Global Technological Competition in Warfare: Impact on Global Security in the 21st Century

Dr. Aiysha Safdar[*] *Shahzeb Chaudhary*[*]

Abstract

The impact of technological advancements on global security from the perspective of classical realism is analysed in this article. The article explores how advanced and powerful nations like China, the US, and Russia are using advanced technologies to reshape strategic competition and power dynamics. The rapid evolution of digital infrastructure, robotics, and Artificial Intelligence (AI) is changing established security paradigms but is also creating new threats and opportunities. By examining these changes, the paper emphasises the strategic importance of technological superiority in projecting influence and bolstering national security. The incorporation of these advanced technologies into military strategies signals a shift from traditional warfare tactics to a more complex security environment where both physical and digital threats coexist. As technology advances, the line between traditional and emerging threats is becoming increasingly ambiguous, leading to the need for a reassessment of global security regulations and strategies. The intersection of classical realism theory and these advanced technologies is set to have a significant impact on the future dynamics of global security.

Keywords: *Technological Advancements, Strategic Competition, Global Security, Artificial Intelligence, Defence Modernisation.*

[*] Head of Department, International Relations Department, Kinnaird College for Women, Lahore. She can be reached at aiysha.safdar@kinnaird.edu.pk.

[*] MPhil Scholar, International Relations Department, Kinnaird College for Women, Lahore. She can be reached at zaibshahzad244@gmail.com.

Introduction

The current global security landscape is undergoing significant and revolutionary changes due to the rapid evolution of technology. The advancements in robotics, artificial intelligence, and digital technology have not only reshaped traditional security frameworks and power structures but also prompted a re-evaluation of established concepts in International Relations. These technological advancements represent more than just incremental progress, they signify a revolution in military affairs, fundamentally altering how nations perceive and respond to security challenges. This article explores the complex connection between the theory of classical realism and technological innovation in international politics, examining how advanced technologies are reshaping the conventional understanding of security and power.

Classical realism, which underscores the anarchic nature of the international system and the continual pursuit of power, offers a crucial lens to interpret these transitions. Traditionally, classical realism focused on state behaviour and power dynamics within an anarchic system. However, the emergence of advanced technology has expanded the scope of security considerations, encompassing environmental, economic, and social factors in governments' strategic calculations. The increasing reliance on advanced technology reflects a broader understanding of power and security, wherein technological superiority is intertwined with geopolitical strategies (Schmidt 2022).

As major nations invest heavily in advanced technologies, they expedite the revolution in military affairs and integrate new elements into their strategic assessments. The digital revolution has brought about significant changes in warfare, where technology has become indispensable to national security and military capabilities. This shift underscores the transformative impact of technological breakthroughs on global security, as governments adapt to new forms of conflicts and heightened threats. The significance of modern technologies in reshaping landscapes of competition and conflict is evident as states navigate the complexities of a technology-driven International System. This transformation emphasises the importance of comprehending the evolving nature of global security in light of technological advancements, representing a complex interplay between contemporary realities and traditional concepts (Kheyrian, 2019).

Moreover, this article presents an exploratory and qualitative study that investigates technological advancements and their implications for global security and modern warfare. The research assessed the influence of these technologies primarily using secondary sources such as reports, scholarly publications, journals, and books. The study aims to contribute to a better understanding of how the technological revolution is influencing the strategic behaviour of key nations and reshaping global security dynamics by integrating classical realism with contemporary technological advancements. The objective of this study is to explore how these digital breakthroughs align with principles of classical realism and how they will improve future global security challenges.

Fundamentally, the rapid advancement of technology is reshaping global security dynamics, presenting new threats and opportunities to governments. Analysing these digital breakthroughs through the lens of classical realism reveals that the nature of security and power is undergoing fundamental changes, impacting how nations engage in conflict and shape their strategic behaviour. This paradigm shift not only reaffirms the relevance of classical realism but also underscores the necessity of adapting our understanding of global security in an era characterised by technological advancements.

From Realism to Classical Realism: A Theoretical Analysis

The realist perspective in international relations became more important after the World War II and the waning of idealism in the late 1930's and early 1940's. The theory of realism focuses on the competitive and conflict-driven aspects of global politics. It states that nations are the main actors that are responsible for protecting their national objectives, power, and security in the international system. The theory of realism has a deep philosophical history, with roots that can be traced back to ancient scholars like Kautilya and Thucydides, whose writings are based on statecraft, war, and power that echo present-day realist principles. Machiavelli's "The Prince" further developed realist ideas by stressing the pragmatic pursuit of political stability and security, even at the expense of ruthlessness. Realists contend that there is anarchy in the international system which lacking a central authority to enforce laws, and that, as rational actors, nations, prioritize survival and national security (Korab-Karpowicz, 2010).

This anarchy fosters a competitive environment where governments, akin individuals engage in aggressive and self-interested behaviour, often disregarding legal and moral constraints to protect and advance their interests. Moreover, the theory of classical realism emerged as a response to the chaotic conditions of the 20th century and focuses on self-interest and power as key factors in explaining state behaviour in the international system. It underscores human nature as the primary motivator behind power conflicts which forecast the actions of a state, with an emphasis on national interest, power, and security.

This perspective underscores the inherent competition among nations, as well as their pursuit of dominance. It forms a robust basis for comprehending how advancements in technology in warfare, mirror and intensify power struggles among states. In contrast to other theories that emphasise cooperation or social construct, classical realism presents a pragmatic viewpoint on the competitive nature of global security within the realm of digital innovation. As such, it is well suited for examining how nations leverage technological advancements to expand their influence and power (Heriamsal, 2023).

Furthermore, advocates of classical realism like Hans Morgenthau and Thomas Hobbes, contend that human behaviour is inherently self-interested and driven by the pursuit of power and security, which is demonstrated through military strength, economic dominance, and political influence. States primarily act in their interests, prioritizing border security, economic expansion, and political sovereignty, often leading to conflict and competition. Classical realists maintain that the egoistic nature of individuals shapes state behaviour and reject the notion of an ideal international order, viewing conflict as an inherent aspect of the international system. They harbour scepticism towards international treaties and organizations, asserting their futility due to governments prioritizing their national interests and adhering to international law only when it aligns with their interests (Patel, 2020).

Evolution of the Concept of 'Security'

The concept of security has evolved significantly over time, initially focusing on military defence and territorial safeguarding. As described by Barry Buzan, "Security is understood as the pursuit of freedom from threats and the capacity of states and societies to preserve their independent identity and functional integrity against perceived hostile forces" (Buzan, 1991). Presently, security encompasses broader dimensions such as social cohesion, economic prosperity, protection of individual rights, political stability, and environmental stability.

This inclusive approach acknowledges the interconnected nature of global crises and underscores the necessity of coordinated solutions. Contemporary security frameworks recognise that issues in one part of the world can impact global stability, thus requiring cooperative and collaborative responses to transnational menaces such as cybercrime, organized crime, and terrorism. The changes demonstrate a wider recognition that the security of a nation is closely connected to global security, requiring collaborative actions that go beyond conventional military strategies (Wallace, 2019).

Revolution in Military Affairs: Changing the Definition of Security and Transforming the Notion of War

The idea of security has experienced significant changes because of the Revolution in Military Affairs (RMA), which has been driven by rapid advancement in technology in military capabilities. RMA represents periods of transformation characterised by the emergence of new technologies and doctrines that redefine the nature of warfare, similar to historical milestones such as the introduction of gunpowder and nuclear weapons. Each RMA brings about new defensive capabilities, ethical challenges, and vulnerabilities, which also highlight the complex relationship between innovation and security (Cordesman, 2014). The table outlines the historical progression of military technology, highlighting significant advancements and their impact on warfare. It begins with the formation of permanent armies funded through taxation and financial institutions, marking the shift from irregular conscriptions to centralised governance. This transformation is known as the first RMA, brought stability and control, enabling centralized authority to conduct large-scale warfare.

Military Revolution	Implications
First Revolution	
Westphalian System	Taxes for financing war, revenue generation, professional militaries, and banking
Second Revolution	
French Revolution	Large-scale armies with conscription, levy on masses, and national mobilization
Third Revolution	
Industrial Revolution	Large-scale economic exploitation, standardization, and mass production
Fourth Revolution	
World Wars I and II	Combined arms, jets, carriers' bombers, and armoured blitzkrieg
Fifth Revolution	
Nuclear Revolution and Missiles	Intercontinental ballistic missiles and nuclear weapons
Sixth Revolution	
Information Revolution	Cyber levy on masse by violent extremists, connectivity, imagery, command and control, and instant global reach
Seventh Revolution	
Autonomous Revolution	Machine and deep-learning programs, self-organizing defensive systems, big data analytics, swarm of robotic vehicles in multiple domains, automated weapons, and autonomous weapons

Table 1: *Revolution in Military Affairs* (Morton, 2020).

The text discusses the historical evolution of military affairs and highlights significant developments such as the French Revolution, then moving forward to World War I and II, and the development of nuclear weapons. It outlines the ongoing 7th Revolution in Military Affairs, characterised by independent weaponry, artificial intelligence, and advanced robotics. While these technologies enhance combat capabilities, they also raise ethical concerns and the risk of autonomous escalation.

Perspective of Classical Realism on the Role of Technological Advancements

The dynamics of politics are undergoing significant changes due to two major factors: the shifting international power balance and the technological revolution. The US, once a dominant power following the Cold War, is now facing various challenges and competitors. At the same time, advancements in telecommunications and computers have increased global inter-connectedness and given rise to new threats, such as cyber assaults. From a classical realist perspective, the technological advancements of the 21st century exemplify how governments utilise technology to achieve national interest, ensure state security, and gain power in the realm of international affairs (Kegley, 2021).

Quest for Power and Technological Competition In the 21st Century

The book "The Pursuit of Power and Technological Competition in the 21st Century" delves into the intricate interplay between technology, military strength, and global diplomacy from the perspective of classical realism. William H. McNeill's influential work, "The Pursuit of Power," explores the historical impact of technological advancements on power dynamics and military strategy. The ceaseless drive for supremacy through innovation has profoundly reshaped global power dynamics and economies (McNeill, 1982). Presently, technological competition, particularly in the realms of AI and Lethal Autonomous Weapons Systems, is a manifestation of this pursuit.

Nations are allocating resources towards AI-enabled weaponry, cyber capabilities, and space technologies to bolster their strategic advantage. Cyber warfare, cognitive warfare, and advanced robots all illustrate the transformative impact of technology on conflict and power dynamics (Roland, 2009). Despite technological progress, nations' core objectives such as sovereignty, territorial integrity, and self-preservation remain unwavering, reflecting the enduring principles of classical realism. The ongoing evolution of military technology underscores the perpetual quest for power and security in the context of international relations.

Dilemma of Security: How Competition for Arms Race Escalated in the Era of Technological Advancements

The concept of security dilemma, a fundamental element of classical realism, underscores the paradox in which a state's efforts to enhance its security are perceived as threats by other states, leading to a competitive arms race. The advent of advanced technology has exacerbated this issue, with nations responding to perceived threats by investing in new military capabilities, resulting in a technological arms race. States continually seek superior weaponry, spanning from nuclear armaments to AI, LAWS, cyber capabilities, and military robotics, to protect their national interests and assert dominance. This technological competition has heightened instability and mistrust within the international system (Kovarsky, 2006). Consequently, there is an urgent requirement for responsible management of military technology and the formulation of long-term security strategies in the 21st century.

Role of US, China and Russia – Concerning Technological Advancements

The US, China, and Russia are leading in technological advancements and invest significantly in R&D to drive innovation in areas such as space technology, AI, and cyber capabilities. R&D spending plays a crucial role in a country's innovation and competitive edges, impacting various sectors including science, technology, engineering, and defence. The US allocates the highest R&D expenditure ($467.5 billion), followed by China ($370.6 billion) and Russia ($39.8 billion) (Desjardins, 2018). Despite comparatively lower defence budgets, Russia's strong military-industrial complex, historical technological innovation, strategic nuclear position, and foreign policy underscore its global security significance, necessitating recognition alongside China and the US.

➢ Russia

Russia is actively pursuing advanced technology to enhance its military capabilities, particularly with the deployment and development of military systems and strategic technology such as the S-400 Triumf Air Defence System. Russia has also heavily invested in AI, quantum computing, cyber capabilities, and space technologies to increase its economic and geo-political power (Cook, 2023). However, these efforts have created a security dilemma, as they may be perceived as a potential threat to the security of other states. The purported involvement of Russia in the 2016, US presidential elections and its cyber-attacks on US essential infrastructure have increased security challenges in the international system leading states towards security dilemma. This has prompted the affected nations to implement defensive actions and cyber projects, intensifying the competition in the global system (Atta, 2018).

➢ China

The rapid technological advancements in China have had a significant impact on the global power equilibrium. This progress is the result of a mix of investment from government policies, the private sector, and a strong emphasis on innovation. China's ambitious initiative "Made in China 2025" represents its aim to achieve technological superiority in vital sectors, such as AI and military robotics. This has raised concerns about cyber capabilities and has triggered an international competition focused on space exploration, cyber security, and hypersonic missiles. Moreover, China's demonstration of advanced weaponry, like DF-17, has intensified rivalry among major nations especially raising security concerns in the US (Maizland, 2020).

➢ United States

The robust commitment of the US to progress cutting-edge technology, particularly AI, for both military and economic objectives, is clearly shown through significant funding for the AI initiatives within the Department of Defence, including the Joint Artificial Intelligence Centre (JAIC) and Project Maven. The country also addresses cyber security concerns by establishing the US Cyber Command and investing in Unmanned Aerial Vehicles (UAVs) for military operations. Furthermore, the US is actively engaging in an arms race, particularly focusing on hypersonic technologies. Overall, these efforts signify the US dedication to technological advancement, aiming to uphold its status as a dominant global power (William, 1989).

Technological Advancements: Redefining the Dynamics of Global Security

The current global landscape is witnessing an unparalleled surge in digital advancements, driven by various contributing factors such as the heightened cost-effectiveness and accessibility of cutting-edge computing equipment, the proliferation of high-speed internet, and the explosion of data stemming from an increasingly interconnected society. This surge is primarily steered by pivotal technologies including quantum computing, Machine Learning (ML), and AI. AI and ML are instrumental in enabling autonomous data processing and decision-making, thereby spearheading revolutionary, finance, and defence.

The impact of IoT is further magnified through the creation of extensive networks of interconnected devices, enhancing automation and efficiency, albeit accompanied by pronounced privacy and security considerations (Yannakogeorgos, 2012). With the escalating dependence on digital infrastructure and the concurrent rise of cyber threats, cybersecurity has rightfully emerged as a leading priority. Furthermore, the potential of quantum computing to deliver substantial advancements is matched by the challenges it presents in security and scalability. In essence, this digital surge is affecting transformative changes in societal, economic, and security realms, signifying a paradigm shift in the influence of technology on the world (Horowitz, 2020).

Technological Surge: Key Components

The current rise of digitalisation, marked by the swift expansion of technology into every facet of life, is leading to a significant change in the global landscape. Several critical factors drive this technological surge, each with major security implications. A comprehensive analysis of these factors is discussed below:

➢ Information Warfare and Cyber Security

In the modern era, the protection of digital assets and the management of information warfare are of the utmost importance for ensuring the security of digital infrastructure, preserving the integrity of data, and thwarting malicious attacks. Cyber security is crucial for defending data against unauthorised disruptions and access, while information warfare strategically utilises information and communication technologies (ICTs) to shape perceptions and achieve geopolitical aims. The US is at the forefront of cyber security efforts, with organisations such as the Cyber Security and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) taking the lead.

The US Cyber Command conducts cyber operations to counter threats from both non-state and state actors. Russia combines defensive cyber security measures with offensive capabilities, leveraging cyber operations to target critical infrastructure and conduct propaganda campaigns. China, as part of its national security strategy, prioritises cyber security by enacting legislation and implementing measures to protect digital infrastructure and combat cyber threats. Additionally, China utilises information warfare tactics, including online propaganda and censorship, to shape global narratives (Iasiello, 2021).

➢ Machine Learning and Artificial Intelligence (AI)

AI and ML play a critical role in the ongoing digital revolution, significantly impacting decision-making processes and global security dynamics. AI systems perform tasks that traditionally require human intellect, while ML a subset of AI, enables computers to adapt through the use of statistical models and algorithms. The increasing integration of artificial intelligence and machine learning into military systems and intelligence practices have had a profound effect on national security and defence strategies (King, 2024). In the US, efforts such as the Department of Defence's Joint Artificial Intelligence Centre (JAIC) and Project Maven underscore the promotion of AI in cybersecurity, predictive analytics, and autonomous systems. Meanwhile, Russia is prioritising AI in military modernisation, with the Advanced Research Foundation (ARF) developing AI-powered autonomous weapons and unmanned aerial vehicles (Johnson, 2019). China, renowned for its AI research, is incorporating AI into the People's Liberation Army command and control systems, information warfare capabilities, and unmanned systems, supported by its National Artificial Intelligence Development Plan.

➢ Internet of Things (IoT)

The technological revolution is empowered by the IoT and connectivity, enabling real-time communication among objects, sensors, and systems. IoT technology encompasses a network of interconnected devices that enhances national security by protecting critical infrastructure, enhancing situational awareness, and optimising operations. In the US, IoT is utilised for battlefield sensors, unmanned systems, and logistics operations thereby enhancing military capabilities and enabling remote asset monitoring (Gotarane, 2019). Russia is integrating IoT into industrial automation and defence, deploying sensors, network devices, and surveillance cameras in military locations and urban infrastructure to bolster resource management and situational awareness. China leverages IoT for smart grid systems, industrial automation, military logistics, and command and control systems, leading to improved operational efficiency and decision-making (Morelli, 2016).

➢ Quantum Computing

The field of quantum computing has the potential to revolutionise computational capabilities with its exceptional capabilities. Key to this potential is quantum bits (qubits), which can exist in multiple states simultaneously, enabling parallel computing and significant advancements in cryptography, code-breaking, simulations, and optimisation. Russia, the US, and China are very heavily invested in quantum computing research and development for various applications, including quantum-resistant encryption, quantum key distribution (QKD), cryptography, and quantum-enabled sensors for military applications. These advancements have far-reaching implications for national security and cyber security (Krelina, 2021).

Implications of the Technological Surge on Global Security

The rapid progress of advanced technologies has important consequences for global security as it amplifies the abilities of both governmental and non-governmental entities in different areas. It encompasses a broader range of military uses, such as cyber warfare and autonomous weapon systems, UAVs, information collection, and advanced monitoring, especially through the use of drones. Recognising these outcomes is vital for dealing with the increasing security risks and creating effective solutions in the digital age.

➢ Enhanced Military Applications

The rapid advancements in digital technology have significantly accelerated the development and utilisation of autonomous weapons systems, fundamentally transforming the global landscape of military capabilities. Autonomous weapons, including unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), robotic systems, and autonomous drones, leverage advanced algorithms and sensors to operate independently of direct human oversight. These systems offer advantages in terms of speed, precision, and stamina, as they can perform tasks such as reconnaissance, target acquisition, surveillance, and offensive operations with minimal human intervention (Rashid, 2023). Nevertheless, their deployment raises profound ethical and practical considerations, encompassing issues of accountability, human control, and unforeseen consequences, thus prompting scrutiny of international treaties and regulations.

Moreover, the digital revolution has endangered the emergence of cyber warfare, where both state and non-state actors leverage cyber capabilities for strategic, disruptive, and covert purposes (Cummings, 2017). Cyber warfare techniques cover a variety of actions, including information manipulation, cyber spying, and cyber-attacks. Nation backed cyber assaults focus on military communications, crucial systems, private sector organisations, and government networks, aiming to disrupt operations, steal data, or cause harm to opponents. Instances of such activities involve DDoS attacks, data breaches, the use of malicious software, and ransomware offensives, often carried out by state entities or cybercriminal factions with geopolitical goals in mind (Kuo, 2022).

➢ Surveillance and Intelligence Gathering

Technological advancements have transformed the methods of intelligence gathering and surveillance, granting unparalleled access to information and understandings that enhance decision-making and assessment of threats. Tools such as social media monitoring, sensors, drones, CCTV cameras, satellites, and data analytics allow for the real-time monitoring and examination of activities, movements, and conversations. The advanced technologies are used by governments to enforce law, protect national security, manage borders, and counter-terrorism. For instance, drones equipped with high resolution cameras are used for aerial surveillance and border control, while satellite images offer crucial intelligence about military operations (Marwala 2023). In intelligence collections, digital technologies bolster Signals Intelligence (SIGINT), Image Intelligence (IMINIT), Human Intelligence (HUMINT), and Open-source Intelligence (OSINT). AI-driven analytics scrutinise vast volumes of data, uncovering patterns and irregularities to generate actionable insights for decision-makers (Burch 2020).

➢ Cyber Warfare and Critical Infrastructure Vulnerabilities

The rise of cyber warfare has revealed weaknesses in global critical infrastructure systems, which have become more reliant on digital technology. Cyber assaults on these systems could lead to significant disturbances and financial losses, posing a threat to national interests. For instance, the Stuxnet Virus, uncovered in 2010, targeted Iran's nuclear enrichment facilities (Lindsay, 2013). Another case in 2017 WannaCry ransomware attack, impacted hundreds of thousands of computers worldwide, underscoring the far-reaching consequences of cyber threats. The increasing inter-connectedness of infrastructure through the 'Internet of Things' has broadened the potential scope of cyber attackers (Cavelty, 2007).

➢ Information Manipulation and Influence Operations

In today's time of advanced technologies, there has been an increase in information manipulation, with which the opinion of public can be influenced and misinformation can be easily spread through the use of social media and other online platforms. Both non-state actors and state actors make use of these social media platforms to control narratives, divide populations, undermine democratic processes, and divide populations. For instance, the involvement of the Russian government in the 2016 US presidential elections, false social media accounts, and troll farms were used to spread controversial information to create political turmoil. Such manipulation of information has the potential to incite social unrest, erode people's trust in democratic institutions, and worsen political tensions. (Hwang, 2019).

➢ Blurring of Boundaries Between Physical and Digital Threats

The convergence of traditional security and cyber risks due to incorporation of advanced technologies has given rise to hybrid threats. These threats encompass economic coercion, cyber capabilities, military tactics, and information warfare. For example, Russia used a hybrid warfare strategy in Ukraine, such as propaganda, hacking, support for rebels, and attacking its critical infrastructure. Additionally, dual-use technologies like drones, originally designed for civilian use, can be adapted for military purposes, which blurs the line between military and civilian functions. Moreover, the widespread use of digital communication channels has facilitated the spread of disinformation and enabled influence operations, allowing individuals to distort information and erode public trust (Malik, 2004).

➢ Disruptive Technologies and Asymmetric Warfare

The advancement of disruptive technology has empowered non-state actors to effectively utilise asymmetric warfare strategies. Organisations like the ISIS have leveraged drones armed with explosives to carry out precise attacks, reducing their own risk while gaining a technological advantage. Similarly, non-state actors and criminals have embraced new tactics to carry out assault and ransomware attacks on civilians and also on vital infrastructure, leading to extensive financial damage and disruption. Unlike, traditional military operations, these cyber-attacks are carried out from secretive and distant positions, allowing attackers to aim at important networks with considerable immunity (Kunstler, 2011).

➢ Dual-Use Technologies Implications

The potential for misuse of technologies that can serve both military and civilian purposes presents significant challenges due to their dual nature. These dual-use technologies can be exploited by non-state and state actors for military purposes, to carry out criminal acts, and to circumvent export regulations. The use of drones, biotechnology, quantum computing, AI, and cyber tools, can enhance strategic capabilities, on the other hand, they have the potential to fuel an arms race and disrupt strategic stability. Satellites and other civilian technologies can be used for military objectives, and non-state actors could exploit these technologies for harmful activities (Ballantine, 2013).

➢ Potential for Escalation in Conflicts

The rapid digitalisation of modern society has introduced new risks regarding conflict escalation. The inter-connected, high-speed nature of digital operations and the potential for unforeseen consequences have heightened concerns around escalation. Cyber operations are often shrouded in secrecy, and issues related to attribution can quickly lead to heightened tensions if critical infrastructure is targeted, potentially resulting in retaliatory actions. Additionally, the use of autonomous technology, such as drones, introduces the risk of unintentional escalations due to technological malfunctions or misinterpretation of data. Information warfare, including tactics such as disinformation and propaganda, has the potential to exacerbate existing tensions and hinder diplomatic efforts. Both state and non-state actors utilise digital technology in proxy conflicts, contributing to regional instability and posing significant security risks (Patomaki, 2008).

➢ Emerging Threats in the Space Domain

The rapid advancement of anti-satellite and space-based technology has raised concerns about the potential for future space warfare and its implications for global security. The 2007 test of anti-satellite missiles by China highlighted the significant danger posed by space debris, which jeopardises the functioning of space missions and satellites. Moreover, Russia's advancement in creating manoeuvrable and surveillance satellites based in space brings about added challenges and complexities, including issues related to avoiding collisions, understanding the space station, and preventing satellite interference. (Porras, 2022).

➢ Environmental Impact and T echnological Fallout

The swift progress of space-based and anti-satellites technologies has sparked concerns about potential future space warfare and its impact on global security. The creation of space-based surveillance by Russia has introduced new challenges leading to concerns about satellite interference, and collision avoidance. Additionally, China's demonstration of an anti-satellite missile test in 2007 drew attention to the crucial threats that are posed by space debris to operational satellites and space missions. (Caldwell, 1988).

➢ Strategic Imbalance and Regional Instability

The spread of advanced military technologies, such as the positioning of the US THAAD systems in South Korea, has caused strategic imbalance and instability in the region. Development of these advanced technologies can increase tensions with neighbouring countries, as seen in China's worries about THAAD's effect on its regional power dynamics and missile defence capabilities. These deployments can impact how security is perceived and have the potential to increase regional competition among states thus increasing the chances of instability in the International System. The establishment of long-range precise missiles adds to the complexity of security dynamics, potentially leading to an arms race and increased tensions. (Ford, 2020).

➢ Economic Costs and Resource Allocation

The cost of developing advanced military technologies can affect the allocation of resources, potentially conflicting with important social programs and infrastructure projects. For instance, the US military budget gives priority to investing in advanced weapons and R&D, eventually result in redirection of funds from areas like environmental stability, education, and healthcare. Additionally, substantial defence spending may overshadow long-term aspirations for sustainable development and economic diversification. The economic effects go beyond initial costs and encompass maintenance and operational expenses, placing strain on national budgets and constraining the ability to address broader socio-economic and environmental issues. Achieving a balance between defence requirements and other economic objectives requires a thorough assessment of opportunity costs, long-term strategic planning costs and long-term strategic planning to ensure alignment with national interests and sustainable development goals (Skaperdas, 2007).

➢ Humanitarian Consequences and Civilian Vulnerability

The utilisation of advanced military technology, including precision-guide munitions and Unmanned Aerial Vehicles (UAVs), in densely populated areas raises significant humanitarian concerns. Despite their intended purpose to enhance precision and reduce collateral damage, these technologies can still lead to civilian casualties and the destruction of essential infrastructure such as hospitals and schools. In complex combat scenarios, the precision of modern weaponry may not always prevent harm, resulting in severe consequences for civilians such as loss of life, displacement, psychological trauma, and disruption of critical services. This gives rise to ethical and legal dilemmas related to international humanitarian law (IHL) and the protection of individuals in conflict zones (Khorram-Manesh, 2023). Moreover, the use of modern weaponry by both state and non-state actors has the potential to escalate violence, hinder humanitarian efforts, exacerbate humanitarian crises, and complicate conflict resolution processes.

Conclusion

The confluence of classical realism and technological progress has created a multifaceted and continuously changing environment in the field of global security. Powerful nations like China, Russia, and the US are using these modern technologies to strengthen their strategic capabilities, resulting in significant changes to the traditional notion of security and power. This technological revolution encompasses advanced robotics, cybersecurity, lethal autonomous weapons, digital infrastructure, and artificial intelligence as it heightened the rivalry among states but also introduced unprecedented levels of threats and challenges.

The integration of these technologies into military and strategic frameworks signifies the change from traditional warfare and a move towards a more comprehensive understanding of security, where digital and physical threats intersect. An evaluation of the implications of these advancements from the viewpoint of classical realism theory highlights the pursuit of technological dominance as a crucial factor in the international system. As technology advances, the distinction between traditional and contemporary security considerations is set to become increasingly blurred, necessitating a re-evaluation of policies and strategies. The ongoing interplay between established power dynamics and technological progress is changing the future of global security, requiring adaptability and foresight from all main players on the world stage.

Disclosure Statement

No potential conflict of interest was reported by the authors.

References

Atta, D. V. (2018). Why They Did It: The Context of Russian Interference in the 2016 Presidential Elections. *SSRN*. https://dx.doi.org/10.2139/ssrn.4117812

Ballantine, W. C. (2013). International Friction and Cooperation in High-Technology Development and Trade: Papers and Proceedings. *National Academies Press*, Chapter 6, pg. 130.

Burch, J. (2020). Operationalizing Intelligence Collection in Complex World: Bridging the Domestic and Foreign Intelligence Divide. *Global Security and Intelligence Studies*, 5(2).

Buzan, B. (1991). New Pattern of Global Security in the Twenty-First Century. *International Affairs (Royal Institute of International Affairs)*, 67(3), 431-451.

Caldwell, L. K. (1988). Environment Impact Analysis (EIA): Origins, Evolutions, and Future Directions. *Taylor & Francis.*

Cavelty, M. D. (2007). Critica Information Infrastructure: Vulnerabilities, Threats, and Responses. *Disarmament Forum*, Vol. 3, pp. 15 -22.

Cook, E. (2023). Russia's S-400 Air Defense Systems are Being Cut to Shreds. *Newsweek*.

Cordesman, A. H. (2014). The Real Revolution in Military Affairs. *Center For Strategic and International Studies*. https://www.csis.org/analysis/real-revolution-military-affairs

Cummings, M. L. (2017). Artificial Intelligence and the Future of Warfare. *Catham House, The Royal Institute of International Affairs*.

Desjardins, J. (2018). Visualizing How Much Countries Spend on R&D. *Visual Capitalist*.

Ford, C. A. (2020). Strategic Stability and the Global Race for Technology Leadership. *Arms Control and International Security Papers*.

Gotarane, V. &. (2019). IoT Practices in Military Applications. *In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, (pp. pp. 891-894. IEEE). https://doi.org/10.1109/ICOEI.2019.8862559

Heriamsal, K. (2023). The World Today: Realism Still Relevant (Security Context). *Modern Diplomacy*.

Horowitz, M. C. (2020). Do Emerging Military Technologies Matter For International Politics? *Annual Review of Political Science*, Vol. 23, pp. 385 -400. https://dx.doi.org/10.1146/annurev-polisci-050718-032725

Hwang, T. (2019). Maneuver and Manipulation: On the Military Strategy of Online Information Warfare. *USAWC Press*.

Iasiello, E. (2021). What is the Role of Cyber Operations in Information Warfare. *Journal of Strategic Security*, 14, no. 4: 72-86.

Johnson, J. (2019). Artificial Intelligence and Future Warfare: Implications for International Security. *Defense & Security Analysis*, 35(2), 147-169. https://doi.org/10.1080/14751798.2019.1600800

Kegley, C. W. (2021). Realism in the Age of Cyber Warfare. *Ethics and International Affairs*.

Kheyrian, M. (2019). What are the implications of realisms apparent dominance of the study of International Relations? *CGSRS*.

Khorram-Manesh, A. &. (2023). Civilian Population Victimization: A systematic Review Comparing Humanitarian and Health Outcomes in Conventional and Hybrid Warfare. *Disaster Medicine and Public Health Preparedness*.

King, A. (2024). Digital Targeting: Artificial Intelligence, Data, and Military Intelligence. *Journal of Global Security Studies*, Volume 9, Issue 2. https://doi.org/10.1093/jogss/ogae009

Korab-Karpowicz, W. J. (2010). Political Realism in International Relations. *The Standford Encyclopedia of Philosophy*.

Kovarsky, L. (2006). A Technological Theory of the Arms Race. *Indiana Law Journal*. https://www.repository.law.indiana.edu/ilj/vol81/iss3/3

Krelina, M. (2021). Quantum Technology for Military Applications. *EPJ Quantum Technology*, 8, 24. https://doi.org/10.1140/epjqt/s40507-021-00113-y

Kunstler, B. (2011). Extreme Asymmetric Warfare of the Future: Insidious, Inevitable, Iconoclastic. *World Future Review*.

Kuo, K. (2022). Dangerous Changes: When Military Innovation Harms Combat Effectiveness. *International Security*, 47(20): 48-87.

Leiter, B. (2001). Classical Realism. *JSTOR*.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3), 365-404. https://doi.org/10.1080/09636412.2013.816122

Maizland, L. (2020). China's Modernizing MilitarY. *Council on Foreign Policy*.

Malik, A. (2004). Technology and Security in the 21st Century. *SIPRI Research Report*.

Marwala, T. (2023). Militarization of AI has Severe Implications for Global Security and Warfare. *UNU Centre*.

McNeill, W. H. (1982). The Pursuit of Power: Technology, Armed Force, and Security Since A.D. 1000. The University of Chicago Press.

Morelli, M. T. (2016). Leveraging Internet of Things within Military Network Environment-Challenges and Solutions. *IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp. 111-116.

Morton, A. (2020). To What Extend Will the Development of Artificial Intelligence Change the Nature of War and What are the Strategic Implications for the United Kingdom? *University of Exeter*.

Patel, A. (2020). International Relations: Classical Realism vs Neorealism. *Medium*.

Patomaki, H. (2008). The Political Economy of Global Security: War, Future Crsisi, and Changes in Global Governance. *Routledge*.

Porras, D. V. (2022). Space as a Competition Domain: Threats and Opportunities. *Journal of International Analytics*.

Rashid, A. B. (2023). Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges. *International Journal of Intelligent Systems*. https://doi.org/10.1155/2023/8676366

Roland, A. (2009). War and Technology. *The Foreign Policy Research Institute*.

Schmidt, B. C. (2022). Realist International Theory and the Military. *Springer Link*.

Skaperdas, M. (2007). Economic of Conflict: An Overview. *Handbook of Defense Economics*.

Wallace, W. C. (2019). Global Security. *Springer Link*. https://doi.org/10.1007/978-3-319-74336-3_52-1

William, J. C. (1989). The Role of the US Government in Encouraging Technological Innovation. *Canada-US Law Journal*, Volume 15.

Yannakogeorgos, P. A. (2012). Internet Governance and National Security. *Strategic Studies Quarterly*, 6(3), 102-125.