," *Washington, DC: U.S. Department of Defense,* 2024. [Online]. Available: https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/Military-and-securitydevelopments-involving-the-peoples-republicof-china-2024.pdF [Accessed January 31, 2026].

[31] C. S. Fang, "Bill passed to counter digitally manipulated content, deepfakes during elections," *The Straits Times*, October 15, 2024. [Online]. Available: https://www.straitstimes.com/singapore/politics/bill-passed-to-counter-digitally-manipulated-content-deepfakes-during-elections [Accessed February 26, 2026].

[32] B. A. Chang, "*Artificial Intelligence and the US-China Balance of Power,*" Master's thesis, Massachusetts Institute of Technology, 2021.

[33] S. Munawar, S. Afzal, and R. Shahid, "Realism: Revisiting the concept of power in the age of information," *Global Strategic & Security Studies Review*, 2021. [Online]. Available: https://www.gsssrjournal.com/article/realism-revisiting-the-concept-of-power-in-the-age-of-information [Accessed January 29, 2026].

[34] K. M. Sayler, "Emerging Military Technologies: Background and Issues for Congress," *Congressional Research Service*, February 2024. [Online]. Available: https://www.congress.gov/crs-product/R46458 [Accessed January 29, 2026].

[35] Y. Peng, "The relationship between US-China semiconductor friction and US national security: A realism perspective," *Obrana a strategie*, June 30, 2024. [Online]. Available: https://www.obranaastrategie.cz/filemanager/files/3702116.pdf [Accessed January 29, 2026].

[36] H. Farrell and A. L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *Int. Secur.*, vol. 44, no. 1, pp. 42–79, Jul. 2019, doi: 10.1162/isec_a_00351.

[37] N. Flaherty, "Dutch government revokes license for ASML DUV lithography shipment," *EE News Europe*, January 03, 2024. [Online]. Available: https://www.eenewseurope.com/en/dutch-government-revokes-license-for-asml-duv-lithography-shipment/ [Accessed February 27, 2026].

[38] H. van Manen, S. Kim, A. Meszaros, and M. Gorecki, "Emerging Disruptive Technologies in an Era of Great Power Competition," *The Hague: Hague Centre for Strategic Studies,* 2022. [Online]. Available: https://hcss.nl/wp-content/uploads/2023/01/Emerging-Disruptive-Technologies-HCSS-2022.pdf [Accessed January 29, 2026].

[39] J. Dhingra, "Analysing AI Warfare Through Realist Critique of International Law," *JuWissBlog.* 2025, [Online]. Available: https://intrechtdok.de/servlets/MCRFileNodeServlet/mir_derivate_00020316/Analysing_AI_Warfare_Through_Realist_Critique_of_International_Law.pdf [Accessed January 30, 2026].