IKR Publishers

IKR Journal of Engineering and Technology (IKRJET)
Journal homepage: https://ikrpublishers.com/ikrjet/
Volume-2, Issue-4 (July-August) 2026
OPEN ACCESS
ISSN: 3107-7331 (Online)

Reshaping Global Warfare Through Cyber Security and Technology: A Critical Review

Ezirim Kelechi ThankGod[1*], Obi Obichukwu Immanuel[2], Sani Abubakar Muhammed[3], Nwaokolo Ikechukwu Frank[4], Okoronkwo Iheanyi Chinedu[5] & Opara Uchechukwu Victor[6]

[1,2,3,4,5]Mechatronics Engineering Department; Federal University of Technology, Owerri, Imo State, Nigeria

[6]Mechanical Engineering Department Federal University of Technology Owerri Imo State Nigeria

DOI:*10.5281/zenodo.21433577*

ARTICLE INFO

Article history:
Received : 23-06-2026
Accepted : 01-07-2026
Available online : 18-07-2026

Citation: Ezirim, K. T., Obi, O. I., Sani, A. M., Nwaokolo, I. F., Okoronkwo, I. C., & Opara, U. V. (2026). Reshaping Global Warfare Through Cyber Security and Technology: A Critical Review. *IKR Journal of Engineering and Technology (IKRJET), 2*(4), 41-44.

ABSTRACT **Review Article**

Cyber as Cyber security and emerging technologies are redefining the logic and operational mechanism of the entire global conflict. This chapter critically reviews how offensive cyber operations, defensive resilience, artificial intelligence, autonomous systems, and information warfare have shifted competition from kinetic and physical dominance to control of networks, algorithms, and perception. With reference to military doctrine, post-2020 case studies, and peer-reviewed publications, a critical assessment of five domains viz:

(a) an operational domain;
(b) AI and autonomous weapons;
(c) cyber-physical attacks on critical infrastructure;
(d) information operations and cognitive warfare; and
(e) emerging governance and norms.

Evidence from Ukraine, ransomware campaigns, and Department of Defense AI programs confirms that technology lowers the threshold for conflict and increases the role of non - state actors (Horowitz, 2021; Scharre, 2024).

However, strategic outcomes reasonably still depend on organizational capacity, data infrastructure, and legal frameworks rather than technology alone (U.S. Department of Defense, 2020; Bistron & Piotrowski, 2021). Hence, the enumeration of design principles for resilient defense and recommendations for multilateral norms to manage escalation in an increasingly digital battlespace.

Keywords: Cyber Warfare, Cybersecurity, Artificial Intelligence, Autonomous Weapons, Critical Infrastructure, Information Operations, Norms.

**Corresponding author: Ezirim Kelechi ThankGod*
Mechatronics Engineering Department; Federal University of Technology, Owerri, Imo State, Nigeria

Introduction

Warfare in the 2020s is increasingly fought in and through digital infrastructure. Three notable shifts among others define this period to wit: Firstly, cyberspace was formally but unofficially integrated into joint military doctrine as a contested domain, with cyber effects used alongside kinetic operations in conflicts such as Ukraine (NATO Cooperative Cyber Defense Centre of Excellence [CCDCOE], 2022). Secondly, artificial intelligence moved from research labs to operational systems for Intelligence, Surveillance and Reconnaissance (ISR) analysis, logistics, and decision support (U.S. Department of Defense, 2020). Thirdly, generative AI and ransomware lowered the barrier for influence operations and disruption by non-state actors (Greenberg, 2022; Maibach et al., 2023). [DoD]

This chapter further attempts to review how cyber security and technology are reshaping global warfare since 2020 by addressing three critical questions:

1. How have cyber operations and AI changed conflict dynamics?
2. What vulnerabilities have emerged in critical infrastructure and information environments?

3. What governance gaps exist and how can resilience be built?

It's relatively argued that while technology creates new capabilities, strategic advantage rather accrues to actors that integrate tools with doctrine, training, and norms (Horowitz, 2021; Scharre, 2024).

Cyber Operations as an Operational Domain

The 2022 conflict in Ukraine marked the first obvious and noted large - scale war where cyber operations were coordinated with conventional military operations from day one (NATO CCDCOE, 2022). Russian actors deployed wiper malware such as WhisperGate and HermeticWiper against Ukrainian government and financial networks, while Ukrainian and allied actors on the other hand used cyber tools for disruption and intelligence collection (Microsoft, 2022).

Offensive Trends: 2020–2025

Cyber-attacks whether intentional or unintentional increasingly target civilian systems to create strategic effect. The 2021 Colonial Pipeline ransomware attack among others caused fuel shortages across the U.S. East Coast, demonstrating how criminal groups can generate national - level disruption (Cybersecurity and Infrastructure Security Agency [CISA], 2021). The 2023 MOVEit vulnerability exploitation affected hundreds of organizations globally, showing supply chain risk and vulnerable exposure to cyber-attacks (CISA, 2023).

Defensive Resilience:

Cyber security in some quarters is now framed as operational resilience by some schools of thought. The Department of Defense Artificial Intelligence Strategy emphasized that data, talent, and infrastructure are prerequisites for effective cyber defense (DoD, 2020). Zero-trust architecture, segmentation, and rapid incident response have become additional standard doctrine for critical networks (CISA, 2022).

Vital Insight

Cyber operations on themselves alone rarely achieve decisive effects. Rather more often than not, they function as "shaping" tools that degrade command and control, logistics, and public confidence before or alongside kinetic operations (NATO CCDCOE, 2022).

Artificial Intelligence and Autonomous Systems

AI adoption and acceptability radically increased after 2020 through programs like department of defense Project Maven and the Joint All-Domain Command and Control initiative (DoD, 2020).

Perception and Intelligence Surveillance & Reconnaissance

Interestingly, machine learning models presently process satellite and drone imagery at scale. What required hours of analyst time in 2019 can now be completed in minutes by 2023, compressing the observe-orient-decide-act loop (Horowitz, 2021). This increases tempo but unavoidably shifts the risk to verification and human oversight.

Autonomy:

Loitering munitions and drone swarms with onboard AI for navigation and target selection were widely used in Ukraine after 2022 (Scharre, 2024) and presently in Iran in 2026 by the US and Israel. DoD Directive 3000.09, updated in 2023 guidance, continues to require human judgment for lethal force, but the technical capability for higher autonomy exists (DoD, 2012/2023).

Risks:

AI systems are undisputably vulnerable to adversarial examples and data poisoning, as well as data corruption which can grossly degrade the optimal performance under electronic warfare conditions (Bistron & Piotrowski, 2021). Bias and mistrust in training data can also adversely affect targeting and collateral damage estimation (Frontera, 2022). Indeed, the speed of AI-assisted decisions has been observed to further increase chances of miscalculation risk during crises (Horowitz, 2021).

Cyber - Physical Attacks on Critical Infrastructure

Critical infrastructure is considered in many quarters as both a civilian necessity and also a military target. Ironically, technology makes these systems efficient but interdependent and vulnerable (Zheng et al., 2024).

Selected Major Incidents Between 2020–2025:

1. Ransomware in healthcare: Healthcare systems globally faced repeated attacks, with 2021–2023 showing increased targeting of hospitals during COVID-19 recovery (NHS Digital, 2022).
2. Colonial Pipeline, 2021: A ransomware attack disrupted fuel distribution for 5,500 miles of pipeline, prompting the first U.S. emergency declaration for a cyber incident (CISA, 2021).
3. Ukraine energy grid, 2022–2023: Repeated cyber-attacks targeted energy infrastructure during winter, combining cyber and kinetic effects to maximize civilian impact (Microsoft, 2022).

Resilience Principles:

Estonia's post-2007 model of cyber resilience emphasizing data backups, distributed systems, and whole - of - society training has been adopted by NATO members after 2020 as a baseline (NATO CCDCOE, 2022). CISA's 2022 Zero Trust Maturity Model provides a framework now adopted by U.S. federal agencies (CISA, 2022).

Information Operations and Cognitive Warfare

Post - 2022 era in human history overwhelmingly experienced Generative AI transformed information

operations by enabling cheap, high-volume, personalized content (Maibach et al., 2023; Zheng et al., 2024).

Mechanisms 2020–2025:

1. Deepfakes and synthetic media: Used to impersonate officials and spread false orders, including a 2023 deepfake of the Ukrainian president surrendering (NATO Strategic Communications Centre of Excellence [StratCom COE], 2023).
2. Algorithmic amplification: Platforms amplify and exaggerate emotionally charged content, which adversarial actors exploit to polarize audiences (Lewandowsky et al., 2022).
3. Microtargeting: Data-driven messaging adapts framing to individual values, greatly increasing persuasion but constrained by raising privacy concerns (Ballew et al., 2021).

Cognitive impact and defense:

"Cognitive warfare" targets reasoning processes attention, memory, and trust promotion rather than just information accuracy (Pernik, 2022). It was observed that "Inoculation" or pre-bunking interventions developed between 2020–2022 aided the reduction of susceptibility to misinformation by exposing audiences to weakened forms of manipulation techniques (van der Linden et al., 2020). Little wonder, NATO StratCom COE (2023) maintains that Platform transparency and media literacy are now central to NATO's information defense doctrine.

Governance, Norms, and Escalation Control

It appears technology is evolving at a faster rate than relevant regulatory legal regime. Considering four challenges that dominate post-2020 era to wit:

1. Attribution: States and proxies mask cyber operations, complicating deterrence (Rid & Buchanan, 2020).
2. Escalation risk: Machine - speed AI decisions compress deliberation time, increasing risk of unintended escalation during crises (Horowitz, 2021).
3. International law: The Tallinn Manual 2.0 updated with 2021 commentary, clarifies how international humanitarian law applies to cyber operations, but operationalizing "distinction" and "proportionality" remains difficult when civilian networks are dual - use (Schmitt, 2021).
4. Autonomous weapons: No binding treaty exists on lethal autonomous weapons systems as of 2025, though the UN Group of Governmental Experts continues negotiations (UN GGE, 2021).

Emerging norms 2021–2025

The UN GGE 2021 report affirmed that states should not conduct cyber operations against critical infrastructure and should cooperate on attribution (UN GGE, 2021). Similarly, NATO's 2022 Strategic Concept explicitly includes cyber and emerging tech as core tasks. The U.S. launched the Joint Cyber Defense Collaborative in 2021 to improve public - private coordination (CISA, 2022).

All these efforts were geared towards reasonable control of application in the engagement of machine learning and AI driven- cyber security weapons.

Critical Assessment and Prospective Target

Post-2020 evidence conspicuously reveals three major consistent patterns viz:

1. Lowered barriers: Ransomware groups and small states can achieve strategic disruption previously limited to great powers (Greenberg, 2022).
2. Blurred boundaries: War and peace, civilian and military infrastructure, human and machine decision are increasingly overlapping (Scharre, 2024).
3. Organizational advantage: Technical tools matter less than data infrastructure, doctrine, and civil-military coordination (DoD, 2020; Horowitz, 2021).

Prospective Research Priorities 2024–2026:

1. Human-machine teaming: Design AI systems that handle data fusion while humans retain mission command and ethical judgment (Scharre, 2024).
2. Resilience by design: Build critical systems assuming breach, with redundancy, offline backups, and rapid recovery (CISA, 2022; Zheng et al., 2024).
3. Norms and verification: Develop multilateral agreements on responsible cyber behavior and limits on autonomous weapons, with verification mechanisms (UN GGE, 2021).
4. Cognitive defense: Scale pre-bunking and media literacy programs to build societal resistance to manipulation (van der Linden et al., 2020).

Conclusion

It's obvious that between 2020–2025, cyber security and technology have undeniably moved from supporting tools to central drivers of military strategy. Unfortunately, Conflict is becoming faster, more frequent, more diffuse, and more cognitive (Horowitz, 2021; Scharre, 2024). Thus, opening up for strategic advantage going to actors that treat cyber and AI as socio-technical systems, and not just merely software (DoD, 2020). Admittedly, without governance, technology makes war more frequent, lucrative and ambiguous but with governance and regulation, it can make war more controllable and less destructive both to humans and non - humans.

References

1. Ballew, M. T., Maibach, E., Kotcher, J., Bergquist, P., & Leiserowitz, A. (2021). Values and climate change: A field experiment on the effects of value-congruent messaging. Journal of Environmental Psychology, 74, 101576. https://doi.org/10.1016/j.jenvp.2021.101576.
2. Bistron, M., & Piotrowski, Z. (2021). Artificial intelligence applications in military systems and their

influence on sense of security of citizens. Sensors, 21(8), 2631. https://doi.org/10.3390/s21082631.
3. Cybersecurity and Infrastructure Security Agency. (2021). Ransomware attack on Colonial Pipeline. https://www.cisa.gov/news/2021/05/10/ransomware-attack-colonial-pipeline.
4. Cybersecurity and Infrastructure Security Agency. (2022). Zero trust maturity model(Version 1.0). https://www.cisa.gov/zero-trust-maturity-model.
5. Cybersecurity and Infrastructure Security Agency. (2023). MOVEit transfer vulnerability exploitation. https://www.cisa.gov/news-events/alerts/2023/06/01/moveit-transfer-vulnerability-exploitation.
6. Frontera, L. (2022). The comparative ethics of artificial-intelligence methods for military applications. Frontiers in Big Data, 5, 991759. https://doi.org/10.3389/fdata.2022.991759.
7. Greenberg, A. (2022). Tracers in the dark: The global hunt for the crime lords of cryptocurrency. Doubleday.
8. Horowitz, M. C. (2021). The race to develop military AI. Army University Press. https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2021-OLE/The-Coming-Military-AI-Revolution.
9. Lewandowsky, S., van der Linden, S., & Cook, J. (2022). The effects of automated fact-checking interventions on the spread of misinformation. Nature Human Behaviour, 6(8), 1123–1131. https://doi.org/10.1038/s41562-022-01428-6.
10. Maibach, E., Zhao, X., & Witte, J. (2023). Communicating climate change with generative AI: Effects of disclosure and framing. Climatic Change, 176(5), 59. https://doi.org/10.1007/s10584-023-03545-1.
11. Microsoft. (2022). Defending Ukraine: Early lessons from the cyber war. https://www.microsoft.com/en-us/download/details.aspx?id=104532.
12. NATO Cooperative Cyber Defense Centre of Excellence. (2022). Cyber operations in Ukraine: 24 February – 31 December 2022. https://ccdcoe.org/uploads/2023/01/CCDCOE_Ukraine_Cyber_Operations_Report_2022.pdf.
13. NATO Strategic Communications Centre of Excellence. (2023). Deepfakes and disinformation in the Russia-Ukraine war. https://stratcomcoe.org/publications/deepfakes-and-disinformation-in-the-russia-ukraine-war/251.
14. NHS Digital. (2022). Data security and protection toolkit: Annual report 2021/22. https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance.
15. Pernik, P. (2022). Cognitive warfare: An attack on truth and thought. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/cognitive-warfare-an-attack-on-truth-and-thought/220
16. Rid, T., & Buchanan, B. (2020). Attributing cyber-attacks after 2018: An update. Journal of Strategic Studies, 43(4), 509–531. https://doi.org/10.1080/01402390.2019.1668132.
17. Scharre, P. (2024). Four battlegrounds: Power in the age of artificial intelligence. W. W. Norton & Company.
18. Schmitt, M. N. (2021). Tallinn Manual 2.0 on the international law applicable to cyber operations (2nd ed., updated commentary). Cambridge University Press.
19. United Nations Group of Governmental Experts. (2021). Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace. UN Document A/76/135.
20. U.S. Department of Defense. (2012, updated 2023). Directive 3000.09: Autonomy in weapon systems. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf.
21. U.S. Department of Defense. (2020). DoD artificial intelligence strategy: Harnessing AI to advance our security and prosperity. https://www.ai.mil/docs/DoD_AI_Strategy.pdf.
22. van der Linden, S., Roozenbeek, J., & Compton, J. (2020). Inoculating against misinformation. Science, 368(6488), 235–237. https://doi.org/10.1126/science.aaz5496.
23. Zheng, L., Li, N., Zhang, T., & Chen, X. (2024). Evaluating the carbon footprint of generative AI in communication workflows. Sustainable Computing: Informatics and Systems, 38, 100892. https://doi.org/10.1016/j.suscom.2024.100892.