World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

AI at War: The next revolution for military and defense

Ashikur Rahman Nazil *

Department of Computer Science and Information Technology, Belhaven University.

World Journal of Advanced Research and Reviews, 2025, 27(01), 1998-2004

Publication history: Received on 14 June 2025; revised on 18 July 2025; accepted on 22 July 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.1.2735

Abstract

The rapid transformation of Artificial Intelligence (AI) from a disruptive civilian technology into a fundamental component of modern military capability signals a significant shift in warfare and defense. The multifaceted integration of AI across military domains is the subject of this comprehensive study, which examines its current applications, potential for the future, and intricate ethical and strategic ramifications. Autonomous Systems & Robotics (UAVs, UGVs, logistics), Enhanced Data Analysis & Predictive Modeling (intelligence fusion, threat anticipation), Cybersecurity & Network Defense (proactive threat detection, adaptive resilience), AI-augmented Command and Control (C2) (real-time SA, decision support), and Combat Operations Support (target identification, semi-autonomous systems) are some of the key areas we investigate, with a primary focus on the U.S. military but also taking into account AI's role as a force multiplier, enhancing lethality, efficiency, and force protection, is clearly demonstrated by the analysis. However, this revolution presents significant challenges: ethical dilemmas surrounding Lethal Autonomous Weapons Systems (LAWS), the imperative of human oversight (meaningful human control), vulnerabilities in AI systems (adversarial attacks, data poisoning), the risks of an accelerating AI arms race, and the need for robust international governance frameworks. This paper concludes that while AI offers unprecedented advantages in defense preparedness and operational effectiveness, responsible development, rigorous ethical guidelines, robust testing, and international dialogue are paramount to mitigate risks and ensure strategic stability in the emerging AI-augmented battlespace.

Keywords: Artificial Intelligence; Military AI; Autonomous Systems; Cybersecurity; Command and Control; Lethal Autonomous Weapons Systems (LAWS); Military Robotics; Data Analytics; Predictive Modeling; Force Multiplier; Ethical AI; Defense Strategy

1. Introduction

The global landscape is fundamentally changing as a result of the unstoppable advancement of Artificial Intelligence (AI), which is exemplified by breakthroughs in machine learning (ML), deep learning (DL), computer vision, natural language processing (NLP), and autonomous systems. Although it has been widely discussed for its transformative effects on healthcare, finance, and transportation, its most significant and potentially disruptive applications are in the field of warfare and national defense [1].

The "Next Revolution" in military affairs (RMA) is a paradigm shift that is poised to alter the nature of conflict, redefine strategic advantage, and reshape geopolitical power dynamics [2].

The incorporation of AI into military systems is not just an incremental improvement. The fundamental capabilities of AI, which enable real-time decision-making in hyper-dynamic environments and the autonomous operation of sophisticated physical systems, are what make this revolution so significant: processing vast datasets at a rate that is orders of magnitude faster than that of humans; recognizing intricate patterns that are invisible to human analysts.

* Corresponding author: Ashikur Rahman Nazil; ORCID: 0009-0006-8069-2271

Nations that effectively harness these capabilities stand to gain substantial advantages in intelligence, surveillance, and reconnaissance (ISR); command and control (C2); logistics; cyber warfare; and kinetic operations [3].

On the other hand, failing to adapt puts strategic obsolescence at risk.

2. The Need for Military AI: Factors and Settings

The rapid use of AI in defense is driven by a number of converging factors:

Information Overload: Modern sensors (satellites, drones, ground stations, cyber monitoring) generate petabytes of data daily. The overcrowding of traditional human-centric analysis results in critical intelligence gaps and delays [4]. The only viable option for timely processing and exploitation is artificial intelligence. Accelerated Battlefield Tempo: Future conflicts, which involve operations in multiple domains (land, sea, air, space, cyber, electromagnetic spectrum), necessitate rapid decision-making [5]. AI makes it possible to compress the Observe, Orient, Decide, Act (OODA) loop.

Adversarial AI Development: Major powers such as the United States, China, and Russia are putting a significant amount of money into military AI [6]. In order to maintain deterrence and a competitive edge, perceived advantages gained by adversaries create a compelling security imperative for parallel development.

Personnel and Force Multiplier Issues: AI enhances human capabilities, enabling smaller forces to produce greater effects. This is essential in light of recruitment shortages and the need to lessen employees' exposure to high-risk settings [7]. Cost and Efficiency: While research and development is expensive, AI can optimize resource allocation, logistics, predictive maintenance, training, and efficiency [8]. This could potentially reduce long-term operational costs and increase efficiency.

Complexity of Modern Threats: Asymmetric threats, cyber warfare, disinformation campaigns, and hybrid warfare tactics create complex, ambiguous threat landscapes where AI's pattern recognition and predictive capabilities are invaluable [9].

3. Military AI's Main Fields of Use

3.1. Robots and autonomous systems

The foundation of autonomous military platforms of the next generation, AI significantly expands operational reach and reduces personnel risk. Unmanned Aerial Vehicles (UAVs): AI makes it possible for fully autonomous or highly autonomous UAVs to be used for: Long-term surveillance with computer vision-based automated target detection, classification, and tracking is known as persistent ISR [10]. Swarm Operations are coordinated swarms of small, inexpensive drones managed by AI for emergent behavior and resilience (e.g., DARPA's OFFSET, Air Force's Golden Horde) that are capable of overwhelming defenses, distributed sensing, or cooperative strike missions [11]. Loyal Wingman: AI-controlled unmanned combat aerial vehicles (UCAVs) that operate alongside human-piloted fighter jets and carry out jamming, sensing, or weapon delivery under pilot command [12]. UAVs: Artificial Intelligence-driven UGVs are used for: Logistics & Resupply: Autonomous convoys delivering supplies in contested environments (e.g., U.S. variants of the Army's Robotic Combat Vehicle program) [13]. Mine Clearance and Explosive Ordnance Disposal: Improved safety for personnel performing risky bomb disposal tasks. Sentry and reconnaissance work entails patrolling the perimeter, looking into potentially hazardous structures, and maintaining constant surveillance. AI makes it possible for autonomous surface vessels (USVs) and underwater drones (UUVs) to be used in the following applications: Autonomous Sea mine detection and neutralization are known as Mine Countermeasures (MCM). Undersea Warfare: Persistent submarine tracking and oceanographic sensing.

Swarming tactics for patrol or attack missions in surface warfare. Impact: Provides scalable force projection, extends operational endurance, enables access to restricted or hazardous areas, automates tedious or risky tasks, and reduces human life risk.

3.2. Enhanced Data Analysis and Predictive Modeling

The transformation of vast and dispersed data streams into intelligence and foresight that can be put into action is a strength of AI algorithms. Multi-INT Fusion: Artificial intelligence (especially machine learning) combines signals intelligence (SIGINT), geospatial intelligence (GEOINT), human intelligence (HUMINT), open-source intelligence (OSINT), and measurement and signature intelligence (MASINT) into a single operational picture that identifies

correlations and anomalies that humans miss [14]. One example of this is the DoD's Project Maven, which focuses on AI for object detection in video. Predictive Analytics and Threat Prediction: AI models look at environmental factors, current intelligence, and historical data in order to: Predict the intent of the adversary, as well as troop movements and potential attack vectors (kinetic, cyber, and hybrid) [15]. Forecast equipment failures (Predictive Maintenance), optimizing readiness and logistics [16].

Improve your emergency planning by wargaming complex scenarios. Automated Intelligence Processing: NLP algorithms speed up the intelligence cycle by translating, summarizing, and extracting key entities and events from intercepted communications, reports, and news feeds [17]. Impact: Significantly speeds up intelligence processing, improves situational awareness (SA), enables proactive strategies rather than reactive ones, enhances resource allocation, and encourages command decisions based on more accurate information.

3.3. Network Safety and Security

AI-driven defense is required because of the speed and scale of the cyber domain. Anomaly Detection & Intrusion Prevention: ML algorithms continuously monitor network traffic, user behavior, and system logs to detect subtle deviations indicative of zero-day attacks, advanced persistent threats (APTs), or insider threats far faster than signature-based methods [18].

Automated Response and Threat Hunting: AI systems can automatically isolate compromised systems, block malicious traffic, and actively look for hidden threats within vast networks [19] (such as the "IKE" cyber reasoning system developed by the Department of Defense). Adaptive Defense: AI systems adapt defensive measures and enhance their detection capabilities over time, learning from previous attacks to build more resilient networks [20]. Vulnerability Assessment: AI can scan systems and code to find potential flaws before adversaries can take advantage of them. Impact: Provides the continuous, scalable monitoring that is necessary for modern networks; makes it possible to quickly detect and respond to sophisticated cyberattacks; improves the resilience of the network; and makes it easier for human cyber defenders to do their jobs.

3.4. Command and Control with AI Integration (C2)

C2 is transformed by AI into dynamic decision support instead of a hierarchical information relay. Real-Time Situational Awareness (SA): AI creates a unified, constantly updated Common Operating Picture (COP) for commanders by integrating feeds from sensors, intelligence reports, and unit positions across all domains [21]. Decision Support Systems (DSS): Based on mission objectives, rules of engagement (ROE), and resource constraints, AI algorithms evaluate the SA picture, evaluate options, predict outcomes, and recommend optimal courses of action (COAs) [22]. Commander's judgment is supported rather than replaced by this. Resource Optimization and Logistics Coordination: In complex, dynamic environments, AI optimizes the distribution of forces, weapons systems, and logistical support [23]. Streamlined Communication: AI can filter, prioritize, and route critical information to the right personnel at the right time, reducing cognitive load and communication friction.

Impact: Reduces commander cognitive burden, speeds up decision-making cycles, improves the quality and speed of decisions made under pressure, improves coordination among dispersed forces and domains, and optimizes resource utilization.

3.5. Assistance with Combat Operations

AI directly enhances the effectiveness and survivability of warfighters in kinetic engagements.

- Target Identification and Acquisition: Computer vision algorithms rapidly analyze imagery/video from drones, satellites, ground sensors, and soldier-worn systems to detect, classify, and pinpoint potential targets or threats with high accuracy, reducing friendly fire and collateral damage risks [24]. (e.g., Integrated Visual Augmentation System - IVAS).
- Precision Guidance: AI enhances the accuracy and resilience of guidance systems for missiles and munitions, including countering jamming attempts.
- Semi-Autonomous Weapons Systems: While the debate on LAWS rages (Section 5), current focus is on "human-on-the-loop" or "human-in-the-loop" systems:
- Loitering Munitions: AI enables target acquisition and engagement after launch, but typically requires human confirmation.
- Active Protection Systems (APS): AI rapidly detects incoming threats (rockets, missiles) and automatically triggers countermeasures on armored vehicles [25].

- Counter-UAS Systems: AI detects, tracks, classifies, and enables rapid engagement of hostile drones.

AI aids in triage, diagnosis, and treatment recommendations in field hospitals or via remote medical support in battlefield medicine. Impact: Increases soldier lethality and survivability; improves precision and reduces collateral damage; provides critical real-time threat awareness; automates defensive reactions at machine speed.

4. AI as a Force Multiplier: Enhancing Capabilities

The role of AI as a powerful force multiplier is the common thread that runs through all of these application areas. It achieves this by:

- Enhancing Human Capability: Allowing employees to concentrate on higher-level cognition, judgment, creativity, and leadership by freeing them from tedious, risky, or data-intensive tasks [7].
- Increasing Operational Tempo: enabling faster sensing, comprehension, decision-making, and action than adversaries that rely solely on human cognition and legacy systems. Autonomous systems operate in environments or for durations that are unsuitable for humans, such as the deep sea, radioactive zones, and 24 hours a day, 7 days a week. Improving targeting accuracy, minimizing collateral damage, and removing people from direct harm's way in high-threat scenarios (such as EOD, MCM, and reconnaissance under fire) are all ways to reduce risk and improve precision. Optimizing Resource Utilization: Making more efficient use of personnel, equipment, fuel, and munitions through predictive maintenance, logistics optimization, and mission planning.

Providing commanders with deeper insights, predictive foresight, and evaluated options based on comprehensive data analysis is one way to improve decision quality.

5. Important Issues, Dangers, and Ethical Considerations

The immense potential of military AI is counterbalanced by significant challenges and risks demanding urgent attention:

Lethal Autonomous Weapons Systems (LAWS) Ethics:

- The "Slope" Argument: There are concerns that giving targets more freedom to choose and engage targets reduces moral agency and accountability among humans, which could lead to machines making decisions about life and death without meaningful human control [26]. Defining "meaningful control" is contentious.
- Accountability Gap: Determining who is accountable for an autonomous system's actions (the system itself, the programmer, or the operator? is complicated morally and legally [27]. Compliance with International Humanitarian Law (IHL): In complex, chaotic battlefields, can LAWS reliably distinguish civilians from combatants, evaluate proportionality, and adhere to principles of distinction and proportionality? [28]
- lowering the threshold for conflict: policymakers may be more tempted to start a conflict if they see fewer casualties from their own forces [29]. Maintaining "appropriate levels of human judgment" (as stated in DoD Directive 3000.09) is technically and operationally difficult, particularly at high speeds or in contested communications environments [30]. Ensuring Human Oversight and Control The balance between necessary speed and sufficient human control is delicate.
- Adversarial Exploitation and AI Vulnerabilities: Adversarial Attacks: The malicious manipulation of input data (such as images and sensor data) to cause AI misclassification or malfunction [31]. For instance, a targeting system might mistake a school bus for a tank. Data Poisoning: Corrupting training data to embed biases or vulnerabilities into the AI model itself [32].

Methods for extracting or reverse-engineering proprietary AI models are known as model theft or inversion. Cyber Vulnerability: AI systems themselves become high-value cyber targets.

- Algorithmic Bias and Discrimination: Artificial intelligence (AI) models based on biased historical data have the potential to amplify or perpetuate discriminatory outcomes, resulting in unfair targeting or resource allocation with severe ethical and operational repercussions [33]. Diverse datasets and rigorous testing are essential but challenging. Robustness, explainability, and dependability: "Black Box" Problem: Complex AI models (especially deep learning) can be opaque, making it difficult to understand why they reached a particular decision, hindering trust, debugging, and accountability [34].

- Unpredictability & Edge Cases: AI may behave unexpectedly in novel situations not encountered during training, potentially leading to catastrophic failures in high-stakes military contexts.
- Testing & Validation: Developing rigorous methodologies to test and certify the safety, reliability, and robustness of AI systems for combat use is an ongoing challenge [35].

5.1. The AI Arms Race and Strategic Instability:

- Risks of Escalation: Unintentional escalation could result from misinterpreting AI-driven actions, such as rapid autonomous responses interpreted as aggressive [36]. Crisis Instability: First-strike postures may be motivated by the fear of an adversary launching a preemptive "decapitating" strike with AI-speed capabilities [37]. Proliferation Risks: Diffusion of dual-use AI technology increases the risk of advanced autonomous weapons falling into the hands of non-state actors or unstable regimes.
- Impact on Military Personnel and Doctrine: Integrating AI requires significant changes in training, recruitment (emphasizing STEM and AI literacy), organizational structures, and traditional military doctrines. Obstacles include resistance to change and cultural adaptation.

6. Governance and Strategies for Mitigation

A multifaceted strategy is required to address these obstacles: Ethical Principles and Policies: Establishing and strictly enforcing ethical guidelines for the creation and application of military AI. Key frameworks include:

DoD AI Ethical Principles: Responsible, Equitable, Traceable, Reliable, Governable [38].

Lawfulness, Responsibility and Accountability, Explainability and Traceability, Reliability, Governability, and Bias Mitigation are the NATO Principles of Responsible Use [39]. International Discussions: The UN Convention on Certain Conventional Weapons (CCW) Group of Governmental Experts (GGE) on LAWS continues multilateral dialogue with the goal of developing normative frameworks or potentially binding instruments [40]. Solid Technical Protections: Adversarial Robustness: The study and application of methods for making AI models immune to data poisoning and adversarial attacks. Making AI decision-making processes more transparent and comprehensible, particularly for critical applications, is the goal of Explainable AI (XAI) [34]. Comprehensive T&E frameworks designed specifically for military AI are implemented, including stress testing and realistic operational scenarios. Rigorous testing and evaluation Cybersecurity hardening: Protecting AI systems and their data pipelines with cutting-edge cybersecurity measures. Focus on Human-Machine Teaming (HMT): Making systems that use the strengths of both humans and AI to work together better. Clear doctrine defining roles, responsibilities, and procedures for HMT is essential [41].

International Norms and Arms Control: Encouraging international dialogue and cooperation to establish standards of responsible behavior, improve transparency whenever possible, and possibly create arms control agreements that limit the most dangerous uses of autonomous weapons. Measures that boost confidence are crucial. Investment in Safety and Security Research: Putting AI safety, security, reliability, and verification/validation methods ahead of AI capabilities when funding research and development.

7. The Path of the Future

The evolution of military AI is accelerating:

- Increased Autonomy: Systems will handle more complex tasks and operate with higher levels of independence, though human oversight will likely remain paramount for lethal decisions.
- AI that is everywhere: AI will become deeply ingrained in almost all military systems, from intelligence analysis platforms to equipment for individual soldiers. Cognitive Warfare: Artificial intelligence (AI) will play a crucial role in information operations, influence campaigns, and influencing adversary decision-making [42]. AI vs. AI Warfare: Throughout all domains, conflicts will increasingly involve AI systems directly countering, attempting to deceive, or degrading rival AI systems. Convergence with Other Technologies: New capabilities and complexities will emerge from synergies with advanced materials, biotechnology (enhanced soldiers), quantum computing (for faster AI training and breaking encryption), hypersonic, and other technologies. Emphasis on Resilience: Designing AI systems and networks that can operate effectively in degraded or contested environments (jamming, cyber-attacks) will be critical.

8. Conclusion

The military and national defense are unquestionably being transformed by artificial intelligence. Unprecedented capabilities as a force multiplier are provided by its integration across domains, including autonomous systems, data analysis, cybersecurity, command and control, and combat support. Lethality, efficiency, speed, force protection, and decision-making are all improved by AI, offering early adopters potentially significant advantages.

However, there are significant obstacles to this revolution. Ethical boundaries and urgent international attention are required to resolve the LAWS ethical quagmire. Critical technical and operational obstacles include ensuring meaningful human control, mitigating algorithmic bias, protecting AI systems from sophisticated adversarial attacks, and guaranteeing reliability in high-stakes situations. Global security is in serious jeopardy due to the possibility of an unchecked AI arms race and the strategic instability that this could bring. Responsible integration is paramount.

This calls for: Integrating frameworks like the DoD AI Ethical Principles and NATO guidelines into every stage of development and deployment. Robust Governance and Oversight: Clear accountability chains and rigorous testing, validation, and certification procedures. Safety and security are top priorities. A lot of money is being spent on research to make AI systems strong, easy to understand, and resistant to failure and exploitation. Advancing Human-Machine Teaming: Designing systems that augment human judgment, not replace it, especially concerning the use of force.

Engaging in sustained multilateral efforts to establish norms, build confidence, and possibly develop arms control measures to mitigate the most dangerous risks is one way to foster international dialogue. The so-called "Next Revolution" is already in motion. The trajectory of AI in warfare will be shaped not only by technological breakthroughs but fundamentally by the choices made regarding its governance, ethics, and integration. Foresight, accountability, and an unwavering commitment to ensuring that the pursuit of security through AI does not inadvertently undermine the very values and stability it seeks to protect are necessary for navigating this complex landscape. The challenge is ensuring that AI-augmented warfare remains ethically grounded under human control.

Compliance with ethical standards

Acknowledgments

The author would like to express gratitude for the academic support provided by Belhaven University and the Department of Information Technology.

References

[1] S. J. Lukasik, "Why Bad Things Happen to Good Technology: The Case of Smart Weapons," IEEE Technology and Society Magazine, vol. 31, no. 1, pp. 16-21, Spring 2012.

[2] M. C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," Texas National Security Review, vol. 1, no. 3, pp. 36-57, May 2018.

[3] U.S. Department of Defense, "Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity," Feb. 2019.

[4] D. S. Alberts, "The Agility Advantage: A Survival Guide for Complex Enterprises and Endeavors," DoD Command and Control Research Program (CCRP), 2011.

[5] J. R. Boyd, "Destruction and Creation," 1976. [Online]. Available: https://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf

[6] E. B. Kania, "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power," Center for a New American Security (CNAS), Nov. 2017.

[7] R. O. Work and G. Grant, "Beating the Americans at Their Own Game: An Offset Strategy with Chinese Characteristics," Center for Strategic and Budgetary Assessments (CSBA), 2019.

[8] M. J. M. Houck et al., "Predictive Maintenance for Military Systems Using Machine Learning," Procedia Manufacturing, vol. 16, pp. 1093-1100, 2018.

[9] NATO StratCom COE, "Cognitive Warfare," Mar. 2021. [Online]. Available: https://www.stratcomcoe.org/cognitive-warfare

[10] B. M. Perera et al., "Deep Learning for UAV-Based Object Detection and Tracking: A Review," IEEE Geoscience and Remote Sensing Magazine, vol. 10, no. 1, pp. 91-124, Mar. 2022.

[11] N. Michael et al., "The GRASP Multiple Micro-UAV Testbed," IEEE Robotics & Automation Magazine, vol. 17, no. 3, pp. 56-65, Sept. 2010.

[12] M. J. Rutherford et al., "Loyal Wingman: Concepts for Manned-Unmanned Teaming," AIAA Scitech 2020 Forum, Jan. 2020.

[13] U.S. Army, "Robotic Combat Vehicle (RCV) Family of Systems," [Program Briefing], 2023.

[14] D. L. Hall and J. Llinas, "Handbook of Multisensor Data Fusion: Theory and Practice," 2nd ed., CRC Press, 2008.

[15] A. Kott et al., "AI and the Future of Cyber Competition and Conflict," Journal of Information Warfare, vol. 18, no. 4, pp. 1-9, 2019.

[16] J. Lee et al., "Intelligent Maintenance Systems and Predictive Manufacturing," Journal of Manufacturing Science and Engineering, vol. 128, no. 4, pp. 807-822, Nov. 2006.

[17] G. Petkus et al., "Natural Language Processing for Military Intelligence: A Systematic Review," IEEE Access, vol. 9, pp. 137127-137148, 2021.

[18] I. Ahmad et al., "Deep Learning for Network Intrusion Detection Systems: A Comprehensive Review," IEEE Access, vol. 9, pp. 101574-101598, 2021.

[19] DARPA, "Cyber Grand Challenge (CGC)," [Online]. Available: https://www.darpa.mil/program/cyber-grand-challenge

[20] Y. Mirsky et al., "The Security of Machine Learning Systems: A Survey," IEEE Security & Privacy, vol. 20, no. 2, pp. 47-57, Mar./Apr. 2022.

[21] A. Kott and P. G. Neumann, "A Comprehensive Approach to Cyber Resilience," IEEE Security & Privacy, vol. 16, no. 6, pp. 10-12, Nov./Dec. 2018.

[22] D. A. Fulghum, "AI Steps Up for Air Combat," Aviation Week & Space Technology, Nov. 2020.

[23] M. K. Lauren and R. T. Stephen, "Modelling and Wargaming the Integration of Autonomous Systems into Land Forces," Journal of Defense Modeling and Simulation, vol. 16, no. 4, pp. 389-406, Oct. 2019.

[24] R. J. Lin et al., "Deep Learning for Military Object Detection in Aerial Images: A Review," Remote Sensing, vol. 14, no. 19, 5010, Oct. 2022.

[25] M. J. Merkle et al., "Active Protection Systems: Technological Assessment," Institute for Defense Analyses (IDA), IDA Paper P-8615, Feb. 2017.

[26] P. Asaro, "On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making," International Review of the Red Cross, vol. 94, no. 886, pp. 687-709, Summer 2012.

[27] M. E. O'Connell, "Banning Autonomous Killing - The Legal and Ethical Requirement That Humans Make Near-Time Lethal Decisions," in The American Way of Bombing: Changing Ethical and Legal Norms, from Flying Fortresses to Drones, M. Evangelista and H. Shue (eds.), Cornell University Press, 2014, pp. 224-235.

[28] ICRC, "Autonomous weapon systems: Implications of increasing autonomy in the critical functions of weapons," Expert Meeting Report, Geneva, Mar. 2016.

[29] R. Sparrow, "Killer Robots," Journal of Applied Philosophy, vol. 24, no. 1, pp. 62-77, 2007.

[30] U.S. Department of Defense, "Directive 3000.09: Autonomy in Weapon Systems," Nov. 21, 2012 (Updated Jan. 25, 2017).

[31] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and Harnessing Adversarial Examples," arXiv:1412.6572 [stat.ML], Dec. 2014.