Policy Perspectives
No:6 | June 2025

Photo Credit: Designed by IPATC

The Digital Warfare: An Emerging Challenge

Authors

Prof Siphamandla Zondi: IPATC and Institute for Global African Affairs; University of Johannesburg (UJ), South Africa.

Ms Naledi Ramontja: Researcher, IPATC UJ, South Africa.

Abstract

- The integration of digital technologies and the deployment of weapons of war is a growing and complex challenge
- Digital warfare poses the risk of expanding, increasing, and intensifying wars and conflicts, making them harder to manage and resolve
- The use of digital technologies in conflict raises the risk of escalation, often with no oversight mechanisms in place
- Digital warfare places us into catastrophic errors of algorithms that have no human heart
- The policy note calls for urgent responses, including updating laws, regulations, norms, and standards on the use and abuse of digital technologies in wars

5 Molesey Avenue, Auckland Park 2029, Johannesburg, South Africa.

+27 11 559 7230 http://ipatc.joburg

Introduction

The recent Operation Spider Web conducted by Ukraine against Russian targets exemplifies the rapid evolution and proliferation of digital technologies in modern conflict. The integration of drones, artificial intelligence (AI), cyber capabilities, and networked systems presents profound challenges to global security, humanitarian protection, arms control, and strategic stability. These technologies lower barriers to lethal force, accelerate decision cycles, complicate attribution, and create significant risks of unintended escalation and violations of International Humanitarian Law (IHL). Urgent multilateral action is needed to develop norms, enhance resilience, and establish governance frameworks for these rapidly advancing capabilities before they further destabilize the international order.

The Digital Warfare Landscape: Key Technologies & Trends:

Proliferation of Unmanned Systems (Drones):

Commercial and military drones offer unprecedented Intelligence, Surveillance, Reconnaissance (ISR) and strike capabilities at low cost. Swarming technology (multiple drones coordinating autonomously) amplifies this threat, enabling saturation attacks and complex operations like Spider Web. Their accessibility empowers non-state actors and smaller states (Johnson, 2023).

Integration of Artificial Intelligence (AI):

AI is used for target identification, battle management, cyber operations, logistics optimization, and enabling autonomy in weapons systems. While potentially increasing precision, AI introduces risks of algorithmic bias, unanticipated failures, lack of human judgment in lethal decisions ("meaningful human control"), and vulnerability to data poisoning or adversarial attacks (Scharre, 2024).

Convergence of Cyber & Kinetic Effects:

Operations like Spider Web demonstrate the blending of cyber-attacks (disabling sensors, networks) with drone strikes. Cyber capabilities can cripple infrastructure, spread disinformation, and create openings for physical attacks, blurring the lines between traditional domains and complicating defense and response (Rid & Buchanan, 2023).

Increased Autonomy:

The trend towards greater autonomy in weapons systems (from automated defenses to potential LAWS) raises fundamental ethical, legal, and strategic questions about accountability and the role of human judgment in the use of force (ICRC, 2021).

Core Challenges Posed:

1. Erosion of the Threshold for Conflict: Low-cost drones and accessible cyber tools lower the barrier to initiating armed attacks or provocative acts, potentially leading to more frequent, smaller-scale conflicts or "constant conflict" below the threshold of war (Freedman, 2022).
2. Accountability and IHL Complience:

- *Attribution Difficulty:* Cyber-attacks and drone strikes using commercial platforms are notoriously hard to attribute quickly and reliably, hindering accountability and retaliation (Lin, 2023).
- *Precision vs. Collateral Damage:* While touted for precision, algorithmic errors, sensor failures, or flawed data can lead to catastrophic mistakes and civilian casualties. Verifying compliance with proportionality and distinction principles is complex (Human Rights Watch, 2022).
- *Autonomy & Accountability Gap:* Who is responsible if an autonomous weapon makes an unlawful decision? The operator, programmer, commander, or the machine itself? This gap threatens core IHL principles (Asaro, 2023).

3. Escalation Risks:

- *Speed & Miscalculation:* AI-driven systems and rapid drone/counter-drone engagements compress decision times, increasing the risk of rapid, unintended escalation based on misinterpreted data or automated responses (Horowitz, 2024).
- *Entanglement:* Attacks on dual-use infrastructure (e.g., power grids hit by cyber/drone attacks essential for civilian life and military operations) can have cascading effects, drawing in more actors or escalating conflict levels unpredictably (Acton et al., 2023).

4. Strategic Instability:

- *Arms Racing:* Intense competition in AI, autonomous systems, and counters to drones/cyber threats fuels a new arms race, diverting resources and increasing tensions (SIPRI, 2024).
- *Vulnerability of Critical Infrastructure:* Societies are increasingly vulnerable to disruptive cyber and drone attacks on power, communications, and finance, creating significant societal and economic risks even outside declared conflicts (Lewis, 2023).

5. Empowerment of Non State Actors:

- These technologies are relatively accessible, allowing insurgent groups and terrorists to conduct sophisticated attacks, gather intelligence, and challenge state forces asymmetrically, as seen globally (Bunker, 2023).

Policy Recommendations

1. Strengthen Norms and International Law: Intensify diplomatic efforts within the UN GGE on LAWS and other forums to develop legally binding rules prohibiting AWS operating without meaningful human control (GGE on LAWS, 2023). Clarify and reaffirm the application of existing IHL (Geneva Conventions, Additional Protocols) to all digital warfare technologies. Promote new norms against attacking critical civilian infrastructure with cyber or drone strikes.
2. Enhance Resilience and Defense: Invest significantly in R&D for counter-drone (C-UAS) and cyber defense technologies, including AI-enabled detection and mitigation. Harden critical national infrastructure against cyber and physical drone attacks. Develop robust attribution capabilities for both state and non-state actors.
3. Promote Transparency and Risk Reduction: Establish multilateral dialogues and confidence-building measures (CBMs) focused on digital warfare risks, including incident communication

hotlines. Encourage voluntary transparency reports on military AI and autonomous system policies. Develop shared protocols for investigating and responding to ambiguous attacks.

4.Responsible Development and Export Controls: Implement stringent national and multilateral export controls on advanced military AI, drone swarm technologies, and offensive cyber tools (akin to MTCR for missiles). Establish ethical guidelines for the development and deployment of military AI within national defense establishments.

5.Invest in Legal and Ethical Frameworks: Support legal research and training for militaries and policymakers on IHL compliance in digital warfare. Foster multidisciplinary dialogue involving technologists, ethicists, lawyers, and policymakers.

Conclusion

The digitalization of war, vividly demonstrated by operations like Spider Web, is not a distant future but a present reality. The challenges posed by drones, AI, and cyber capabilities are complex, multifaceted, and evolving rapidly. Without proactive, collaborative, and decisive international action to establish effective governance, enhance resilience, and uphold humanitarian law, the risks of unintended escalation, widespread harm to civilians, erosion of accountability, and strategic instability will continue to grow. Addressing these challenges must be an urgent priority for the international community.

References

Acton, J. M., Vaddi, P., & Williams, H. (2023). Escalation and Entanglement: How the Ukraine War Could Go Nuclear. Carnegie Endowment for International Peace.

Arkin, R. C. (2023). Ethical Issues in Lethal Autonomous Systems. Georgia Institute of Technology (Working Paper).

Asaro, P. (2023). The Liability Problem for Autonomous Weapon Systems. International Committee for Robot Arms Control (ICRAC).

Bunker, R. J. (Ed.). (2023). Non-State Actors and Drone Warfare. Routledge.

Freedman, L. (2022). The Future of War: A History. PublicAffairs.

Group of Governmental Experts (GGE) on Lethal Autonomous Weapons Systems (LAWS). (2023). Report of the 2023 Session of the GGE on LAWS. United Nations Office at Geneva (CCW/GGE.2/2023/3).

Horowitz, M. C. (2024). Artificial Intelligence, International Competition, and the Balance of Power. Texas National Security Review, 8(1).

Human Rights Watch (HRW). (2022). Heed the Call: A Moral and Legal Imperative to Ban Killer Robots.

International Committee of the Red Cross (ICRC). (2021). Ethical Principles for the Development, Deployment, and Use of Artificial Intelligence in Armed Conflict.

Johnson, J. (2023). The AI-Enabled Future of Drone Warfare: Swarming and Beyond. Royal United Services Institute (RUSI) Occasional Paper.

Lewis, J. A. (2023). Securing Cyberspace: Strategies for Defense and Deterrence. Center for Strategic and International Studies (CSIS).

Lin, H. (2023). Attribution of Malicious Cyber Incidents: From Soup to Nuts. Journal of Cybersecurity, 9(1).

Rid, T., & Buchanan, B. (2023). The Convergence of Cyber and Kinetic War. International Security, 48(2), 7-44.

Scharre, P. (2024). Four Battlegrounds: Power in the Age of Artificial Intelligence. W.W. Norton & Company.

Stockholm International Peace Research Institute (SIPRI). (2024). SIPRI Yearbook 2024: Armaments, Disarmament and International Security. Oxford University Press. (Chapter on AI & Automation).