International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Integration of Artificial Intelligence into Military Operations: A Kill Chain Perspective

Ethan Alphonso[a]***, Dr. Abhijit Banubakode***[b]

[a]Department of Computer Science, MET Institute of Computer Science, Mumbai 400050, India
[b]Department of Computer Science, MET Institute of Computer Science, Mumbai 400050, India

ABSTRACT :

Integrating Artificial Intelligence into military operations represents a huge shift in how war is perceived. It has redefined how countries deal with threats. This paper demonstrates the transformative role AI plays by examining the “Kill Chain” - a structured framework encompassing processes from identification to post-strike evaluation. Advanced algorithms, machine learning, and real-time data processing are employed to make the perfect Kill Chain. Use of AI boosts military capabilities by enhancing speed, autonomy, and precision of attacks. It is not just a concept; it is actively being shaped into reality by various global powers such as the United States, China, and Russia. For instance, the US’s Project Maven demonstrates AI’s ability to sift through vast amounts of data with almost human-like precision.

With every technological advancement, there is always a dark side to it. It has also been used by regimes with controversial practices, such as Iran in the Middle East and Libya in its civil war. Vladimir Putin, too, famously declared that “The Nation which Leads in AI will Rule the World”. The Cybersecurity gaps also remain a major concern, as the interconnected systems become a prime target for adversaries. The over-reliance on AI could weaken the ability of humans during critical moments. Firm human oversight, ethical administration, and international cooperation are essential to reduce risks and ensure that AI serves as a means for security rather than chaos. As AI in the military proceeds to improve, International standards are to be set to balance technological innovation with accountability in this new chapter of warfare where machines increasingly shape the fate of nations.

Keywords: Artificial Intelligence, Military Operations, Kill Chain, F2T2EA, Autonomous Weapons, Machine Learning, Cybersecurity, Military Ethics

Introduction

Artificial Intelligence has evolved from its roots as a theoretical tool for computation to become a cornerstone of military operations, altering the very nature of warfare in the 21st Century. Once assigned to just theoretical warfare, it now empowers real-time military capabilities, powering everything from advanced surveillance networks to complex autonomous weapon platforms. This vast transition makes a dramatic shift in military strategy, where traditional tactics are gradually enhanced and sometimes partially enhanced by machine-driven precision and speed. There are serious implications of this transition as asserted by Russian President Vladimir Putin in 2017: “Artificial intelligence is the future, not only for Russia, but for all humankind… Whoever becomes the leader in this sphere will be the ruler of the world”. This statement expresses the global race to dominate in AI.

The importance of this race is noticeable across national strategies. China, for instance, has adopted the concept of “Intelligentization”, a term used to describe the fusion of AI with military systems. The U.S., too, is pushing to become an AI superpower. Russia, too, is heavily investing in this race, creating systems capable of countering adversaries with ruthless precision. All this signals a new era where military supremacy hinges not just on manpower or firepower, but on the ability to harness algorithms, data, and automation.

This paper aims to explore the role of AI in military operations within the Find, Fix, Track, Target, Engage, Assess (F2T2EA) kill chain – a widely implemented system that structures the process of identifying, tracking, and neutralising threats. It was designed to streamline human decision-making in combat. We can observe how AI contributes to each phase with its complex algorithms and data-driven insights. This tremendous rise of AI in warfare brings critical issues to light – should machines be trusted with life and death situations? Should we rely on this to such an extent?

Methodology

This study is to investigate the integration of AI into military operations with more emphasis on the Kill Chain Framework.

Data Collection

To ensure data robustness and credibility, it creates a triangular set with primary and secondary sources for better analysis.

1. Military Reports and Official Documentation from leading global powers, such as the U.S. Department of Defence's AI Strategy and the DARPA program updates. We used concrete examples of the systems deployed, performance metrics, and strategic priorities.
2. Peer-reviewed academic literature.
3. Open-source intelligence, in the form of news reports and publicly available case studies.

Case Study Selection

To demonstrate AI's real-world impact, only cases relevant to the Kill Chain Framework were selected. Project Maven of the U.S. shows AI-powered threat detection and targeting, showcasing the innovations in computer vision and data processing. Similarly, China's Sky Net Program showcases surveillance and tracking capabilities. Uran-9, Russia's combat drone, has autonomous engagement capabilities requiring minimal human oversight. These cases were chosen for their technical significance and also as a representation of different nations' approaches to military AI.

3. AI in Military Operations: The Kill Chain Framework

The Find, Fix, Track, Target, Engage, Assess (F2T2EA) Kill Chain is a cornerstone of modern military, offering a sequential and optimal process for identifying, localizing, monitoring, prioritizing, striking, and evaluating threats. Artificial Intelligence (AI) has enhanced this framework by blending each phase with data-driven accuracy, automation, and adaptability. Harnessing advances in machine learning, sensor technology, and real-time analytics, AI accelerates the decision-making process and elevates operational outcomes. This section explores AI's contributions across the Kill Chain by referring to real-world applications from global powers like the U.S., China, and Russia. Each phase is studied for its benefits and challenges, unveiling both the radical potential as well as the risks of AI in Warfare.

3.1 Find: Threat Detection and Identification

The "Find" phase begins the Kill Chain by detecting and identifying potential threats from the tremendous datasets. Inputs from diverse sources– drones, satellites, ground sensors, and intelligence feeds are processed by AI with speed and accuracy not feasible by human analysts. Project Maven of the U.S. showcases this capability. By using Convolutional Neural Networks (CNNs), it evaluates images from Unidentified Aerial Vehicles (UAVs) to identify targets such as personnel or vehicles, achieving an accuracy of 90-98% compared to 70-80% manually. Israel, too, has a similar AI-driven facial recognition system in conflict zones like Gaza to sift through surveillance footage to pinpoint individuals in minutes rather than hours.

CNN extracts spatial features (edges, shapes) from pixel data by aggregating Convolutional layers for classification. This facilitates quick pattern recognition even on a noisy image feed, such as drone feeds with bad clarity.

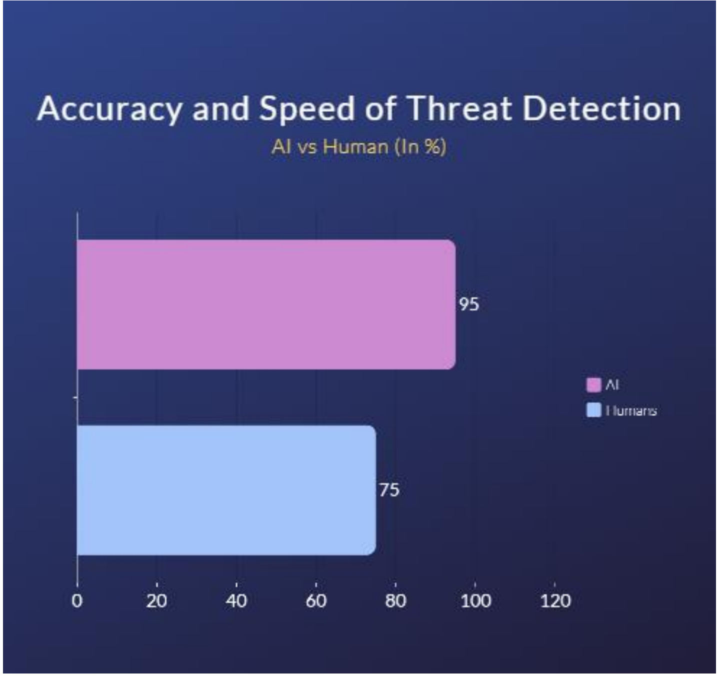

Fig 1

Benefits:

AI's speed and accuracy amplify the military commander's situational awareness by allowing them to detect threats earlier and optimally allocate resources. For instance, Project Maven, when used in Syria, reduced the image analysis time from days to hours.

Challenges:

Misclassifications pose a significant risk. In Afghanistan, during a drone strike, the U.S. system gave a faulty AI interpretation and misidentified civilians as terrorists, which resulted in unintended casualties. Such incidents show the dangers of over-reliance on AI without human verification.

3.2 Fix: Accurate Positioning

Once a threat is identified, the "Fix" phase pinpoints its location with precision sufficient for targeting. Through advanced algorithms, AI integrates multi-sensor data for the best results. For instance, by analyzing heat signatures, moment patterns, and electromagnetic patterns, the AI-integrated radar systems can distinguish military targets from decoys. The U.S. military uses AI in Aegis, a missile defence system that counters fast-moving targets and pinpoints coordinates with the help of machine learning.

Algorithms such as Kalman Filters are used in predicting and updating the target's position by fusing noisy sensor inputs. This approach ensures accuracy in dynamic conditions for targets manoeuvring at high speed.

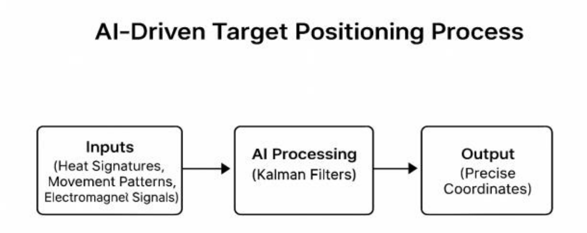
AI-Driven Target Positioning Process
Inputs (Heat Signatures, Movement Patterns, Electromagnet Signals)
AI Processing (Kalman Filters)
Output (Precise Coordinates)

Fig 2

Benefits:

Collateral damages are reduced by narrowing the strike zone. Compared to traditional methods it achieved a 50% reduction in errors.

Challenges:

This precision is threatened by cybersecurity vulnerabilities. In 2019, at the Black Sea, using falsified signals, the AI navigation was misled, directing the strikes off course.

3.3 Track: Continuous Monitoring

In this phase, constant surveillance of a moving target is kept, and AI handles this task with unrivalled consistency. The Sky Net system of China is a good example of this as it integrates AI with a vast network of satellites, drones, and CCTV cameras to monitor the enemy in real-time. Similarly, the (JADC2) Joint All Domain Command and Control of the U.S. fuses data from air, land, sea, and space sensors to provide a real-time operational picture, which helps track hypersonic targets that evade traditional radars.

Recurrent Neural Networks (RNNs) help predict target trajectories, learning from historical datasets. This helps to anticipate the movements of targets even in cluttered battle spaces.

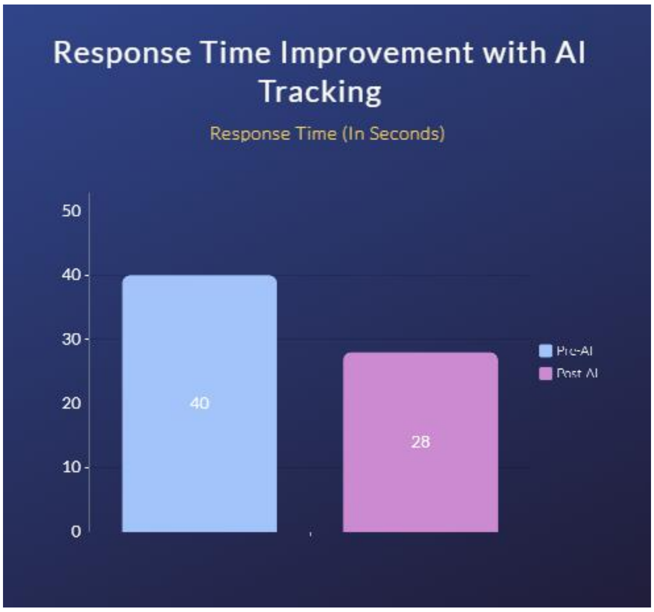

Fig 3

Benefits:

Persistent tracking of threats helps forces respond to them as required. There's an improvement in response times by 30% in exercises by using JADC2, as it possesses the ability to update target data every few seconds.

Challenges:

Data integrity is a key pillar for smooth functioning. In 2022, there was a JADC2 test failure, caused due to failed sensors, which led to misalignment of the forces. To avoid such catastrophes from repeating again, it is necessary to build more optimal and error-proof systems.

3.4 Target: Optimised Weapon Assignment

In this phase, AI to neutralize a target assigns an optimal weapon while keeping in mind factors such as range, payload, and defences. Using reinforcement learning, the U.S. 's (LRASM) Long Range Anti-Ship Missile evades countermeasures with a 95% success rate. Similarly, Russia's hypersonic Kinzhal missile uses AI to prioritize targets based on real-time battlefield data.

Multiple scenarios are evaluated using decision trees to maximize mission success and reduce risks. It is further refined by using reinforcement learning.

Benefits:

Precision and efficiency increased by using optimized targeting. LRASM can even autonomously switch to secondary targets if the primary targets are neutralized.

Challenges:

The United Nations and various NGOs are all against systems that ban systems that can independently select targets.

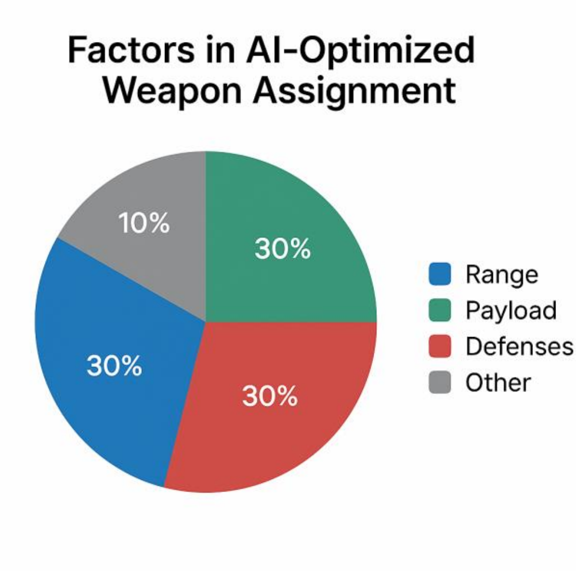

Fig 4

3.5 Engage: Autonomous Execution

In this stage, AI is used in executing strikes with minimal human input. Deployed in Syria, Russia's Uran-9 combat drone autonomously uses onboard sensors and objectives, neutralizing targets. The U.S. Navy conducts anti-submarine patrols using the Sea Hunter, an unmanned surface vessel that can even engage threats when authorized. These examples exhibit AI-powered combat execution capabilities.

Behaviour-based AI, which reacts when a specific criterion is met. This makes them quick in responding.

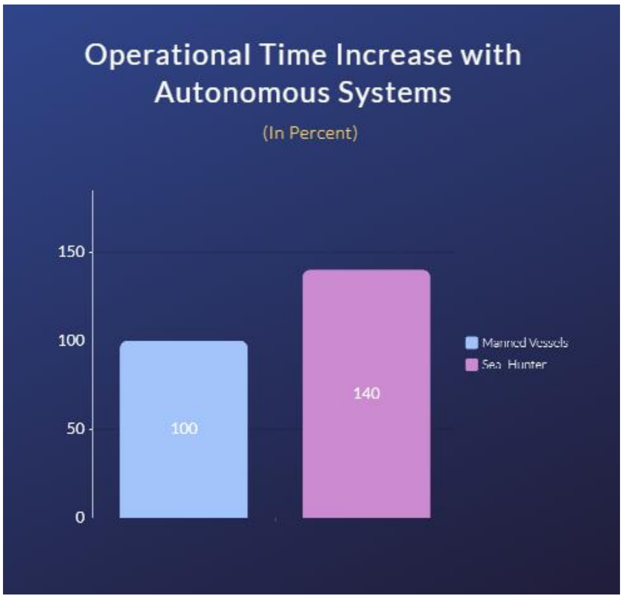

Fig 5

Benefits:

It accelerates response times and reduces the soldiers' engagement in real war situations. By being unmanned, the Sea Hunter can increase their operational times by 40% as compared to manned vessels.

Challenges:

A 2021 incident in Libya, where a Turkish-made Kargu-2 drone reportedly attacked without human orders. This fueled debates over the ethics of autonomous engagement.

3.6 Assess: Evaluation

This phase examines the strike outcomes, which help the AI models to learn and us to analyse the performance of the systems deployed. JADC2 in its post-mission evaluation, uses machine learning to assess damage, impact on civilians, and aim fulfillment. This analysis is observed in future missions. The MQ-9 Reaper drone compares pre- and post-strike imagery, analysing effectiveness in real time.

Bayesian analysis is done, enabling AI to refine the models. By following this iterative process, each mission turns into a learning opportunity.

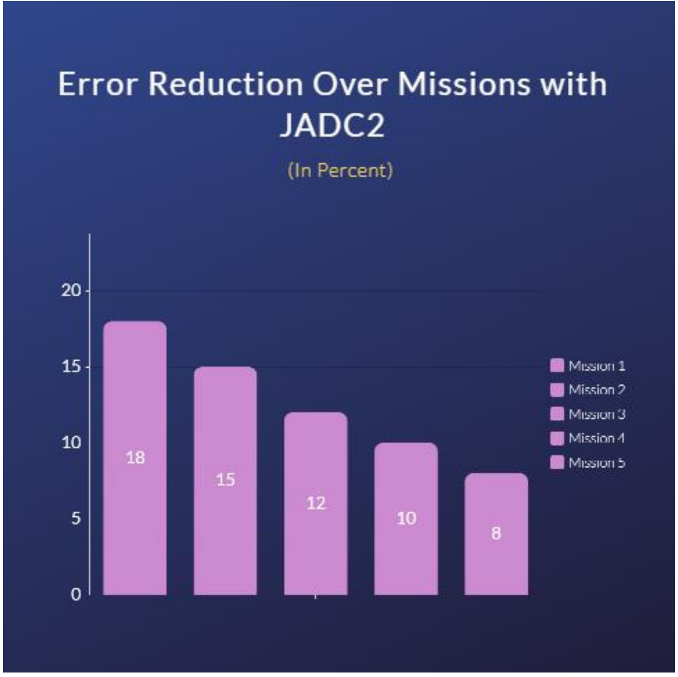

Fig 6

Benefits:

Continuously improving on every mission makes the performance much more desirable. JADC2's learning processes helped to reduce errors by 15%.

Challenges:

Accurate evaluation is dependent on good reconnaissance. If the data is incomplete or manipulated, then it can misrepresent the evaluation, resulting in flaws in future operations. It is important to have human oversight to validate these analyses.

Benefits of AI Integration

Integrating AI with military operations delivers significant advantages, amplifying its effectiveness across the F2T2EA Kill Chain. Employing capabilities such as machine learning and sensor fusion, AI-equipped militaries have far superior abilities in speed, precision, and scalability, when compared to traditional militaries. These advantages in real-world applications are also validated by performance metrics. It positions AI as a force multiplier, reshaping how wars are planned, fought, and won. Below are three key benefits: speed and efficiency, precision, and autonomy.

Speed and Efficiency

AI dramatically improves operation dynamics, reducing execution timelines from days or hours to mere seconds. 80% of the processing time is slashed in the Find phase by Project Maven's AI-driven analysis, enabling U.S. forces to identify threats in near real-time. Similarly, China's Sky Net processes millions of surveillance feeds simultaneously, faster and more efficiently than any human analysts ever could. This speed is also extended to logistics and planning. Supply chain is also optimized by AI algorithms, used by the U.S. Army to reduce equipment uptime by 25%.

Autonomy

AI-driven autonomy reduces human risk and increases operational capabilities in the form of unmanned systems. The U.S. Navy's Sea Hunter has such capabilities, autonomously patrolling vast oceans without requiring to pose any danger to the crew. Similarly, Russia's Uram-9 drone engages with ground targets independently while keeping the soldiers at a safe distance. Autonomy also scales operations, as a swarm of AI-controlled drones can stun defences with coordinated attacks, previously considered impossible.

By reducing human exposure to combat, autonomy preserves lives. It also makes hazardous operations possible without endangering any lives.

Precision

AI enhances precision across targeting and engagement, minimizing errors and collateral damage. LRASM (Long Range Anti-Ship Missile) of the U.S. is guided by reinforcement learning, achieving an accuracy of 95% in simulations, and is even able to evade defenses with surgical precision. Israel's Iron Dome is also AI-equipped, refining target coordinates to meters, intercepting 90% of incoming rockets. This precision is also carried over to Israel's AI-driven facial recognition, which enables it to isolate combatants from civilians with low misidentification rates.

Higher precision is not only important from the mission point of view, but it is also necessary from an ethical perspective, by not harming civilians. In such non-traditional warfare, where the perception of the public matters, such precision can strengthen credibility and reduce public outcry.

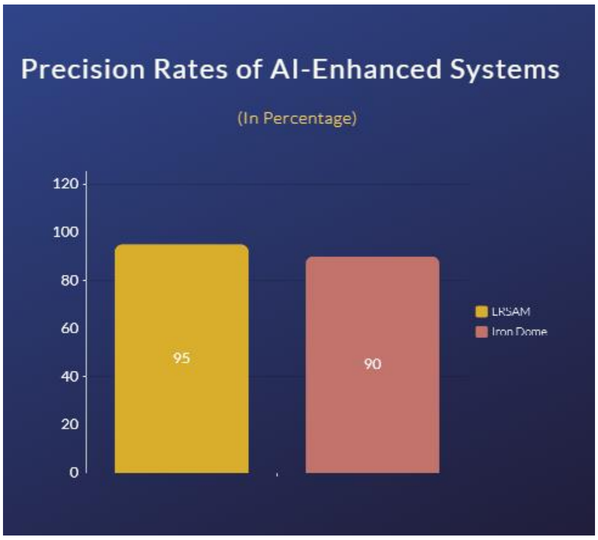

Fig 7

Challenges and Ethical Considerations

While integrating AI with military operations offers transformative benefits, it is also plagued by challenges that hinder future developments. Challenges include cybersecurity risks, ethical conflicts, and a lack of human oversight. Integrating AI in warfare introduces a lot of moral questions that require scrutiny. This section delves into the hurdles in this, showing its consequences in operational reliability, global security, and fatalities. Addressing these issues is essential to ensure AI acts as a tool toward military advancements rather than causing any harm.

5.1 Technical Limitations

Despite being a quite complex system, AI is not completely flawless. There can be inaccuracies due to biases in training data, algorithm misjudgment or unpredictability, which can eventually lead to catastrophic outputs. In a 2018 study by Buolamwini and Gebru, it was revealed that AI misclassified darker-skinned individuals 34% more than lighter-skinned individuals. These flaws were traced back to misleading datasets. From a military point of view, such biases may lead to misidentification of friends from foes. Such an incident occurred in 2020 where, due to an AI misinterpretation, a U.S. drone strike was conducted on civilians, eliminating them. Environmental factors are also a challenge, as observed in 2022, the JADC2 systems couldn’t track due to fog blocking the sensors, delaying response time by 20 minutes.

Technical limitations erode trust in AI, especially in high-stakes scenarios where precision is mandatory. Robust testing, diverse datasets and secondary systems are critical to reduce risks.

5.2 Cybersecurity Risks

AI functions on network systems and vast datasets, making it a prime target for cyber threats. Adversaries exploit vulnerabilities through hacking, spoofing or data poisoning, lessening AI’s effectiveness. In 2017, a Russian cyberattack was carried out crippling global infrastructure, demonstrating how malware could cause chaos in global economies. GPS spoofing caused the U.S.’s navigational AI in the Black Sea to perceive the ship's location miles away from the actual location.

Cybersecurity breaches can turn AI from being an asset to a liability, misdirecting strikes or even exploring strategies. Toughening the systems with encryption, redundancy and real-time anomaly detection is vital in this day and age.

5.3 Ethical Challenges

Using AI in military operations raises strong ethical questions around principles like distinction (separating combatants from civilians) and proportionality (balancing military gain and harm). Russia’s Uran-9 and Turkey's Kargu-2 autonomous drones lack much accountability, as seen in Libya, where the AI drone reportedly killed without human authorization. Critics argue that machines lack the moral judgment to weigh life and death situations. Supporters of AI like Arkin challenged this by showing that autonomous systems outperformed fatigued soldiers in target discrimination. Yet in the 2020 Afghanistan strike, we see that including AI can amplify mistakes rather than eliminating them, where 10 civilians were killed due to AI misrepresenting them as terrorists.

Ethical dilemmas call for regulations. Without clear norms, AI risks eroding the moral framework of warfare.

5.4 Human Oversight

Keeping AI in human control is both practically and legally important. It remains uncontrollable as autonomy grows. If any missteps are taken, who will remain responsible? The programmer, operator or the commander? International laws remain behind in this, offering no clear laws. The Geneva Conventions, 1949, predate AI so there is nothing to keep everyone in check. In the 2021 U.S. Navy exercise, the operators were left puzzled looking at the Sea Hunter’s autonomous maneuvers, raising doubts about any actual meaningful control.

Weak human oversight risks unaccountable actions. Collaborative Human-AI models should be created, where humans set the parameters and AI executes them. All this requires training, transparency and time to refine. Till no proper resolutions are found, the tensions between autonomy and accountability will continue to exist.

Conclusion

Integrating AI into military operations marks a pivotal evolution in warfare, reshaping the F2T2EA Kill Chain with unmatched speed, precision and autonomy. AI has proven to be a force multiplier, from the threat detection systems of Project Maven to Russia’s Uran-9 autonomous drones, and the surveillance network of China’s Sky Net. These technological breakthroughs help nations to respond to threats with agility and accuracy, optimising the allocation of resources throughout.

As AI is redefining the art of war, it demands a balanced perspective. The benefits should be harnessed by keeping in check the adverse effects such as over-reliance, ethical ambiguity and potential misuse. Establishing international laws ensuring firm human oversight are important to avoid any dangers and maintain peace and stability. The future of AI hinges not only on technological prowess but also on the wisdom to wield it responsibly.

REFERENCES

[1] U.S. Department of Defense, "Artificial Intelligence Strategy," Dept. Defense, Washington, DC, USA, 2023. [Online]. Available: https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/

[2] Defense Advanced Research Projects Agency, "DARPA Annual Report 2023," DARPA, Arlington, VA, USA, 2023. [Online]. Available: https://www.darpa.mil/about-us/publications/annual-reports

[3] United Nations, "Final report of the Panel of Experts on Libya established pursuant to resolution 1973 (2011)," United Nations Security Council, New York, NY, USA, Rep. S/2021/229, Mar. 8, 2021. [Online]. Available: https://undocs.org/S/2021/229

[4] P. Scharre, *Army of None: Autonomous Weapons and the Future of War*, W.W. Norton & Company, New York, NY, USA, 2018.

[5] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, Cambridge, MA, USA, 2016.

[6] A. Zhang, Z. C. Lipton, M. Li, and A. J. Smola, *Dive into Deep Learning*, Cambridge Univ. Press, Cambridge, UK, 2023. [Online]. Available: https://d2l.ai/

[7] W. Wallach and C. Allen, "Artificial intelligence and armed conflicts," in *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, R. Almeida, M. Whittaker, and S. Woolley, Eds., Cambridge Univ. Press, Cambridge, UK, 2025, ch. 20, pp. 391-408. [Online]. Available: https://www.cambridge.org/core/books/cambridge-handbook-of-the-law-ethics-and-policy-of-artificial-intelligence/artificial-intelligence-and-armed-conflicts/46B20A780349FA8939E8B886E77C4B93

[8] J. B. Tucker, "Ukraine's future vision and current capabilities for waging AI-enabled autonomous warfare," Center for Strategic and International Studies (CSIS), Washington, DC, USA, Feb. 2025. [Online]. Available: https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare

[9] World Intellectual Property Organization, "WIPO Technology Trends 2023: Artificial Intelligence," WIPO, Geneva, Switzerland, 2023. [Online]. Available: https://www.wipo.int/publications/en/details.jsp?id=4650

[10] K. Takagi, "China's military AI: The push for intelligentization," *The Diplomat*, [exact date unavailable], 2023. [Online]. Available: https://thediplomat.com/tag/china-military-ai/