

Social Sciences Spectrum

A Double-Blind, Peer-Reviewed, HEC recognized [Y-category](#) Research Journal

E-ISSN: [3006-0427](#) P-ISSN: [3006-0419](#)

Volume 04, Issue 04, 2025

Web link: <https://sss.org.pk/index.php/sss>



Check for updates

Artificial Intelligence as the New Security Dilemma: A Neorealist Analysis

Adnan Saghir¹

M Phil International Relations, Muslim Youth University,
Islamabad, Pakistan

Correspondence Author: dnnssaghir@gmail.com

Dr. Asia Karim²

Assistant Professor, Riphah Institute of Public Policy,
Riphah International University, Islamabad, Pakistan

Email: asia.karim@riphah.edu.pk

Dr. Raziq Hussain³

Assistant Professor, Department of International Relations,
MY University, Islamabad, Pakistan

Article Information [YY-MM-DD]

Received 2025-08-25

Revised 2025-09-13

Accepted 2025-10-27

Citation (APA):

Saghir, A., Karim, A & Hussain, R. (2025). Artificial intelligence as the new security dilemma: A neorealist analysis. *Social Sciences Spectrum*, 4(4), 96-116. <https://doi.org/10.71085/sss.04.04.364>

Abstract

This paper evaluates the use of AI in military applications in autonomous weapons, intelligence surveillance reconnaissance, cyber warfare, and command-control systems, including its contribution to power distribution. The conflict between Russia and Ukraine is an illustration of asymmetric AI approaches with Russia using mass-produced AI-powered drones to maintain a continuous aerial campaign and Ukraine deploying precision AI-controlled strikes and this is the way the new technologies are changing the modern war. The modern AI geopolitics is dominated by U.S.-China rivalry, and structural concerns support competition instead of collaboration. Russia engages in asymmetric policies that are combining AI and the nuclear doctrine, and the secondary powers are building regional capacity, increasing risks of proliferation. The entire structure of anarchic is a limiting factor in the successful governance of AI- there is a problem of verification (as well as enforcement) and relative gains (that do not allow full arms control). Even though there is still limited cooperation in existential risks, core competitive dynamics prevail, which requires policies to balance strategic hedging and selective cooperation.

Keywords: Artificial Intelligence, Weapons, Russia and Ukraine, Modern War, U.S.-China Rivalry.



Content from this work may be used under the terms of the [Creative Commons Attribution-Share-Alike 4.0 International License](#) that allows others to share the work with an acknowledgment of the work's authorship and initial publication in this journal.

1. Introduction

The rise of the transformative form of military technology, artificial intelligence, is one of the most significant events in international security today. Profoundly changing the balance of military potential among states and redefining the strategic competition of the twenty-first century, AI systems, including machine learning algorithms, autonomous decision-making platforms, and intelligent weapons systems, are transforming the distribution of military capabilities among states. According to Horowitz (2018), AI is one of the possible game-changing technologies that can be compared to nuclear arms or precision-guided munitions in terms of their threats to warfare and deterrence. The dual-use characteristic of the technology, the pace of its development, and the integration of all spheres of the military have become the reasons behind the intense competition among the great powers aiming to use AI as a strategic advantage. Autonomous drones, intelligent surveillance systems, AI-enhanced cyber potential, and algorithmic decision support are operationalised at an increasing rate, with immense implications on international stability.

In a neorealist approach, AI competition should be conceptualised in terms of structural imperatives of the anarchic international system. Since Waltz (1979) has laid the groundwork in his classic study of structural realism, the lack of some central authority in global politics forces states to adopt self-help as a mode of survival and relative power accumulation. States cannot overlook technological advances that may give enemies the upper hand in this environment. AI is precisely such an innovation, a power amplifier that can significantly modify the balance of power between rival states. In recent literature, the neorealist conceptualisations have been extended to the dynamic of emerging technologies, most notably by Johnson (2019), exploring the effects of AI in increasing security dilemmas due to its obscurity, velocity, and utility in both applications. The security dilemma, when the defensive actions of another state are perceived as offensive actions by other states, is especially acutely manifested in the context of AI competition since the boundaries between the offensive and defensive capabilities are, in this case, inherently unclear.

The Russia-Ukraine conflict is a landmark event in the history of the military; the use of artificial intelligence and autonomous systems has become the key to the asymmetric warfare strategy. The two aggressors use AI-enhanced drones in very different ways: Russia by mass-producing and using in high volume, Ukraine by targeting with precision and creating more innovations in operations and essentially changing the battles of the modern world. The incident resembles the general trends of the Russia-Ukraine conflict, in which both parties have utilised numerous independent systems, AI-driven intelligence tools, and algorithmic warfare proficiencies since 2022 (Boulanin et al., 2020; Payne, 2021).

The main idea of this article is to focus on AI technologies in terms of a neorealist theory, the structural aspects of the international system (anarchy, the capabilities distribution, and the relative gains issue) that stimulates an AI arms race between the great powers. It is further divided into a series of steps: defining the concept of neorealist theory and applying it to new technologies, exploring the issue of AI and its use in the military, exploring its strategic consequences, discussing the mechanisms of uncertainty, first-movers, and arms race as the sources of security dilemma, evaluating the new challenges posed by AI that are not available to the old security dilemma, assess the challenges that great power competition presents in developing AI, and

considering the possibilities of governance within this structural constraint. In applying the neorealist theory to the competition of AI, this article sheds light on the structural forces that drive states to competitive and not cooperative strategies with this revolutionary technology.

2. Neorealist Theoretical Framework

2.1 Core Principles

Neorealism or structural realism is a lean but effective theory of international security relations that puts system-level variables first and unit-level traits second. Kenneth Waltz (1979) transformed realist thinking by suggesting that the patterns of state conduct are not defined by human nature or state characteristics but by the construction of the international system. This structure is characterised by anarchy, the lack of a central power on top of the states that have an effective monopoly on applying force. This principle of anarchic ordering is the basic factor in the interaction of states forming a self-help system in which no state can count on the support of others in ensuring its security (Waltz, 1979). Anarchy poses the problem of uncertainty over the intentions of other states, as Mearsheimer (2001) points out; rational actors need to presume evil motives on the part of the potential adversary.

Sharing capabilities among states defines the polarity of the system: the concentration of power in a single state (unipolarity), its division between two superpowers (bipolarity), or its dispersion among several great powers (multipolarity). Waltz (1979) asserted that bipolar systems are more likely to be stable than multipolar setups because they are more likely to assess threat, and they are less likely to have uncertainty about the commitment of the alliances. States do not just gauge their results according to what they acquire but also how their gains are relative to those of their competitor, as Grieco (1988) puts it. Such an issue of relative gain poses significant barriers to cross-border collaboration, especially in areas of security in which the current technical superiority is the technological inferiority of tomorrow, should it be divulged to possible enemies.

2.2 The Security Dilemma in Anarchic Systems

Security dilemma is a tragic event that is brought about by structural anarchy. This was first expressed by John Herz (1950), who noted that the things that measure states do to enhance their own security, such as building military forces, creating alliances, and obtaining new weapons, can, in effect, make other states less secure as they retaliate by doing the same. This is observed even in situations where the states have only purely defensive intentions, because anarchy does not allow the intentions to be checked. According to Jervis (1978), the magnitude of the security dilemma is based on the ability to differentiate offensive and defensive military positions and whether offence or defence is superior.

In neorealism, there is a controversy between the defensive and offensive variants on the motivation of states and their action. Waltz (1979) would maintain the idea of defensive realists, where insecurity is the ultimate motivation behind expansion, and that states aim at security and maintenance of the status quo, not because they are inherently aggressive. Other offensive realists, especially Mearsheimer (2001), argue that great powers are naturally assertive and concerned with maximising relative power and gaining regional hegemony wherever possible. According to Glaser (2010), it generates spirals where the defensive preparations of one state seem threatening to another, which produces a response that confirms the original fears. In times of predominance of offence, competition is more intense because states are in danger of being vulnerable to preemptive attacks.

The security dilemma remains relevant in international relations; as contemporary security concerns indicate. The growing and modernisation processes of the military, cyber power and strategic competition between the major powers show that states' quest towards security is still creating insecurity among themselves even in the twenty-first century. According to Tang (2009), transparency, reassurance measures and the establishment of defensive military postures can ease a security dilemma by clearly indicating non-aggressive intentions. Nevertheless, the success of these solutions will depend on the overall strategic environment and the existence of what Booth and Wheeler (2008) call security communities, in which the states can build the necessary confidence to get out of the logic of the dilemma. It is especially acute in areas that are in transition of power or in regions where there are disputes over territories and where the uncertainty about intentions is grouped with the shift in capabilities, threat perceptions grow, and arms competition intensifies (Christensen and Snyder, 1990).

2.3 Technology and Power Distribution

Technology is a material ability that modifies the balance of power between states, which can instigate systemic instability. As Horowitz (2010) illustrates, military innovations cause gaps in the creation of adoption capacities between early and late adopters, moving the relative power balance. Those states that can utilise the revolutionary technologies successfully can jump over competitors, and those that lag see their security deteriorate. The power transition theory formulated by Organski (1958) and developed by other scholars assumes that the periods of the observed rapid changes in relative capabilities, with the impact of uneven technological advancements, cause dangerous conditions. According to Copeland (2000), preventive war is most hazardous during power changes because states with short-run military superiority have incentives to wage war against their long-term adversaries.

Past experiences demonstrate the revolutionary nature of technology in global security. Nuclear armaments essentially changed the strategic calculations in the Cold War, where the two superpowers became vulnerable to each other, and relative bipolar deterrence prevailed, even though the arms race did not stop (Jervis, 1989). Cyber capabilities have recently created new levels of conflict that have discussed attribution challenges, minimal barriers of entry, and unclear differences between peace and war (Buchanan, 2020). Cyber weapons are used under grey legal jurisdictions, facilitate secret operations and are not easily checked by the conventional arms control mechanisms.

Figure 1: *Neorealist Theoretical Framework*



Source: Created by the Researcher

3. AI as Military Capability: Applications and Strategic Implications

3.1 Defining AI and Its Military Variants

Artificial intelligence refers to the computational systems capable of executing activities traditionally performed by human cognitive capacities, such as perception, reasoning, learning, and decision-making. Machine learning is a core AI concept that helps systems to enhance performance, learn new things through experience, and recognise the trends in data without being told all possible contingencies (Russell and Norvig, 2020). Image recognition, natural language processing, and strategic game-playing have seen breakthrough performance by deep learning, which is based on artificial neural networks with more than one layer, and often human performance is outperformed in a narrow domain (LeCun et al., 2015). Autonomous systems combine AI algorithms with sensors, actuators, and decision-making systems to perform in dynamic settings under minimal human control (Scharre, 2018). These systems can adapt to unstable conditions, move on jagged terrain, and perform missions without constant human direction, a qualitative alteration in military capabilities. The following AI systems are currently being developed as narrow systems adapted to handle only a few functions, instead of general intelligence, which is the defining property of human cognition. Artificial General Intelligence (AGI) hypothetical systems with the ability to reason and think on a human level in various fields are aspirational, even though extensive research on the systems has been conducted (Goertzel and Pennachin, 2007). Nevertheless, the narrow AI systems are sophisticated enough to be used militarily significantly, which causes significant strategic and ethical concerns regarding the ability of human beings to control lethal force (Cummings, 2017).

3.2 Military Applications as Power Resources

The most controversial use of AI in the military is Lethal Autonomous Weapons Systems (LAWS). These systems can recognise, monitor, and interact with targets without human operators deciding on attacks separately and radically change the role of humans in war (Altmann & Sauer, 2017). Autonomous drones, road vehicles and sea platforms incorporating AI targeting algorithms can work in denied environments with no or impractical communication with human controllers. The systems based on the use of AI, known as Intelligent Surveillance and Reconnaissance (ISR), offer the intelligence advantage of gathering, processing, and utilising information more quickly and comprehensively than the enemy. AI algorithms examine satellite imagery, signals intelligence, and open-source data on scales that human analysts cannot study, finding patterns, predicting the behaviour of adversaries and delivering actionable intelligence to commanders (Work & Brimley, 2014). This capability has now taken intelligence to a predictive anticipation rather than a reactive analysis, which gives states strategic benefits. According to Allen and Chan (2017), AI-enabled ISR systems are systems based on a fundamental alteration in the balance of offence and defence due to the impossibility of hiding. Machine learning supports offensive and defensive activities in AI-enabled cyber warfare capabilities, such as automated vulnerability identification, adaptive malware learning defensive actions, and phishing attack generation by AI (Brundage et al., 2018). Systems of command and control that are complemented with AI combine information across these areas, optimise the use of forces, and offer decision support in complex operations to ensure commanders can control larger forces over broader regions than previously (Johnson, 2020).

3.3 Ukrainian Drone Attack on Russian airbase

On June 1, 2025, Ukrainian forces presented one of the boldest military operations of the war, called Operation Spiderweb, and attacked several Russian airbases (Al Jazeera, 2025a; CNN, 2025b). It entailed the deployment of 117 attack drones launched by trucks that were covertly positioned near Russian air bases, and some of whom were in Siberia, thousands of kilometers away in Ukraine (Axios, 2025).

The drone attacks were directed at the Russian military air bases in five regions: Murmansk, Irkutsk, Ivanovo, Ryazan, and Amur (Al Jazeera, 2025a). The Russian airbases have been struck by at least 41 of its heavy bombers, including Tu-95 and Tu-22 strategic bombers, which the Russian employs to launch long-range missiles on the Ukrainian cities (Al Jazeera, 2025b). It was aimed at the Belaya airbase in Irkutsk, which is about 4,300 kilometers away from the Ukrainian border and the Olenya airbase in Murmansk, which is about 1,800 kilometers away from the Ukrainian border (Al Jazeera, 2025a).

The drones were transported by wooden buildings topped with retractable roofs that were trucked, and the roofs were showered with remote control to open at the right time, enabling the drones to take off and hit Russian bombers (CNN, 2025b). The mission involved the drones in the first-person shooting and was equipped with explosives that were smuggled into Russia and planted in the trucks and beneath the roofs of houses (Stern, 2025). It required the Ukrainian President Volodymyr Zelenskyy to personally oversee the attack, which took more than 18 months (NPR, 2025).

The Security Service of Ukraine alleged that the strikes struck Russian military aeroplanes worth a total of \$7 billion and demolished 34 per cent of Russian strategic cruise missile launchers based at air skydocks (Al Jazeera, 2025a). Two US officials interviewed by Reuters revealed that approximately 20 military aircraft were struck during the attack, with ten being destroyed (Wikipedia, 2025). In the video posted by the SBU, the drones were seen nearing dozens of aeroplanes of various kinds in multiple airfields, and the planes were burning and exploding around them (CNN, 2025a).

The strike was regarded as a masterpiece of the special services of Ukraine, where the ability to attack precisely and cause harm or destruction to military aircraft used by Moscow to bomb Ukrainian citizens (CNN, 2025a). The operation demonstrated the vulnerability of Russian major military equipment thousands of miles behind the fighting line. It could have caused a massive blow to Russian capabilities in an aerial cruise missile attack (Stern, 2025).

3.4 Strategic Advantages and Capability Distribution

AI will offer several strategic benefits with respect to relative power positions. The ability of states to synchronise their operations within the decision-making processes and cycles of adversaries by providing speed and efficiency leads to the achievement of dominance due to tempo rather than the presence of firepower (Kania, 2020). AI systems examine circumstances, develop reactions, and carry out activities on timescales that a human operator is incapable of, and they may offer decisive benefits in a high-paced conflict. The decisive competitive aspect of AI-empowered war is the decisional upper hand to make decisions quicker than opponents. Due to the automation of political costs of warfare, casualty-averse publics no longer support military action. States that use autonomous systems risk having fewer staff, so continuous operation is possible in politically viable situations where people would create internal resistance (Kreps,

2016). This may reduce thresholds of utilising force and make it harder to deter aggression because opponents will not count on the sensitivity to casualties to limit aggression. AI surveillance and predictive capabilities allow continuous monitoring of the adversaries, and allow them to foresee their actions. The ones with better AI systems will be able to study the rival movements of armies, anticipate their strategy, and deploy their forces beforehand (Horowitz, 2019). This advantage in asymmetric information directly applies to military performance, where smaller troops can accomplish their tasks against bigger foes, unsupported by the same AI spectrum of capabilities.

4. AI and the Neorealist Security Dilemma

4.1 Uncertainty, Opacity, and the Verification Problem Under Anarchy

Anarchic international politics is the key factor determining AI competition because the situation causes irreducible uncertainty about the capabilities and intentions of adversaries. The current deep learning systems are black boxes; none of their developers understand the inner decision rule, and the neural networks provide predictions based on millions of weighted parameters humans cannot explain (Burrell, 2016). Geist (2016) states that the dual-use aspect of AI capabilities essentially obliterates the separations between offensive and defensive postures, which escalates the dynamics of the security dilemma. The offensive-defensive equilibrium with AI is also always ambiguous; the same computer vision to detect incoming missiles can also control offensive drones.

Difficulties in attribution add confusion in anarchy. In damage caused by AI-enhanced cyber-attacks or autonomous systems, locating the implicated state is impossible (Schneider, 2019). With no central authority, it exacerbates the worst-case thinking- states can suspect their enemies are taking actions hostile to them when evidence is unclear, leading to a spiral dynamic. The verification issue is especially acute in the case of AI technologies. Conventional arms control is based on the number of weapons, surveillance of testing facilities, and facilities, which will remain intangible and can be duplicated, obscured, or easily tampered with using AI (Horowitz and Scharre, 2021). In case of the impossibility of verification, the wise states are forced to assume that adversaries have more developed, more competent, and more powerful AI military systems than indicated by visible means, which forces arms-length building even in situations where the real capabilities are poor (Payne, 2018).

4.2 First-Move Advantages, Arms Racing, and Crisis Instability

AI technologies develop strong structural motivators of preemptive action due to shortening decision-making timeframes. Future conflicts can be decided within minutes or seconds instead of hours or days as AI systems identify threats, develop answers, and take measures more quickly than the human decision loop can (Schelling, 2018). This velocity edge is defensive, which allows a swift reaction to the attack launched, and offensive, which allows the attack to be delivered when the enemy is not ready to respond. Morgan et al. (2020) suggest that this compression results in instability of crisis as both parties become afraid that waiting offers the opponents an upper hand in the first strike, and therefore, the preemption can seem logical in the context of uncertainty (Slayton, 2020). The June 2025 drone attack by Ukraine showed the pace of the work that can be achieved with systems that are supported by AI and the difficulties involved in human intervention when the engagement is rapidly changing (Defence One, 2025).

Regarding AI, arms race (neorealistically) is a possibility and a structural necessity. Survival of

states in anarchy requires self-help and maximisation of relative capability. AI is one of the most outstanding sources that states will face in this scenario because, without competition, they are at a disadvantage in terms of their strategy (Mearsheimer, 2001). Although there is a possibility that global collaboration on AI safety would result in the formation of the absolute benefits of all participants, states fear that cooperation will favour their competitors better, improving their position on the relative front and establishing strong incentives not to share research or limit development (Maas, 2019). The differences in investment impose further strains, wherein China will exert pressure on American technological supremacy because its data collection and government-industry integration will counter the established technology. In contrast, Ukraine will seek AI as an asymmetric capability to balance the conventional superiority of NATO. The dual purpose of AI technology is to raise security externalities, where civilian usage of AI in universities and companies results in innovations that the military can use. States cannot easily decouple civilian advancement and military capabilities, which implies that the rate of military AI development is partially maintained by civilian innovation happening globally, to which the state is not in complete control (Allen and Husain, 2017).

4.3 Misperception, Inadvertent Escalation, and Systemic Instability

The inability to check the capabilities, along with uncertainty about intentions, results in security dilemmas, which AI worsens. The hostile party is not sure that the developments of AI by its opponents are defensive or offensive, precautionary or offensive and such uncertainty, along with high speed and autonomy of AI systems, are factors that add to the threats of unintentional escalation (Amodei et al., 2016). Such mistakes in military actions involving lethal force or strategic weapons will cause disastrous retaliation. Adversarial machine learning - interacting with AI using designed inputs - establishes new offensive and defensive capabilities (Biggio and Roli, 2018).

Cascading failures are also a further threat because complex AI systems deployed across different military fields can be subjected to the effects of failures to spread, i.e., a failure in one system can introduce an unforeseen impact on other systems (Sagan, 2019). The barriers to communication and reassurance that are inherent to anarchy imply that even by noticing the risk of escalation, the states, to communicate the restraint credibly, find it hard to do so. The opponents feel that reassurance is a lie and meant to weaken the guards before an attack, thus making de-escalation difficult once the crisis is underway, especially when AI systems are working fast. Therefore, there is no chance of diplomacy (Glaser, 2010). The above dynamics indicate that AI technologies enhance the legacy security dilemma pathologies and create newer pathologies that the current crisis management mechanisms are unprepared to confront.

5. Unique Challenges: AI's Departure from Traditional Security Dilemmas

5.1 Verification Impossibility, Autonomy, and Rational Actor Erosion

The AI technologies present a significant threat to the conventional arms control methods due to their intangible character. In contrast to nuclear arms or traditional military equipment that may be counted, verified, and tracked using satellites and on-site detection, the capabilities of AIs lie in computer programs, algorithms, and training data that can be quickly replicated, buried in civilian infrastructure, or altered in several hours (Maas, 2019). This software-hardware contrast makes old verification processes irrelevant. As Schneider (2020) points out, states cannot authoritatively check adherence to any possible AI arms control agreements since the very

computational infrastructure used to build civilian systems can also create military AI systems (Horowitz and Scharre, 2021). Neorealist theory presupposes states would be unitary rational actors, focusing on survival. However, AI technologies threaten this initial assumption when the machine makes the key decisions about survival, and it is not under human meaningful control (Sauer & Schornig, 2012). Competitive pressures cause a paradox: states have to give more powers to AI systems or be disadvantaged against those who can afford to do that (Horowitz, 2019).

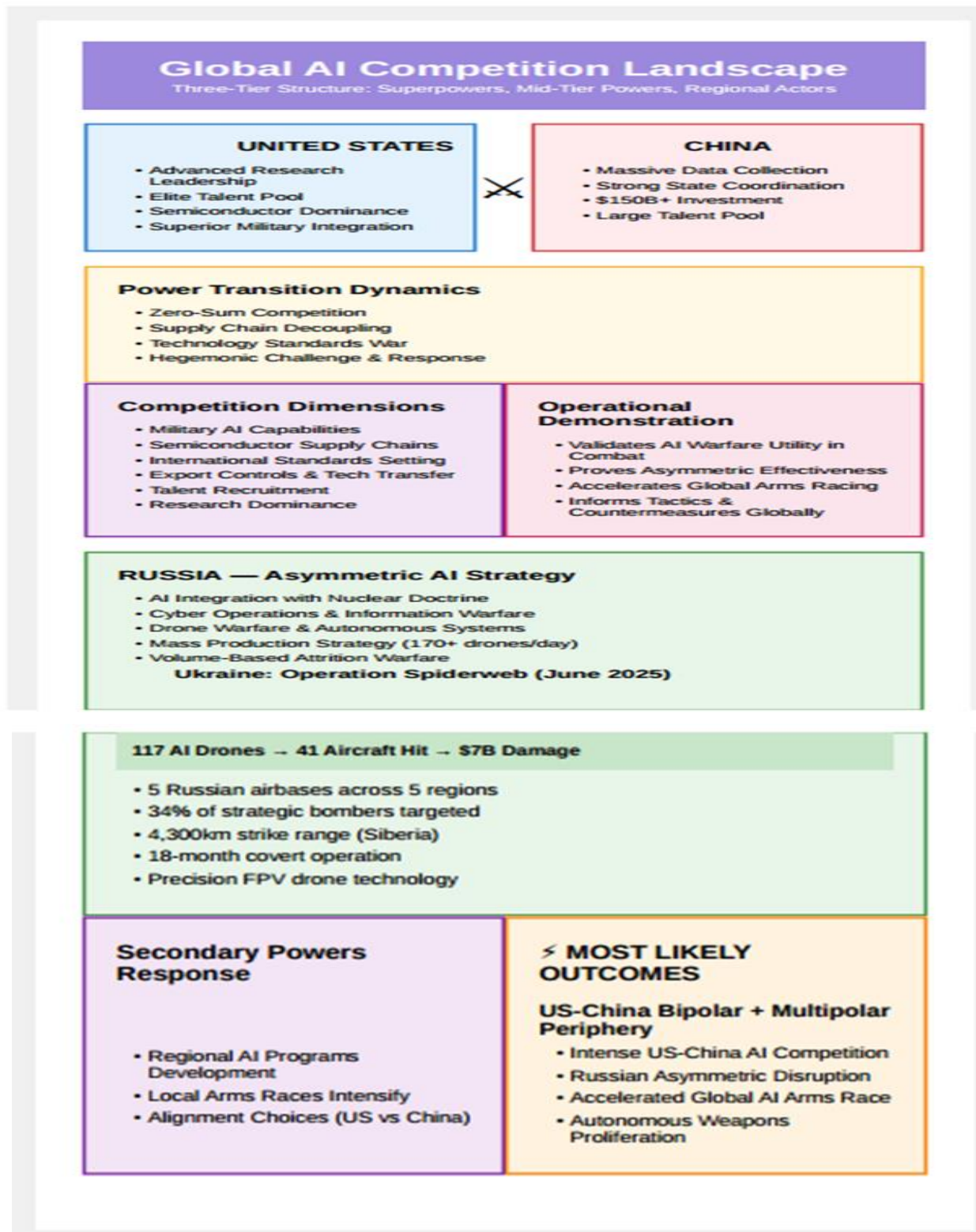
5.2 Proliferation, Dual-Use Dilemma, and System Polarity

The propagation nature of AI technology is quite distinct from the history of military advancement. Whereas nuclear arms need specific materials, which restrict weapons proliferation to developed nations, AI needs to access computational resources, algorithms, and data, resources that are more accessible and can be transferred more easily (Horowitz, 2010). The commercial sources of most AI studies pose particular control problems never faced by the earlier military technology (Johnson, 2019). There are restrictions to export controls because AI algorithms are shared in scholarly journals and open-source libraries, and skilled researchers can cross borders, disseminating knowledge quickly in research communities worldwide (Ding, 2018). This porousness makes competition hard because states that heavily invest in AI are prone to innovations being initially absorbed by competitors through espionage or simultaneous advancements, which makes the demand to develop capabilities fast (Zwetsloot and Dafoe, 2019).

5.3 Algorithmic Unpredictability and Deterrence Destabilisation

The deterrence theory presupposes that rational actors weigh costs, benefits and probabilities; however, AI generates unpredictability, which does not fit these assumptions. Training data bias implies that AI systems mirror past biases, incomplete data and inaccurate samples, which may result in a systematic inaccuracy in evaluations in new circumstances (Selbst et al., 2019). Adversarial attacks are inputs meant to deceive artificial intelligence, which provide further randomness, as studies reveal that the presence of minor changes in pictures or information may lead to disastrous misclassifications (Goodfellow et al., 2018). Emergent behaviours in complex AI systems are possibly the most significant uncertainty. When different systems of AI are used in dynamic settings, group behaviour can radically diverge over individual system designs, due to unexpected feedback interactions and unanticipated interactions (Cave & ÓhÉigeartaigh, 2018). Such unreliability negates the credible commitments to deterrence since states cannot be sure that they will or will not act in specific ways, since they cannot exercise complete control over such systems, which is a fundamental factor in destabilising strategic relations.

Figure 2: Global competition in AI landscape



Source: Created by the Researcher

6. Great Power Competition in AI

6.1 U.S.-China AI Rivalry: Power Transition Dynamics

The U.S.-China AI confrontation is the core of the modern great power conflict, with the traditional patterns of power transition and an established hegemon confronted with an aspiring challenger in the area that defines the following respective power statuses. The 2017 New Generation Artificial Intelligence Development Plan of China aims to achieve AI dominance by 2030, and military use is the priority in modernising the People's Liberation Army (Roberts et al., 2021). The Chinese strengths are the vast accumulation of data due to the presence of surveillance systems, well-coordinated and coordinated governments with civil-military fusion policies, significant financial resources exceeding 150 billion, and a large talent pool (Kania, 2021). The American strengths are the lead in fundamental AI research, semiconductor design, the best talents of the elite institutions, and the best military AI integration, with the challenges of the Chinese progress and global dissemination of AI knowledge (Fedasiuk and Weinstein, 2021). The issues of relative gains prevail in this competition, even when collaboration on AI safety can lead to absolute gains; both states are concerned that collaboration will give more benefits to the other, which will become powerful disincentives to share research (Horowitz, 2018). Although the two states are economically interdependent, they are placing less emphasis on economic efficiency and more on strategic autonomy, with the decoupling of supply chains and limiting technology transfers regardless of the financial costs (Roberts et al., 2020). Competition goes beyond the ability to compete with norms and institutional practices; it is a complex struggle over international order.

6.2 Ukraine and Russia Asymmetric AI Strategy

The current Russia-Ukraine conflict has turned into a significant test ground of the asymmetric warfare strategies, which are promoted by artificial intelligence and the drone technology. The strategy of Russia can also be described as an asymmetric AI strategy, where a high volume of relatively cheap AI-enhanced drones is used to obliterate Ukrainian positions not through technological excellence but by sheer numbers (Al Jazeera, 2025c). Averaging 120-185 strikes daily in every month between January and May 2025, it is possible to note that Russia has persisted with a strategy of long-range aerial pressure on an automated basis (Al Jazeera, 2025c). The type of drones that are mainly used by Russia is Shahed-type drones that are capable of reaching simple AI in terms of navigation and target recognition and can be produced in large quantities to around 170 drones per day and to 190 by the end of 2025 (Al Jazeera, 2025c).

Another approach taken by Ukraine has been a more advanced approach to AI that is asymmetric and precision-driven, intelligence-driven, and operation innovation-driven instead of mass production. An example of such a strategy can be seen in operation Spiderweb where Ukrainian troops used AI-guided reconnaissance, coordination algorithms, and first-person view drones to make surgical attacks on Russian military assets of high value (CNN, 2025b; Stern, 2025). The success of the operation, which eliminated 34 percent of Russian strategic cruise missile carriers using only 117 drones, shows that AI-assisted planning, remote piloting and real-time adjustments, and autonomous navigation systems can do achieve strategic effects that are disproportionate to the resources used (Al Jazeera, 2025a). This imbalance is also seen in the fact that Ukraine can launch drones deep inside Russian airspace with AI-based logistics planning and coordinate attacks in different time zones, hitting targets as far as 4300 kilometers in distance to

the Ukrainian borders (Al Jazeera, 2025a; Axios, 2025).

The opposing strategies of AI indicate a more general asymmetry in the struggle: Russia operates on its industrial potential and the depth of its territory to create swarms of disposable AI-empowered drones to engage in attrition warfare, whereas Ukraine must make up the lack of resources through technological innovations, the application of AI to the tactic, and innovative operational planning (CNN, 2025a). Each strategy highlights the importance of artificial intelligence becoming the focal point of asymmetric warfare in the modern world, where small forces can fight bigger ones and the standard equation of military strength changes (Stern, 2025).

6.3 Secondary Powers and Regional Dynamics

In addition to the great power competition, secondary powers seek AI capabilities that can raise regional security threats and proliferation threats. Israel has one of the most developed military AI systems, which uses autonomous border defence systems, autonomous missile defence, and automated intelligence analysis (Sayler, 2020). India spends a lot on AI in border security with Pakistan and China, autonomous systems, and cyber capabilities, and it considers AI to be the key to regional power status (Behera, 2019). Turkey creates its own autonomous drones that have been proven in Syria, Libya, and Nagorno-Karabakh, and Iran continues to develop AI despite the sanctions, but its priorities include asymmetric warfare, such as drones and cyber warfare. With these regional programs, there exists a local arms race between neighbouring states because of perceived threats, which disaggregate the global governance efforts, thus posing a greater risk of proliferation. Middle powers have alignment options between the U.S and Chinese AI ecosystems, as technology standards, supply chain dependence and normative frameworks play a role in strategic positioning. AI capabilities being spread to unstable areas increase the risk of crises and conflicts where AI systems could get out of control and leave the situation out of human control, putting the stability of the broader system at risk (Raska, 2021).

7. Governance under Anarchy

7.1 Structural Barriers to International Cooperation

Neorealist theory is a theory that forecasts underlying barriers to AI governance based on an anarchic structure. The relative gains issue is especially acute, even when cooperation has absolute benefits to all parties, states fear that an agreement will favour their competitors disproportionately, aggravating their relative power status (Grieco, 1988). The collaboration of safety standards or sharing of research in AI development may benefit all states in terms of their capacity; however, when China has more than the United States, or the opposite, the weaker party will be strategically vulnerable. Relative gains issues become acute when states do not know about potential conflicts or cannot evaluate the impact of existing cooperation on future power distributions, as Powell (1991) illustrated. Lack of enforcement strategies makes cooperation challenges even more complicated, because the global agreements are based on free will to follow the agreements without supranational forces that can penalise the offenders (Downs et al., 1996). States that violate the AI development ban will benefit, and those that observe the rules will lag, leaving strong incentives to cheat. Verification impossibility is possibly the most unbreakable obstacle to the intangible nature of AI, a part of software and algorithms instead of tangible equipment, and the impossibility of traditional monitoring becomes meaningless (Reinhold, 2022). States can build AI hidden within two-use civilian infrastructure, and it is almost impossible to identify the violations.

7.2 Arms Control Lessons and Limitations

There is a grave lesson of arms control in history, which augers poorly for the future of AI governance. Nuclear treaties had minor success in the bipolarity of the Cold War, where the United States and the Soviet Union were assured of mutual destruction, and this formed a common ground in keeping nuclear war at bay (Glaser, 1992). But now AI competition exists in more multipolar terms as China, the United States, Ukraine, Russia and other forces engage with one another on various fronts, which complicates the coordination process greatly. Multipolar systems create more uncertainty regarding the threats and reliability of alliances, which destroys trust as a prerequisite to arms control (Jervis, 2017). Specifically, failures in cyber arms control offer especially pertinent precedents. However, despite numerous efforts based on UN forums and bilateral agreements, there has been no significant limitation of cyber weaponry because of attribution challenges, dual-use technology, and the impossibility of verification (Nye, 2017; Fischerkeller and Harknett, 2019). Any attempts to build confidence in deep distrust environments have inherent constraints and will limit the likelihood of misperception at best, and are incapable of dealing with the root causes of security competition (Sagan, 1985). According to the hegemonic stability theory, dominant powers sometimes settle on international regimes. Still, the American hegemony has lost momentum, and China is emerging, and no hegemony would enforce the AI governance system (Gilpin, 1981).

7.3 Limited Cooperation Possibilities

With structural pessimism, little cooperation can be achieved, but in limited areas of cooperation, the states can identify common existential threats. Research on AI safety that focuses on catastrophic failure modes is one of the places where collaboration may arise because all states have common interests in avoiding AI accidents that may lead to unintended escalation (Dafoe, 2018). Nonetheless, safety cooperation is also not easy since states are afraid of disclosing vulnerable information that can be used by their adversaries (Garfinkel and Dafoe, 2019). Signalling roles may be fulfilled by transparency initiatives, where states convey the message of restraint by voluntarily sharing information (Cihon, 2019). Track II diplomacy and epistemic communities - networks of technical specialists who trade information across borders - are minor participants in enhancing mutual understanding and creating technical standards that limit incompatibility (Adler and Haas, 1992). This is especially challenging with the governance of the private sector, where technology firms tend to be hesitant to comply with the government regulations that they consider a competitive weakness (Bradford, 2023). Export controls are more of a competitive approach than a genuine governance. States limit the transfer of AI technology to their enemies and allow it to flow to friends, using trade policy to secure relative benefits (Hornik, 2021). In general, the opportunities for cooperation are still limited by structural anarchy, and the states seek narrow, self-seeking collaboration, continuing to compete at the broader level.

8. Structural Predictions and Policy Implications

8.1 Neorealist Scenarios for AI Competition

There are three structural scenarios of AI competition. The first scenario is a U.S.-China bipolar AI competition, in which two powerful countries have much more impressive capabilities, establishing a relatively stable duopoly relationship, comparable to cold bipolarity in the nuclear competition with predictable balancing yet high arms races (Monteiro, 2014). Scenario two

propagates multi-polar instability in which AI functionality spreads across several great and middle powers, such as the United States, China, Russia, the EU, India, developing liquid, unstable competition with more profound confusion of threats and loyalty of alliances, aggravating security disasters (Mearsheimer, 2001). Scenario three assumes less cooperation on existential risks; states are aware that some AI developments threaten all actors, such as fully autonomous nuclear systems or uncontrolled AGI, which create common interests and shared interests toward avoiding catastrophic outcomes despite competition (Jervis, 1978). According to structural determinants, scenarios one plus two are the most probable: firstly, bipolar competition between the U.S. and China with substantial multipolar features as the latter builds consequential capabilities. The example of the July 2025 drone operation in Ukraine and Russia is one illustration of the asymmetrical use of AI by mid-level powers, making bipolar relationships difficult to follow (Jane, 2025, Defence Weekly). The pressures of competition will prevail structurally, but there can be little cooperation where great powers coincidentally agree on existential threats.

8.2 Policy Recommendations within Structural Constraints

Relative capabilities and strategic advantage should be prioritised as sustained investments in research and talent, and military AI integration will enable states to lose core security interests due to lagging behind (Horowitz, 2018). Nevertheless, the issue of AI safety is a security imperative because unreliable systems do not maintain effectiveness and allow for the exploitation of vulnerabilities (Amodei et al., 2016). Exercise human control where it is strategically feasible, especially in the area of nuclear arms, when a failure leads to an escalation of devastating proportions. Still, competition pressures lead to greater tactical operations autonomy (Scharre, 2018). Hedge on technologies via several channels and backup. Balance ensured preclusion of cooperation and competition through cooperation on technical standards of small parts and measures of building confidence and keeping up with the development of the military on a competitive basis (Maas, 2019). Follow the example of Russia-Ukraine AI warfare to know about the effectiveness and weaknesses of capabilities and inform countermeasures and innovations (Boulain, 2021).

8.3 Role of International Institutions

International institutions are mainly used as instruments by powerful states to advance their interests and not as autonomous restraints on conduct. The power relations that are manifested at the UN and in multilateral forums that address the issue of AI governance also enable the coordination between those states that may have temporary common interests but have no means to enforce the great powers to comply (Mearsheimer, 1994). Technical standards associations and epistemic communities have narrow yet helpful roles of creating interoperability specifications and having expert dialogues, minimising misconceptions, but not changing the dynamics of competition in a significant way (Haas, 1992). Although institutions are limited by structural anarchy, they offer channels to signal intentions and how to use crises to conduct crises, which are the auxiliary functions in the mostly competitive international system.

9. Conclusion

The opaqueness of AI makes it impossible to recognise offensive and defensive capabilities, the impossibility of verification destroys arms control opportunities, the shrinking of decision-making timeframes poses first-mover advantages and instabilities in a crisis, and the ductility of

dual-use applications erases the civilian-military difference. These aspects enhance the uncertainty, fear, and arms race between great powers that seek to survive using self-help policies.

The AI security dilemma arises mainly due to the structure of the system and not the technological nature or the vices of states. Without central power, the rational states will have to plan worst-case scenarios concerning adversaries' capabilities in terms of AI, which will prompt them to engage in competitive acquisition under the conditions of mutual danger. The issue of relative gains makes cooperation impossible as states are afraid to enhance their enemies' positions. Competitive pressures are so effective structurally that the U.S.-China rivalry characterises AI geopolitics as secondary powers, such as Russia, seek asymmetric approaches. The comparison of the AI strategies used by Russia and Ukraine can show how AI can assist in asymmetric operations in contemporary wars. The experience of Russia's mass-production strategy and Ukraine's precision-oriented operations proves that AI technology enhances quantitative and qualitative advantages, completely changing the strategic count and showing that technological innovation will be able to compensate for traditional military superiority.

Conflict of Interest

The authors showed no conflict of interest.

Funding

The authors did not mention any funding for this research.

References

- Acton, J. M. (2018). Cyber warfare & inadvertent escalation. *Daedalus*, 147(4), 133-146. https://doi.org/10.1162/daed_a_00521
- Adler, E., & Haas, P. M. (1992). Conclusion: Epistemic communities, world order, and the creation of a reflective research program. *International Organization*, 46(1), 367-390. <https://doi.org/10.1017/S002081830000148X>
- Al Jazeera. (2025a, June 1). *Ukrainian drones target Russian airbases in unprecedented operation*. <https://www.aljazeera.com/news/2025/6/1/ukrainian-drones-target-russian-airbases-in-unprecedented-operation>
- Al Jazeera. (2025b, June 2). *Ukraine bombs Russian bases: Here are some of Kyiv's most audacious attacks*. <https://www.aljazeera.com/news/2025/6/2/ukraine-bombs-russian-bases-here-are-some-of-kyivs-most-audacious-attacks>
- Al Jazeera. (2025c, September 9). *Charting the past year of Russian drone and missile attacks on Ukraine*. <https://www.aljazeera.com/news/2025/9/9/charting-the-past-year-of-russian-drone-and-missile-attacks-on-ukraine>
- Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Belfer Center for Science and International Affairs, Harvard Kennedy School.
- Allen, G., & Husain, A. (2017). The next space race is artificial intelligence. *Foreign Policy*. <https://foreignpolicy.com/2017/11/03/the-next-space-race-is-artificial-intelligence-and-america-is-losing-to-china/>
- Altmann, J., & Sauer, F. (2017). Autonomous weapon systems and strategic stability. *Survival*, 59(5), 117-142. <https://doi.org/10.1080/00396338.2017.1375263>
- Amodei, D., et al. (2016). Concrete problems in AI safety. *arXiv preprint arXiv:1606.06565*.
- Axios. (2025, June 1). *Ukraine launches massive drone strike on air bases deep inside Russia*. <https://www.axios.com/2025/06/01/ukraine-drone-strikes-russia>
- Behera, L. K. (2019). India's national strategy for artificial intelligence. *Observer Research Foundation Occasional Paper*, 225.
- Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, 84, 317-331. <https://doi.org/10.1016/j.patcog.2018.07.023>
- Booth, K., & Wheeler, N. J. (2008). *The Security Dilemma: Fear, Cooperation and Trust in World Politics*. Basingstoke: Palgrave Macmillan.
- Boulanin, V., Davison, N., Goussac, N., & Bruun, E. (2020). Limits on autonomy in weapon systems: Identifying practical elements of human control. Stockholm International Peace Research Institute.
- Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.
- Brundage, M., et al. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. Future of Humanity Institute, University of Oxford.

- Buchanan, B. (2020). *The hacker and the state: Cyber-attacks and the new normal of geopolitics*. Harvard University Press.
- Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1). <https://doi.org/10.1177/2053951715622512>
- Cave, S., & ÓhÉigeartaigh, S. S. (2018). An AI race for strategic advantage. *AAAI/ACM Conference on AI, Ethics, and Society*.
- Christensen, T. J., & Snyder, J. (1990). Chain Gangs and Passed Bucks: Predicting Alliance Patterns in Multipolarity. *International Organization*, 44(2), 137-168.
- Cihon, P. (2019). Standards for AI governance: International standards to enable global coordination in AI research & development. *Future of Humanity Institute Technical Report*.
- CNN. (2025a, June 2). *New footage reveals the impact of Ukraine's audacious drone attack on Russian air bases*. <https://www.cnn.com/2025/06/02/europe/inside-ukraine-drone-attack-russian-air-bases-latam-intl>
- CNN. (2025b, June 2). *Operation Spiderweb: Ukraine hits air bases thousands of miles inside Russia in audacious military operation*. <https://www.cnn.com/2025/06/01/europe/ukraine-drones-russia-airbases-intl>
- Copeland, D. C. (2000). The constructivist challenge to structural realism: A review essay. *International Security*, 25(2), 187-212. <https://doi.org/10.1162/016228800560605>
- Cummings, M. L. (2017). Artificial intelligence and the future of warfare. Chatham House Research Paper.
- Dafoe, A. (2018). AI governance: A research agenda. Centre for the Governance of AI, Future of Humanity Institute, University of Oxford.
- Ding, J. (2018). *Deciphering China's AI dream*. Future of Humanity Institute, University of Oxford.
- Downs, G. W., Rocke, D. M., & Barsoom, P. N. (1996). Is the good news about compliance good news about cooperation? *International Organization*, 50(3), 379-406. <https://doi.org/10.1017/S0020818300033427>
- Fedasiuk, R., & Weinstein, E. (2021). Overseas professionals and technology transfer to China. *Center for Security and Emerging Technology*.
- Fischerkeller, M. P., & Harknett, R. J. (2019). Deterrence is not a credible strategy for cyberspace. *Orbis*, 63(3), 381-393. <https://doi.org/10.1016/j.orbis.2019.05.003>
- Garfinkel, B., & Dafoe, A. (2019). How does the offense-defense balance scale? *Journal of Strategic Studies*, 42(6), 736-763. <https://doi.org/10.1080/01402390.2019.1631810>
- Geist, E. (2016). It's already too late to stop the AI arms race. *Bulletin of the Atomic Scientists*, 72(5), 318-321. <https://doi.org/10.1080/00963402.2016.1216672>
- Gilpin, R. (1981). *War and change in world politics*. Cambridge University Press.
- Glaser, C. L. (1992). Political consequences of military strategy: Expanding and refining the spiral and deterrence models. *World Politics*, 44(4), 497-538.

<https://doi.org/10.2307/2010487>

- Glaser, C. L. (2010). *Rational theory of international politics: The logic of competition and cooperation*. Princeton University Press.
- Goertzel, B., & Pennachin, C. (2007). *Artificial general intelligence*. Springer.
- Goodfellow, I., McDaniel, P., & Papernot, N. (2018). Making machine learning robust against adversarial inputs. *Communications of the ACM*, 61(7), 56-66.
- Grieco, J. M. (1988). Anarchy and the limits of cooperation: A realist critique of the newest liberal institutionalism. *International Organization*, 42(3), 485-507. <https://doi.org/10.1017/S0020818300027715>
- Haas, P. M. (1992). Introduction: Epistemic communities and international policy coordination. *International Organization*, 46(1), 1-35. <https://doi.org/10.1017/S0020818300001442>
- Herz, J. H. (1950). Idealist internationalism and the security dilemma. *World Politics*, 2(2), 157-180. <https://doi.org/10.2307/2009187>
- Hornik, J. (2021). The limits of the AI export control debate. *Lawfare Blog*. <https://www.lawfareblog.com/limits-ai-export-control-debate>
- Horowitz, M. C. (2010). *The diffusion of military power: Causes and consequences for international politics*. Princeton University Press.
- Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review*, 1(3), 36-57. <https://doi.org/10.15781/T2639KP49>
- Horowitz, M. C. (2019). When speed kills: Lethal autonomous weapon systems, deterrence and stability. *Journal of Strategic Studies*, 42(6), 764-788. <https://doi.org/10.1080/01402390.2019.1621174>
- Horowitz, M. C., & Scharre, P. (2021). AI and international stability: Risks and confidence-building measures. Center for a New American Security.
- Jervis, R. (1978). Cooperation under the security dilemma. *World Politics*, 30(2), 167-214. <https://doi.org/10.2307/2009958>
- Jervis, R. (1989). *The meaning of the nuclear revolution: Statecraft and the prospect of Armageddon*. Cornell University Press.
- Jervis, R. (2017). *Perception and misperception in international politics* (2nd ed.). Princeton University Press.
- Johnson, J. (2019). Artificial intelligence & future warfare: Implications for international security. *Defense & Security Analysis*, 35(2), 147-169. <https://doi.org/10.1080/14751798.2019.1600800>
- Johnson, J. (2020). Delegating strategic decision-making to machines: Dr. Strangelove redux? In T. Lawson (Ed.), *The frontiers of artificial intelligence ethics* (pp. 345-362). Routledge.
- Kania, E. B. (2020). AI weapons in China's military innovation. Brookings Institution

Report.

- Kania, E. B. (2021). *Chinese military innovation in artificial intelligence*. Center for a New American Security.
- Kreps, S. (2016). *Drones: What everyone needs to know*. Oxford University Press.
- Kreps, S., & Schneider, J. (2019). Escalation firebreaks in the cyber, conventional, and nuclear domains. *Journal of Cybersecurity*, 5(1), tyz007.
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444. <https://doi.org/10.1038/nature14539>
- Maas, M. M. (2019). How viable is international arms control for military artificial intelligence? *Contemporary Security Policy*, 40(3), 285-311. <https://doi.org/10.1080/13523260.2019.1576464>
- Mearsheimer, J. J. (1994). The false promise of international institutions. *International Security*, 19(3), 5-49. <https://doi.org/10.2307/2539078>
- Mearsheimer, J. J. (2001). *The tragedy of great power politics*. W.W. Norton & Company.
- Monteiro, N. P. (2014). *Theory of unipolar politics*. Cambridge University Press.
- Morgan, F. E., et al. (2020). *Military applications of artificial intelligence: Ethical concerns in an uncertain world*. RAND Corporation.
- NPR. (2025, June 1). *Ukraine destroys more than 40 military aircraft in a drone attack deep inside Russia*. <https://www.npr.org/2025/06/01/nx-s1-5419509/ukraine-destroys-military-aircraft-attack-inside-russia-planes>
- Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44-71. https://doi.org/10.1162/ISEC_a_00266
- Organski, A. F. K. (1958). *World politics*. Alfred A. Knopf.
- Payne, K. (2018). Strategy, evolution, and war: From apes to artificial intelligence. *Parameters*, 48(2), 7-18.
- Payne, K. (2021). *Strategy, evolution, and war: From apes to artificial intelligence*. Georgetown University Press.
- Powell, R. (1991). Absolute and relative gains in international relations theory. *American Political Science Review*, 85(4), 1303-1320. <https://doi.org/10.2307/1963947>
- Raska, M. (2021). The sixth RMA wave: Disruption in military affairs? *Journal of Strategic Studies*, 44(4), 456-479. <https://doi.org/10.1080/01402390.2021.1894127>
- Reinhold, T. (2022). Bringing AI under control? Lessons from nuclear arms control for managing artificial intelligence. *Contemporary Security Policy*, 43(3), 493-513. <https://doi.org/10.1080/13523260.2022.2074472>
- Roberts, H., et al. (2020). *The Chinese approach to artificial intelligence: An analysis of policy, ethics, and regulation*. AI Now Institute.
- Roberts, H., et al. (2021). *Understanding Chinese government guidance funds: An analysis of Chinese industrial policy*. Center for Security and Emerging Technology.

- Roff, H. M. (2014). The strategic robot problem. *Journal of Military Ethics*, 13(3), 211-227.
- Russell, S., & Norvig, P. (2020). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
- Sagan, S. D. (1985). Nuclear alerts and crisis management. *International Security*, 9(4), 99-139. <https://doi.org/10.2307/2538543>
- Sagan, S. D. (2019). The Korean missile crisis: Why deterrence is still the best option. *Foreign Affairs*, 96(6), 72-82.
- Sauer, F., & Schörnig, N. (2012). Killer drones. *Security Dialogue*, 43(4), 363-380.
- Sayler, K. M. (2020). *Artificial intelligence and national security*. Congressional Research Service Report R45178.
- Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W.W. Norton & Company.
- Schelling, T. C. (2018). Meteors, mischief, and war. *Bulletin of the Atomic Scientists*, 74(4), 256-261. <https://doi.org/10.1080/00963402.2018.1486618>
- Schneider, J. (2019). The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war. *Journal of Strategic Studies*, 42(6), 841-863. <https://doi.org/10.1080/01402390.2019.1627811>
- Schneider, J. (2020). The unexceptional exceptionalism of AI and cyber weapons. *Texas National Security Review*, 3(4), 118-125.
- Selbst, A. D., et al. (2019). Fairness and abstraction in sociotechnical systems. *Conference on Fairness, Accountability, and Transparency*, 59-68.
- Slayton, R. (2020). Governing a risky technology: How the United States regulates nuclear-weapons command-and-control. *Technology and Culture*, 61(3), 707-740. <https://doi.org/10.1353/tech.2020.0077>
- Stern, D. L. (2025, June 2). *Ukraine attacks Russian air bases in far-reaching drone strikes*. The Washington Post. <https://www.washingtonpost.com/world/2025/06/01/ukraine-russia-war-drone-attack-siberia/>
- Tang, S. (2009). The Security Dilemma: A Conceptual Analysis. *Security Studies*, 18(3), 587-623.
- Waltz, K. N. (1979). *Theory of international politics*. McGraw-Hill.
- Wikipedia. (2025, October). *Operation Spiderweb*. https://en.wikipedia.org/wiki/Operation_Spiderweb
- Work, R., & Brimley, S. (2014). 20YY: Preparing for war in the robotic age. Center for a New American Security.
- Zwetsloot, R., & Dafoe, A. (2019). Thinking about risks from AI: Accidents, misuse and structure. *Lawfare Blog*.