

Legal and Ethical Challenges of Asymmetric Warfare - Technological Breakthroughs as a Model

Ahmed Khaldi*

University of Djelfa
ahmedkhaldi135@gmail.com

📅📅📅

Date of submission: 07/10/2024

- Date of acceptance: 02/01/2026

- Date of publication: 05/01/2026

ABSTRACT:

This article examines the legal and ethical challenges posed by asymmetric warfare in the context of rapid technological advancements. It focuses on how emerging technologies such as cyber warfare, artificial intelligence, drone technology, and information warfare have transformed the nature of conflicts, creating new dilemmas for international law and ethics. The study analyzes the applicability of existing legal frameworks, particularly international humanitarian law, to these modern forms of warfare. It also explores the ethical implications of using advanced technologies in asymmetric conflicts, including issues of proportionality, distinction, human control, and privacy. Through case studies and an examination of potential future scenarios, the article highlights the urgent need for updated legal and ethical frameworks to address the complexities of technologically-driven asymmetric warfare.

key words: Asymmetric warfare, technological breakthroughs, international humanitarian law, ethics of war, cyber warfare.

Introduction:

In the evolving landscape of global conflicts, asymmetric warfare has emerged as a dominant paradigm, challenging traditional notions of combat and blurring the lines between state and non-state actors. This shift in the nature of warfare has been significantly amplified by rapid technological advancements, which have introduced new dimensions to military engagements and strategic

* - Author Correspondent:

thinking. As nations and non-state entities alike harness the power of cutting-edge technologies, from cyberwarfare capabilities to autonomous weapons systems, the legal and ethical frameworks governing armed conflicts face unprecedented challenges.

The concept of asymmetric warfare, characterized by a significant disparity in military capabilities or strategies between opposing forces, is not new. However, the integration of advanced technologies has dramatically altered its dynamics. Cyber attacks can cripple critical infrastructure without a single shot being fired; artificial intelligence can make split-second decisions on the battlefield; drones can conduct surveillance and strikes with minimal risk to the operator; and information warfare can sway public opinion and destabilize societies from afar. These technological breakthroughs have not only changed how wars are fought but have also raised profound questions about the applicability of existing international laws and ethical norms in this new era of conflict.

This article aims to examine the complex interplay between asymmetric warfare, technological innovation, and the legal and ethical challenges that arise from this intersection. By focusing on technological breakthroughs as a model, we seek to illuminate the broader implications for international humanitarian law, the ethics of war, and the future of global security. Our analysis will delve into the specific legal quandaries posed by cyber warfare, autonomous weapons, and information operations, while also grappling with the ethical dilemmas of proportionality, distinction, and human control in an increasingly automated battlespace.

As we navigate these intricate issues, this study will argue that the international community must urgently adapt and expand its legal and ethical frameworks to address the realities of technologically-driven asymmetric warfare. Only through a comprehensive reevaluation of our approach to regulating armed conflicts can we hope to uphold the principles of humanity and the rule of law in the face of rapidly evolving military technologies.

II. Understanding Asymmetric Warfare

A. Definition and Characteristics:

Asymmetric warfare, in its broadest sense, refers to a conflict between belligerents whose relative military power, strategy, or tactics differ significantly¹. This form of warfare is characterized by the use of unexpected or unconventional

¹ Arquilla, J., & Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. RAND Corporation. (p. 6)□

approaches to exploit an opponent's weaknesses, often by a militarily inferior force against a superior one.¹

The concept encompasses a wide range of scenarios, from guerrilla tactics employed by insurgent groups to sophisticated cyber attacks launched by state actors.

Key characteristics of asymmetric warfare include:

1. Disparity in resources and capabilities between opposing forces
2. Use of unconventional tactics and strategies
3. Exploitation of technological or psychological advantages
4. Blurring of lines between combatants and civilians
5. Prolonged, low-intensity conflicts rather than decisive battles².

In the context of technological breakthroughs, asymmetric warfare has taken on new dimensions. Advanced technologies have become force multipliers, allowing weaker parties to challenge stronger opponents in ways previously unimaginable. For instance, a small group of hackers can potentially disrupt the critical infrastructure of a powerful nation, demonstrating how technology can level the playing field in asymmetric conflicts.³

B. Historical Context:

The concept of asymmetric warfare is not a modern invention. Throughout history, military leaders have sought to gain advantages by exploiting asymmetries in warfare. Notable historical examples include:

1. The guerrilla tactics used by Spanish resistance fighters against Napoleon's forces in the early 19th century⁴.
2. The Vietnam War, where the Viet Cong's unconventional tactics challenged the superior military might of the United States⁵.

¹ Lele, A. (2014). Asymmetric warfare: A state vs non-state conflict. OASIS, 20, 97-111. (p. 99)

² Thornton, R. (2007). Asymmetric warfare: Threat and response in the 21st century. Polity Press. (p. 22)

³ Clarke, R. A., & Knake, R. K. (2010). Cyber war: The next threat to national security and what to do about it. Ecco. (p. 70)

⁴ Esdaile, C. J. (2004). Fighting Napoleon: Guerrillas, bandits and adventurers in Spain, 1808-1814. Yale University Press. (p. 154)

⁵ Karnow, S. (1997). Vietnam: A history. Penguin Books. (p. 265)

3. The Afghan Mujahideen's resistance against the Soviet occupation in the 1980s¹.

These historical instances demonstrate that asymmetric approaches have long been a feature of warfare, particularly in conflicts involving disparities in military power or when local forces face foreign invaders.

C. Evolution in the 21st Century:

The 21st century has witnessed a significant evolution in the nature and scope of asymmetric warfare, driven largely by technological advancements and changing geopolitical dynamics. Key factors contributing to this evolution include:

1. **Globalization and Interconnectedness:** The increasing interconnectedness of global systems has created new vulnerabilities that can be exploited in asymmetric conflicts.²
2. **Technological Proliferation:** The widespread availability of advanced technologies has enabled both state and non-state actors to access sophisticated military capabilities.³
3. **Information Revolution:** The rise of the internet and social media has transformed information warfare, making it a critical component of modern asymmetric conflicts.⁴
4. **Urbanization:** The growth of urban areas has shifted the battlespace to cities, complicating military operations and increasing the risk to civilians.⁵
5. **Non-State Actors:** The rise of influential non-state actors, including terrorist organizations and private military companies, has further blurred the lines in asymmetric conflicts.⁶

In this evolving landscape, technological breakthroughs have played a pivotal role in shaping modern asymmetric warfare. Cyber capabilities, artificial intelligence, autonomous systems, and advanced communications technologies

¹ Grau, L. W., & Gress, M. A. (2002). *The Soviet-Afghan War: How a superpower fought and lost*. University Press of Kansas. (p. 315)

² Nye Jr, J. S. (2011). *The future of power*. PublicAffairs. (p. 150)

³ Kramer, F. D. (2009). *Cyberpower and national security*. National Defense University Press. (p. 48)

⁴ Libicki, M. C. (2007). *Conquest in cyberspace: National security and information warfare*. Cambridge University Press. (p. 89)

⁵ Graham, S. (2010). *Cities under siege: The new military urbanism*. Verso Books. (p. 60)

⁶ Kaldor, M. (2012). *New and old wars: Organised violence in a global era*. Polity Press. (p. 172)

have become integral to military strategies, offering new avenues for asymmetric approaches while also presenting novel challenges to international law and ethics.

III. Technological Breakthroughs in Warfare:

A. Cyber Warfare:

Cyber warfare has emerged as a critical domain in modern asymmetric conflicts, offering state and non-state actors the ability to inflict significant damage on adversaries with minimal physical risk. Key aspects of cyber warfare include:

1. **Infrastructure Attacks:** Targeting critical infrastructure such as power grids, financial systems, and transportation networks.¹
2. **Data Breaches:** Theft or manipulation of sensitive information for strategic advantage.²
3. **Disinformation Campaigns:** Using digital platforms to spread false information and manipulate public opinion.³

The Stuxnet worm, which targeted Iranian nuclear facilities in 2010, exemplifies the potential of cyber weapons in asymmetric warfare, demonstrating how a sophisticated cyber attack can cause physical damage to industrial systems.

B. Artificial Intelligence and Autonomous Weapons:

The integration of artificial intelligence (AI) into military systems has revolutionized warfare, introducing new capabilities and ethical dilemmas:

1. **Autonomous Weapons Systems:** Weapons capable of selecting and engaging targets without human intervention.⁴
2. **AI-Driven Decision Making:** Using AI to process vast amounts of data for strategic and tactical decision-making.⁵
3. **Predictive Analytics:** Employing AI to forecast enemy movements and optimize military operations.¹

¹ Brenner, S. W. (2009). *Cyberthreats: The emerging fault lines of the nation state*. Oxford University Press. (p. 71)

² Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age*. Crown. (p. 167)

³ Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Eamon Dolan/Houghton Mifflin Harcourt. (p. 205)

⁴ Krishnan, A. (2009). *Killer robots: Legality and ethicality of autonomous weapons*. Ashgate Publishing. (p. 33)

⁵ Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review*, 1(3), 36-57. (p. 42)

The development of autonomous weapons systems, in particular, has sparked intense debate about the ethical implications of removing human decision-making from lethal force.

C. Drone Technology:

Unmanned aerial vehicles (UAVs) or drones have become ubiquitous in modern warfare, offering significant advantages in surveillance, reconnaissance, and strike capabilities:

1. **Precision Strikes:** Ability to conduct targeted attacks with reduced collateral damage.
2. **Persistent Surveillance:** Long-endurance missions for intelligence gathering.
3. **Force Protection:** Reducing risk to personnel by removing them from dangerous environments .²

The proliferation of drone technology has enabled even non-state actors to conduct sophisticated aerial operations, as evidenced by the use of commercial drones by insurgent groups in recent conflicts .

D. Information Warfare and Social Media:

The digital age has transformed information into a powerful weapon, with social media platforms becoming battlegrounds for influence and perception management:

1. **Social Media Manipulation:** Using platforms to spread propaganda and influence public opinion.
2. **Fake News and Deep Fakes:** Creating and disseminating false or manipulated content to deceive and mislead.
3. **Cognitive Hacking:** Exploiting cognitive biases to influence decision-making processes.³

¹ Work, R. O., & Brimley, S. (2014). 20YY: Preparing for war in the robotic age. Center for a New American Security. (p. 22)

² Kaag, J., & Kreps, S. (2014). Drone warfare. Polity Press. (p. 81)

³ Szfranski, R. (1997). A theory of information warfare: Preparing for 2020. Airpower Journal, 11(1), 56-65. (p. 59)

The alleged Russian interference in the 2016 U.S. presidential election illustrates the potential of information warfare to impact national security and democratic processes .

IV. Legal Challenges:

The rapid evolution of asymmetric warfare, driven by technological advancements, has created significant challenges for existing legal frameworks, particularly international humanitarian law (IHL) and the laws of armed conflict.

A. International Humanitarian Law and its Applicability:

International Humanitarian Law, primarily codified in the Geneva Conventions and their Additional Protocols, faces considerable strain in its application to modern asymmetric conflicts , Key challenges include:¹

1. **Defining Armed Conflict:** The blurred lines between cyber operations, information warfare, and traditional armed conflict complicate the determination of when IHL applies.
2. **Principle of Distinction:** Technological advancements, particularly in cyber and information warfare, make it increasingly difficult to distinguish between military and civilian targets.
3. **Principle of Proportionality:** Assessing proportionality becomes more complex when dealing with non-kinetic attacks that may have wide-ranging, indirect effects.

B. Jus ad Bellum and Jus in Bello in Asymmetric Conflicts:

The principles of jus ad bellum (the right to go to war) and jus in bello (the conduct of war) face new challenges in the context of asymmetric warfare:

1. **Use of Force Thresholds:** Determining when cyber attacks or other non-traditional forms of aggression constitute an "armed attack" under the UN Charter.²
2. **Self-Defense in Cyberspace:** The legality and limits of self-defense actions in response to cyber attacks or other technologically-driven asymmetric threats.¹

¹ Schmitt, M. N. (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press. (p. 75)

² Waxman, M. C. (2011). Cyber-attacks and the use of force: Back to the future of article 2(4). Yale Journal of International Law, 36, 421-459. (p. 431)

3. **Non-State Actors:** The application of jus ad bellum to conflicts involving non-state actors, particularly in the context of transnational terrorist networks.²

C. Legal Status of Combatants in Technologically-Driven Asymmetric Warfare:

The use of advanced technologies in warfare raises questions about the legal status of various actors:

1. **Civilian Participation:** The involvement of civilian technicians and programmers in military cyber operations blurs the line between combatants and civilians.
2. **Autonomous Systems:** The legal status of AI-driven autonomous weapons systems and the question of accountability for their actions.
3. **Remote Operators:** The combatant status of drone operators and cyber warfare specialists operating far from the traditional battlefield.³

D. Attribution and Accountability in Cyber Attacks:

The anonymous and often untraceable nature of cyber attacks poses significant challenges for legal accountability:

1. **Technical Attribution:** The difficulty of conclusively identifying the source of cyber attacks, complicating efforts to hold actors accountable.
2. **State Responsibility:** Determining state responsibility for cyber operations conducted by non-state actors or proxies.
3. **Evidentiary Standards:** Challenges in meeting legal standards of proof for cyber activities in international tribunals.⁴

V. Ethical Challenges:

¹ Roscini, M. (2014). Cyber operations and the use of force in international law. Oxford University Press. (p. 106

² Lubell, N. (2010). Extraterritorial use of force against non-state actors. Oxford University Press. (p. 43)□

³ Beard, J. M. (2009). Law and war in the virtual era. American Journal of International Law, 103(3), 409-445. (p. 420)□

⁴ Hollis, D. B. (2007). Why states need an international law for information operations. Lewis & Clark Law Review, 11(4), 1023-1061. (p. 1035)□

The integration of advanced technologies in asymmetric warfare raises profound ethical questions that challenge traditional notions of military ethics and morality in conflict.

A. Proportionality and Distinction in High-Tech Conflicts:

1. **Collateral Damage in Cyber Operations:** Assessing and minimizing unintended consequences of cyber attacks on civilian infrastructure and services.
2. **Precision vs. Indiscriminate Effects:** Balancing the potential for precise targeting offered by advanced technologies against the risk of indiscriminate effects, particularly in information warfare.
3. **Long-term Impact:** Ethical considerations of actions that may have delayed or long-lasting effects, such as environmental or economic damage from certain types of cyber attacks.¹

B. Human Control vs. Autonomous Decision-Making:

1. **Moral Agency in Autonomous Systems:** The ethical implications of delegating lethal decision-making to AI-driven systems .
2. **Human Judgment in Warfare:** Balancing the potential benefits of AI-driven decision-making against the ethical necessity of human moral judgment in conflict.
3. **Accountability and Responsibility:** Determining ethical responsibility for actions taken by autonomous or semi-autonomous systems.²

C. Privacy and Surveillance Concerns:

1. **Mass Surveillance Technologies:** Ethical implications of using advanced surveillance technologies for military and intelligence purposes.
2. **Data Collection and Use:** Balancing national security needs with individual privacy rights in the collection and analysis of data.
3. **Targeted Digital Profiling:** Ethical considerations in the use of AI and big data analytics for identifying potential threats or targets.¹

¹ Clarke, R. A. (2010). Cyber war: The next threat to national security and what to do about it. Ecco. (p. 189)

² Sparrow, R. (2007). Killer robots. Journal of Applied Philosophy, 24(1),. (p. 65)

D. Ethical Implications of Information Warfare:

1. **Truth and Deception:** The moral dimensions of using disinformation and propaganda as weapons in conflict.
2. **Manipulation of Public Opinion:** Ethical concerns regarding the use of social media and other platforms to influence populations.
3. **Cognitive Liberty:** The right of individuals to make autonomous decisions free from undue technological influence or manipulation [58].²

C. The Future of Warfare Ethics in an Increasingly Digital World

1. **Digital Ethics and Warfare:**
 - The evolution of military ethics in response to the increasing digitalization of warfare .
 - Addressing ethical challenges posed by the blurring of physical and digital battlespaces.³
2. **Global Norms and Values:**
 - The potential for divergent ethical approaches to asymmetric warfare across different cultural and political contexts.
 - Efforts to develop globally accepted ethical norms for the conduct of asymmetric warfare in the digital age.⁴
3. **Long-term Consequences and Responsibility:**
 - Ethical considerations of the long-term impacts of technologically driven asymmetric warfare on global stability and human security.
 - Developing frameworks for assessing and addressing the unintended consequences of new military technologies.¹

¹ Taddeo, M. (2017). The limits of deterrence theory in cyberspace. *Philosophy & Technology*, 30(3), (p. 345)

² Bublitz, J. C. (2013). My mind is mine!? Cognitive liberty as a legal concept. In E. Hildt & A. G. Franke (Eds.), *Cognitive enhancement: An interdisciplinary perspective*. Springer. (p. 240)

³ Floridi, L., & Taddeo, M. (2014). *The Ethics of Information Warfare*. Springer, p. 20

⁴ Roff, H. M. (2019). The Frame Problem: The AI "Arms Race" Isn't One. *Bulletin of the Atomic Scientists*, 75(3), 95-98, p. 96

Conclusion :

The rapid advancement of technology has fundamentally altered the landscape of asymmetric warfare, presenting unprecedented legal and ethical challenges. As we have explored throughout this article, from the evolution of asymmetric warfare to specific case studies and future perspectives, it is clear that existing frameworks are often inadequate to address these new realities.

The international community faces the complex task of balancing the potential benefits of technological innovations in warfare with the need to uphold fundamental principles of international humanitarian law and ethics. This requires a multifaceted approach involving legal adaptation, ethical guideline development, and enhanced international cooperation.

As we look to the future, it is crucial that policymakers, military leaders, technologists, and ethicists work together to develop comprehensive and flexible frameworks that can address the challenges of asymmetric warfare in the digital age. Only through such collaborative efforts can we hope to navigate the complex interplay between technological advancement, legal constraints, and ethical imperatives in the conduct of modern warfare.

The ongoing debates and developments in this field will significantly shape the future of global security, international law, and the ethics of war. As such, continued research, dialogue, and critical examination of these issues remain essential for ensuring that the conduct of warfare, even in its most asymmetric forms, adheres to the fundamental principles of humanity and the rule of law.

List of sources and references:

-Bibliography List setting:

Books:

- [1] Arquilla, J., & Ronfeldt, D. (1997). In Athena's camp: Preparing for conflict in the information age. RAND Corporation.
- [2] Berkowitz, B. (2003). The new face of war: How war will be fought in the 21st century. Free Press.
- [3] Gross, M. L. (2015). The ethics of insurgency: A critical guide to just guerrilla warfare. Cambridge University Press.
- [4] Kaldor, M. (2012). New and old wars: Organized violence in a global era (3rd ed.). Stanford University Press.

¹ Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach. *Science and Engineering Ethics*, 24(2), p. 510.

[5] Singer, P. W. (2009). *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin Press.

Articles:

[6] Beard, J. M. (2014). Law and war in the virtual era. *American Journal of International Law*, 108(3), 409-445.

[7] Blank, L. R. (2017). The limits of inviolability: The parameters for protection of United Nations facilities during armed conflict. *International Law Studies*, 93, 45-101.

[8] Corn, G. S. (2019). Cyber national security: Navigating gray-zone challenges in and through cyberspace. In W. C. Banks (Ed.), *New battlefields/old laws: Critical debates on asymmetric warfare* (pp. 57-74). Columbia University Press.

[9] Schmitt, M. N. (2013). Autonomous weapon systems and international humanitarian law: A reply to the critics. *Harvard National Security Journal*, 4, 1-37.

[10] Watkin, K. (2016). The ICRC updated commentaries: Reconciling form and substance, Part II. *Just Security*. <https://www.justsecurity.org/32538/icrc-updated-commentaries-reconciling-form-substance-part-ii/>

Studies:

[11] Boulanin, V., & Verbruggen, M. (2017). Mapping the development of autonomy in weapon systems. Stockholm International Peace Research Institute.

[12] Lin, P., Bekey, G., & Abney, K. (2008). Autonomous military robotics: Risk, ethics, and design. California Polytechnic State University.

[13] Mayer, J. (2009). The predator war: What are the risks of the C.I.A.'s covert drone program? *The New Yorker*, 85(34), 36-45.

[14] Sander, B. (2017). Cyber insecurity and the politics of international law. *ESIL Reflection*, 6(5).

[15] Sassòli, M. (2006). Transnational armed groups and international humanitarian law. Harvard University Program on Humanitarian Policy and Conflict Research.

Reports:

[16] International Committee of the Red Cross. (2019). International humanitarian law and the challenges of contemporary armed conflicts. 33rd International Conference of the Red Cross and Red Crescent.

[17] United Nations Institute for Disarmament Research. (2015). The weaponization of increasingly autonomous technologies: Considering how meaningful human control might move the discussion forward.

[18] U.S. Department of Defense. (2012). Directive 3000.09: Autonomy in weapon systems.

[19] Human Rights Watch. (2012). Losing humanity: The case against killer robots.