An Examination of Artificial Intelligence in Modern Warfare and Conflict Resolution

An STS Research Paper
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

By
Ronit Reddy

Spring 2025

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISOR

Prof. Kathryn Webb-Destefano, Department of Engineering and Society

Introduction

Spearheaded by the rapid adoption and advancement of artificial intelligence (AI) technology within military operations, modern warfare is undergoing a radical transformation, as evidenced by the unceasing evolution in combat strategies, decision-making processes, and international security dynamics. Nowhere is this transformation more evident than in the ongoing conflict between Russia and Ukraine, a polarizing case that vividly illustrates AI's revolution of traditional combat and diplomacy. Since the onset of this war in 2014, and following its more recent escalation spurred by Russia's full-scale invasion of Ukraine in 2022, AI technologies, including autonomous, on-the-ground systems and digital warfare tools, are being deployed by both nations at unprecedented scales. This illustration signals a seismic shift away from conventional warfare paradigms, where human judgment and physical presence dictated militaristic policy and engagement, and towards an era in which computational efficiency and algorithmic precision exist as the preeminent power structures on and off the battlefield.

Current discourse surrounding AI in warfare from analysts often reduces its role to that of a force multiplier, suggesting that this technology serves to enhance existing military components of logistics, reconnaissance, and targeting, rather than to fundamentally reshape them. Such a perspective, however, fails to recognize the full potential of AI to take on greater roles in strategic combat planning and execution operations and, in the process, disrupt entrenched geopolitical structures, challenge historical doctrines of conflict resolution, and redefine state sovereignty in warfare.

Oversights of this magnitude represent a pressing challenge on behalf of policymakers and military strategists. If AI continues to be underestimated or mischaracterized by the consensus as just a technological enhancement, we, as a society, risk being unprepared for the

complex, multifaceted shifts bound to arise and compromise international stability in today's interconnected security landscape. In this, governments and military institutions may find themselves struggling to respond to AI-driven warfare, from its respective autonomous weapon systems to adversarial cyber attacks to widespread misinformation campaigns. Equally worrying are the consequences of failing to address these realities; soon, society might very well be plagued with frequent miscalculated conflict escalations, increased civilian casualties, and the erosion of prevailing human accountability in wartime.

Consequently, this paper serves to outline and support the notion that AI in the military domain is not simply an incremental technology upgrade, but a true catalyst that is actively reshaping the future of warfare, and hence requires appropriate consideration and mitigation practices. Rooted in Langdon Winner's Technological Politics framework—a theory that posits technology is not simply a neutral tool of progress but, instead, a phenomenon that inherently embodies political values and actions—this analysis explores how AI systems are being ingeniously designed and deployed to alter battlefield systems, information networks, and humanitarian practices as it relates to international conflict. To substantiate this claim, this paper adopts a robust assessment of peer-reviewed articles, academic journals, and research reports from leading authors and organizations concerned with the Russia-Ukraine War that provide a comprehensive perspective on how AI can influence global diplomacy for the foreseeable future. Ultimately, this paper offers insights into the broader implications of AI's militarization through the lens of technological agency and power that could deepen our understanding of digital developments and their effects on the global climate, and, more ambitiously, pave the way for improved approaches to modern international security management in an unrelentingly AI-dominated environment.

Literature Review

Undoubtedly, the growing adoption of AI for military purposes has prompted extensive academic discourse on its implications for modern warfare and international relations. While existing literature primarily examines AI with respect to tactical strategies, conceding its capacity to enhance combat capabilities while remaining skeptical of its abilities beyond this front, an emerging body of work argues that AI is a transformative force in the vast operational and political landscape of military engagements, underscored by its facilitation of disinformation and its restructuring of warfare participation dynamics. This section reviews two key sources that contribute to this evolving argument, with each offering unique, but valuable insights into AI's role in modern conflict.

One of the most prominent concerns surrounding AI in warfare is its role in the propagation of political disinformation. In their review article "Countering AI-Powered Disinformation Through National Regulation: Learning From the Case of Ukraine," Anatolii Marushchak, Stanislav Petrov, and Anayit Khoperiya assess both the ways in which AI technologies are helping Russia to manipulate the Ukrainian digital information ecosystem, and Ukraine's legal responses to this disinformation. Specifically, their study examines Ukraine's Law on Counter Disinformation, which was developed in response to Russia's aggressive propaganda and disinformation dissemination tactics, namely real-time deepfake videos, fake news websites, and fraudulent social media accounts, and facilitates their argument that AI has significantly altered the traditional battlefield by extending conflict into the digital domain, where disinformation is now as potent a weapon as physical military assets and operations. This research is critical to establishing a foundational understanding of how AI is not only dictating

political interactions and long-term conflict resolution strategies through its influence on direct military operations, but also that of external public perceptions and diplomatic relations.

In parallel to influencing the masses with digital disinformation, AI technologies are also redefining how wars are fought by expanding the involvement of non-traditional actors. In their research report *WAR VOLUNTEERS IN THE DIGITAL AGE: HOW NEW TECHNOLOGIES TRANSFORM CONFLICT DYNAMICS*, Jethro Norman explores how digital technologies, namely AI-driven social media and communication platforms, offer citizens real-time recruitment, crowdfunding, and battlefield transmission capabilities from their personal devices, thus helping to cultivate a culture defined by participatory warfare. To this end, this study highlights the increasing involvement of individuals in enriching and supporting open-source military initiatives in modern conflicts, as seen in Ukraine, where civilians continue to contribute to intelligence gathering and reporting through distinct national security smartphone applications. Norman finally articulates that by lowering the barriers to entry for active participation in warfare and enabling the general public to contribute to war efforts through these mediums, AI is blurring the once clear distinction between civilians and combatants, which reinforces the argument that AI is not simply enhancing pre-existing battle strategies, but is actively restructuring the architecture of modern warfare by integrating digital and social dimensions throughout combat operations.

While Marushchak, Petrov, and Khoperiya emphasize the instant dangers of AI-enabled disinformation in warfare, Norman investigates how this propaganda, coupled with mainstream, accessible AI technologies, is transforming tactical strategies and coordination as the ecosystem of warfare participants continues to expand. Although different in focus and limited in scope, given that each literature addresses a singular, seemingly niche consequence of AI in warfare,

both perspectives, together, function to provide a foundational illustration of how AI is reshaping modern military conflicts by extending their realms beyond physical battlefields, and into digital spheres and civilian communities. Thus, with its contextualization in the Russia-Ukraine War, this paper aims to build upon this principal claim and offer a comprehensive assessment of AI's multidisciplinary warfare effects, and highlight the necessity to develop strategic policies that can address its extending ethical, legal, and tactical challenges.

Conceptual Framework

In examining the interdisciplinary role of AI in modern warfare, this paper relies on Langdon Winner's Technological Politics framework, which provides a theoretical lens through which the conventional notion of technology as a neutral instrument of progress can be challenged. First articulated in Winner's seminal 1980 work, this framework contends that technology, despite previous scholarly reductions to abstract subconcepts that portray its relevant manifestations as being mere evocative objects, affordances, or materialized actions, is, in fact, inherently political, as it embodies and reinforces power structures, influences governance, and shapes societal interactions in ways that extend beyond its direct functional applications (Schraube, 2021). Beyond its definition of technology as an instrumental catalyst of human conditions and affairs, shaping societal change through nuanced democratic practices, Winner's framework also fundamentally critiques the assumption that technology develops independently of social and political forces, instead asserting that technologies are designed, implemented, and regulated in ways that aim to reflect and perpetuate existing power dynamics. These ideas are particularly relevant in the intersection of AI and warfare, where the deployment of such

technologies is firmly guided by the political and ideological objectives of the states and institutions that wield them.

Many of this framework's proponents support its emphasis on the complex interplay between technology and governance, contending this form of engagement often helps uncover the otherwise overlooked political dimensions embedded with emerging technological systems. Critics, on the other hand, argue this line of reasoning can overstate technology's innate power and influence, as, at a surface level, it is nothing more than an inanimate social construct. The common perspective falls somewhere in more neutral beliefs, aligned with the claim that while technology plays a large role in shaping power dynamics, its true influence is determined by human decision-makers who control its deployment and regulation.

To best illustrate the applicability of the Technological Politics framework in the intersection of AI and modern conflict with this spectrum of viewpoints in mind, the ongoing Russia-Ukraine war presents itself as a premier case study, with AI having been, and continuing to be, instrumental in altering military strategies, intelligence operations, and public perceptions. By situating AI within this framework's context, this paper seeks to uncover the sociopolitical dimensions present in these various systems, acknowledging that such AI technologies are not neutral tools, but are, indeed, designed to serve specific political objectives, reinforce ideological stances, and reconstruct power hierarchies.

Analysis

Most evidently, AI has optimized contemporary military systems in its ability to both improve data derivation and processing operations at unparalleled efficiency, and reduce the human cost of war through its numerous integrated forms of autonomous weapon systems. It is

no surprise, then, that AI has revolutionized power dynamics in traditional conflict scenarios, as objectives can now be reached by nations with lesser physical and financial burdens, incentivizing them to emerge at the forefront of these technologies in order to attain global superiority. The ongoing conflict between Russia and Ukraine exemplifies exactly how AI technologies are being deployed to reinforce specific political strategies and power structures, as these tools are continuously being engineered to narrow military gaps and provide battlefield advantages.

Since the war's revitalization in 2022, both Russia and Ukraine have demonstrated heightened urgency in employing AI to accelerate the production of their geospatial intelligence, logistics, and detection systems, with Ukraine identifying pressing defense AI priorities for "domestic unmanned systems, mine and ammunition detection and neutralization, and simulation modeling solutions for military operations," while Russia focuses on its "transition to advanced digital, intelligent production technologies, robotic systems, new materials and design methods, [coupled with] the creation of systems for big data processing, machine learning and artificial intelligence" (Goncharuk, 2024b; Zysk, 2024). This intensified push by both nations to adopt and deploy AI systems in different facets of their military operations serves to reflect how both countries view AI as more than just combat enhancements, but as a calculated and strategic means of securing political dominance in what figures to be an extensive, technology-driven race—one where technological superiority through AI seems inseparable from political authority.

Developments have not been made solely in the context of intelligence systems, however; over the years, Ukraine has crafted numerous valuable internal defense and support tools, including Kropyva, a situational awareness system, and GIS Arta, an application to accelerate and synchronize its artillery targeting, along with other decentralized digital infrastructures and

large-scale navigation technologies to deliver supplies and evacuate civilians, all of which have been deployed as counteroffensives in the later months of 2022 after Russia's full-scale invasion (Goncharuk, 2024a). In this, Ukraine has found it necessary to deploy AI-powered solutions to safeguard its civilians and ensure its integrity as a matter of resistance to Russia's military offensive, further representing a political decision to leverage AI's precision and computational speed as protection against oppressive powers, allowing it to preserve its national security. This intentional leveraging of AI illustrates a strategic political choice in recognizing technology as a core asset in preserving democratic sovereignty, and directly countering authoritarianism through innovation instead of mere military force.

Russia, meanwhile, continues to press forward with aggression, having "launched at least 13 waves of attacks using hundreds of long-range missiles and drones carrying explosives" between October 2022 and February 2023 alone, which affected 20 out of 24 of Ukraine's primary regions, and still utilizing AI technologies like Iranian-made Shahed drones and long-range missile systems capable of real-time data processing and course correction to destroy Ukrainian thermal and hydroelectric power installations (Saxon, 2024). This, too, demonstrates an explicit political intent from Russia to leverage AI's precision towards the degradation of Ukrainian morale and energy infrastructure, as it ultimately aims to further its geopolitical aims of invasion, subjugation, and control through these AI technologies and the extending psychological tolls they present on Ukrainian individuals.

Considering these circumstances, many of these aforementioned autonomous AI systems intrinsically introduce fundamental dilemmas in the ambiguity they raise surrounding ethical accountability when deciding critical conflict outcomes. Such predicaments are best encapsulated by the well-known "Morality" and "Intentionality" problems, which assert that

these systems only stand to enlarge disconnects in their awareness of basic human intuition and their associated "will" or "consciousness" as they become more ingrained within the military sphere, and could eventually induce a widespread "deliberate disregard for the moral standards of controlled AI or the spontaneous emergence of aggressive autonomous AI" (Kostenko et al., 2023). These considerations signify the ever-present notion of political choices being encoded into technological designs and the emerging concerns of this intertwining, as relevant state actors, including both Russian and Ukrainian parties in the Russia-Ukraine War, seek to accelerate human capabilities, boost daily liberties, and extend political power through autonomous systems to function in their countries' benefit despite whatever consequences may come forth. That being the case, technology, with greater driving political ambitions and strategic imperatives, may soon come to assume roles traditionally reserved for human judgment, which could create a volatile, potentially grave dynamic in which political calculations eradicate any ethical codes in warfare.

Beyond the battlefield, AI has fundamentally reshaped the landscape of conflict by enabling the rise of pervasive and sophisticated disinformation campaigns, effectively expanding warfare into the digital and social domains. In the Russia-Ukraine war, Russia has been an extreme perpetrator in the spread of disinformation, as it has frequently conducted influence campaigns through AI-supported systems both outside its borders to weaken its adversaries distort public attitudes, and within its borders to embolden nationalistic fervor and raise common support among its constituents. Just prior to its invasion of Ukraine in 2022, the nation carried out numerous massive Distributed Denial-of-Service (DDoS) cyberattacks with the intent of disrupting public Ukrainian support—including banks and ministries—as a preceding measure to create civil unrest and discord, which were promptly followed by spam pro-Russia SMS and

social media messages being sent across Ukrainian communication networks to heighten the national angst (Hunter et al., 2024). Here, these calculated AI operations allowed Russia to effectively weaponize mass uncertainty and confusion, where it could deliberately target and degrade societal cohesion and trust in Ukrainian institutions in order to expedite its centralized political objective of demilitarization and occupation.

Since then, Russia has been incessant in its spread of similar disinformation campaigns and cyberattacks, as it continues to use AI to generate disruptive propaganda and systematically flood worldwide discussion forums, websites, and other media sources with distorted narratives regarding the ongoing conflict and their justification for its necessity, such as "portraying Ukraine as a 'Nazi state,' leveling accusations of 'genocide' and citizen murders,...[and] propagating false narratives about the presence of US bio laboratories in Ukraine, purportedly engaged in developing biological weapons specifically targeting 'Russian DNA'" (Tolmach et al., 2024). These efforts further note Russia's calculated political aim to create confusion and instability through AI-related information manipulation within broader international information warfare dynamics, operating under the rationale that any democratic regime can, and often will, suffer as part of these tactics given the sheer, persistent influx of disinformation across diverse media channels and networks and the ensuing political outrage and countermeasures from influenced global parties.

In order to counteract these numerous forms of AI-driven disinformation campaigns brought on by Russian forces, Ukraine has implemented advanced AI algorithms relying on CommSecure and CIB Guard software throughout its online networks to detect and neutralize false narratives, which function in "[detecting] specific narratives in messages on social networks and communities, such as public groups in messengers" and "analyzing public user

pages, identifying bots, and determining whether they act in a coordinated manner," respectively, and enacted social and legal emergency responses in accordance with European Union legislation and regulations to heighten fact-checking networks and increase digital competency and media literacy among its constituents (Marushchak et al., 2025). Ukraine's actions illustrate how nations and societies often politically strategize to preserve cohesion and unity amidst digital threats, and use AI technology as a means to mitigate the effects of these events and deter potential offenders from partaking in these matters, all done with the aim of preserving internal unity and external perspectives. Accordingly, AI exists, in this case, as a digital form of regulation that does not simply respond to and handle misinformation, but serves as an active instrument of state resilience and narrative sovereignty, institutionalized as an upstanding political mechanism for crisis governance and control.

Such developments have yielded more direct counteractive measures for Ukraine, which has also undergone a significant shift toward participatory warfare spurred by the advent of AI technologies in the communication and connectivity domains, with its civilian participation—enabled by internet platforms such as Telegram and Reddit facilitating battlefield recruitment, and group programs like GoFundMe bringing rise to crowdfunding of military assets and logistical support—continuing to grow in magnitude and, correspondingly, complicate traditional definitions of combatant roles (Norman, 2024). In this expansion of warfare participants, it is clear that AI, by design and implementation, can intentionally reshape warfare into a domain where conventional distinctions between military and civilian actors are blurred, which only erodes the sovereignty of military institutions and redistributes power among a broader spectrum of actors, from independent civilian groups to international donors.

The implications of AI in warfare as it pertains to the treatment of civilians in humanitarian contexts is another key element to consider as technology continues to be brought forth. Following Russia's invasion of Ukraine in 2022, many Ukrainian citizens either sought refuge elsewhere, or were so impassioned they desired to stay and contribute to their nation's independence efforts. To combat the latter of these groups and their ensuing efforts, Russia launched a full-scale application of AI-powered biometric surveillance technologies across its regime, including forced biometric data collection from Ukrainian deportees in its territories and targeted facial recognition tracking of political activists, to actively monitor and prosecute these individuals. In response, Ukraine followed suit with an application of its own biometric technologies, primarily biometric passports, for humanitarian aid and efficient refugee management, which simplified and streamlined migration for Ukrainian refugees to other countries by authorizing them to "travel visa-free to the countries in the Schengen Zone and stay for 90 days ([the Schengen Zone]...consists of 26 European countries with a mutual visa-free travel regime…[and] Ukraine is not in the Schengen Zone)" (Gofman & Villa, 2023). When juxtaposed, these narratives exemplify explicit political choices in the deployment of AI aimed at consolidating authoritarian control and reinforcing state power on one end, and empowering people to lead safe, secure lives on the other end. This magnification of ideological division not only highlights the duality in power of AI as a political agent to equally enable and restrict freedoms, but also, and more importantly, dictates the idea that the expansive repercussions of AI in these international matters fall solely contingent upon the political objectives and intentions guiding its use and capacity.

Furthermore, the broader use of AI within migration-related procedures across the European Union, from security/health risk assessments to document verification to residence

permit examination, has been intensified by this armed conflict and the ensuing desire from millions of Ukrainians and Russians to flee their countries (with over 7 million Ukrainians and 1 million Russians having been estimated to have left their country since the war's resurgence), and illustrates significant opportunities for AI to play a role in enhanced border control and ethical threat handling associated with privacy violations and discriminatory practices relevant to this migration phenomenon (Szwed, 2022). Nonetheless, this scenario also reveals the politically charged nature of AI technology deployment, and the fact it can easily be deployed for better or worse. Pertinent to this case, while AI can certainly reduce bureaucratic inefficiencies and aid displaced populations, it carries the inherent risk of algorithmic bias, which can function towards discriminatory profiling and data privacy violations, especially when deployed without robust oversight mechanisms. Therefore, much of its effectiveness falls on whether this process is guided by a political respect for humanitarian rights and the preservation of innate rights and liberties, or a desire for ultimate control and jurisdiction.

Conclusion

The analysis of the Russia-Ukraine conflict presented in this paper challenges the conventional view of AI as a neutral or purely technical innovation, instead positioning it as a critical factor in contemporary society. Amidst the logic of Langdon Winner's Technological Politics framework, this paper articulates that AI is imbued with political agency and deliberately designed to serve specific power structures and ideological imperatives, in both its direct military applications, and its extending digital and humanitarian impacts.

As nations increasingly leverage AI to gain both tactical and strategic advantages, the stakes at hand extend beyond immediate battlefield outcomes and territorial gains, and now come

to encompass broader issues surrounding the very legitimacy of political regimes and institutions. Military strategists, policymakers, and international organizations alike, therefore, must adopt a more nuanced perspective—one that fully acknowledges the interplay between technological capability and political intent—if they desire to ever address the complex ethical dilemmas and strategic risks AI presents, and ensure its deployment does not undermine democratic values and destabilize international relations. Understanding this, the need for a thorough, informed approach to governance becomes ever-critical in the coming years; herein, by shifting its focus to developing comprehensive legal frameworks and cooperative strategies to regulate AI's role in all aspects of conflict, the international community can harness its tremendous potential for positive transformation while mitigating its potentially destructive pitfalls, thereby promoting responsible technological progress and stability.

References

Gofman, M. I. & Villa, M. (2023). Identity and war: The role of biometrics in the Russia-Ukraine crisis. *International Journal on Engineering, Science, and Technology, 5*(1), 89-111. https://doi.org/10.46328/ijonest.143

Goncharuk, V. (2024a). *Artificial intelligence in defence of Ukraine*. International Centre for Defense and Security. https://icds.ee/wp-content/uploads/dlm_uploads/2024/09/Layout-AI-in-Defence-of-Ukraine.pdf

Goncharuk, V. (2024b). Survival of the smartest? Defense AI in Ukraine. In H. Borchert, T. Schütz, & J. Verbovsky (Eds.), *The very long game: 25 case studies on the global state of defense AI* (pp. 375-395). Springer. https://doi.org/10.1007/978-3-031-58649-1_17

Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., & Hennigan, C. (2024). Artificial intelligence and information warfare in major power states: How the US, China, and Russia are using artificial intelligence in their information warfare and influence operations. *Defense & Security Analysis, 40*(2), 235-269. https://doi.org/10.1080/14751798.2024.2321736

Kostenko, O., Jaynes, T., Zhuravlov, D., Dniprov, O., & Usenko, Y. (2023). PROBLEMS OF USING AUTONOMOUS MILITARY AI AGAINST THE BACKGROUND OF RUSSIA'S MILITARY AGGRESSION AGAINST UKRAINE. *Baltic Journal of Legal and Social Sciences,* (4), 131-145. https://doi.org/10.30525/2592-8813-2022-4-16

Marushchak, A., Petrov, S., & Khoperiya, A. (2025). Countering AI-powered disinformation through national regulation: Learning from the case of Ukraine. *Frontiers in Artificial Intelligence, 7*. https://doi.org/10.3389/frai.2024.1474034

Norman, J. (2024). *WAR VOLUNTEERS IN THE DIGITAL AGE: HOW NEW TECHNOLOGIES TRANSFORM CONFLICT DYNAMICS*. Danish Institute for International Studies. http://www.jstor.org/stable/resrep61112

Saxon, D. (2024). Military AI and accountability of individuals and states for war crimes in the Ukraine. In J. M. Schraagen (Ed.), *Responsible use of AI in military systems* (pp. 169-191). Chapman and Hall/CRC. https://doi.org/10.1201/9781003410379-11

Schraube, E. (2021). Langdon Winner's theory of technological politics: Rethinking science and technology for future society. *Engaging Science, Technology, and Society, 7*(1), 113-117. https://doi.org/10.17351/ests2021.811

Szwed, A. (2022). The use of artificial intelligence in migration-related procedures in the European Union - opportunities and threats. *Procedia Computer Science, 207*, 3645-3651. https://doi.org/10.1016/j.procs.2022.09.424

Tolmach, M., Trach, Y., Chaikovska, O., Volynets, V., Khrushch, S., & Kotsiubivska, K. (2024). Artificial intelligence in countering disinformation and enemy propaganda in the context of Russia's armed aggression against Ukraine. In A. K. Nagar, D. S. Jat, D. K. Mishra, & A. Joshi (Eds.), *Intelligent sustainable systems: Selected papers of WorldS4 2023* (vol. 4, pp. 145-152). Springer. https://doi.org/10.1007/978-981-99-8111-3_14

Zysk, K. (2024). High hopes amid hard realities: Defense AI in Russia. In H. Borchert, T. Schütz, & J. Verbovsky (Eds.), *The very long game: 25 case studies on the global state of defense AI* (pp. 353-374). Springer. https://doi.org/10.1007/978-3-031-58649-1_16