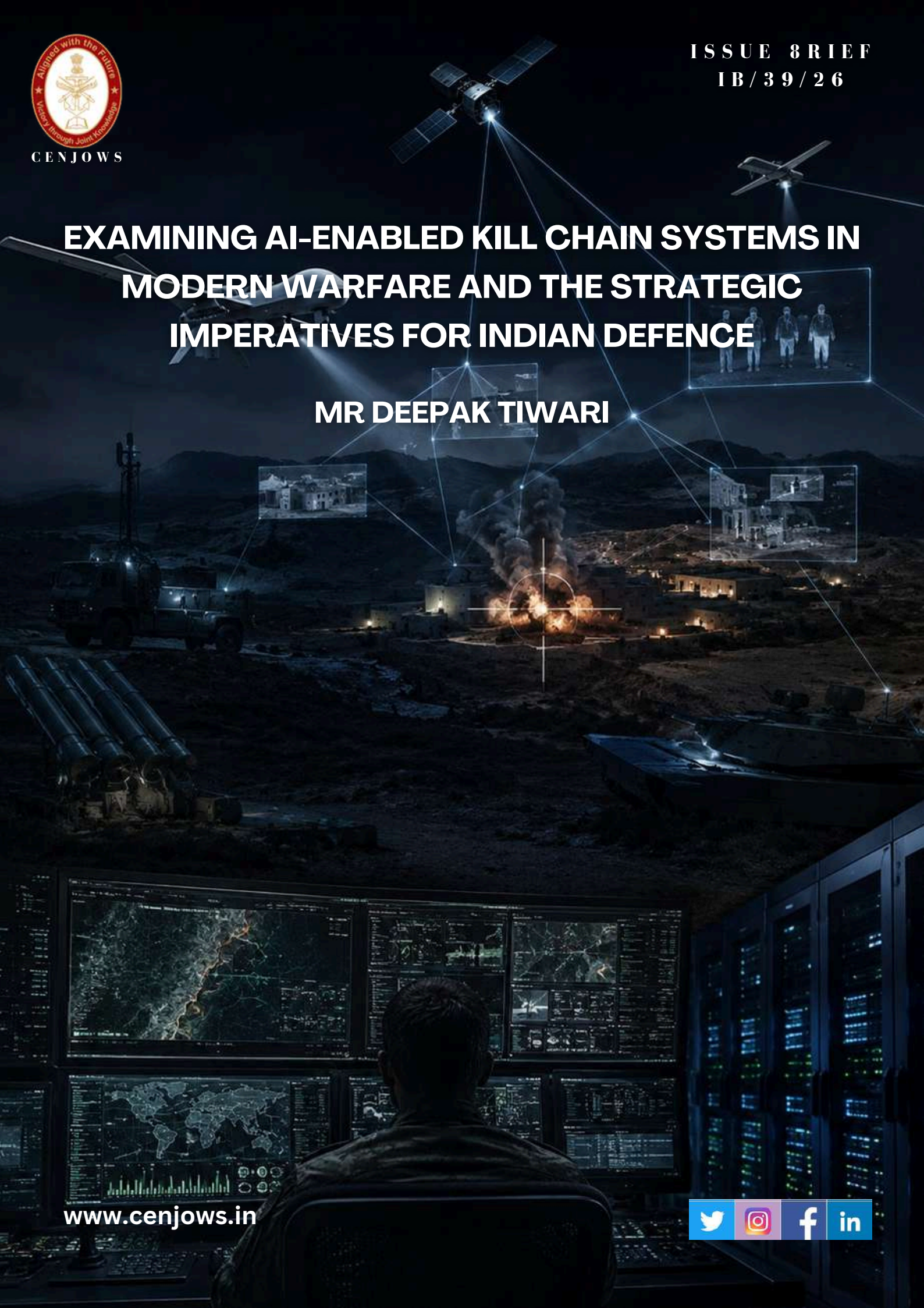
CENJOWS

ISSUE 8RIEF
IB/39/26

EXAMINING AI-ENABLED KILL CHAIN SYSTEMS IN MODERN WARFARE AND THE STRATEGIC IMPERATIVES FOR INDIAN DEFENCE

MR DEEPAK TIWARI



www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Examining AI-Enabled Kill Chain Systems in Modern Warfare and the Strategic Imperatives for Indian Defence

Mr Deepak Tiwari is a technical research assistant at CENJOWS

Abstract

Artificial intelligence has initiated a paradigm shift in the Kuhnian sense. Similar to how Thomas Kuhn describes the evolution of science through revolutionary leaps leading to a paradigm shift, the adoption of AI in battlefield tactics has shifted normal strategic calibrations to a new dimension. The employment of AI on a battlefield and the diverging discourse on its adverse impact and effectiveness are now prevailing narratives. In this context, Israel's use of an AI-enabled kill chain system consisting of three infamous AI tools, namely Lavender, the Gospel, and Where's Daddy, has opened a new dimension of sub-conventional warfare against non-state actors. Predicting the future course of strategic planning in the age of emerging disruptive technologies is a highly daunting task due to the rapid and uncharted evolution of these technologies. However, Israel's confident approach to weaponising AI before it becomes a threat to its own force has shocked the world, frightened its enemies and facilitated capable nations with a new perspective on the use of AI against a brutal enemy. India stands at a position similar to

Israel, plagued by the increasingly hybrid threats from different state and non-state actors. An AI-enabled kill chain system, as shown by the Israel Defence Forces (IDF) in its war against the Hamas terrorist group in Gaza, despite its humanitarian concerns, presents an opportunity for India to have its own AI deterrence against similar threats. To that end, this paper examines the architecture of an AI-enabled kill chain system with a special emphasis on Israel's deployment of such a system. The paper traces the development of a kill chain, its core constituent elements, and how it can be created in India, tailored to the Indian security environment. This paper thus identifies key gaps and challenges in India's evolving defence AI architecture within the parameters of an AI-enabled kill chain, and proposes a 'two-armed structure' to develop India's indigenous foundational AI capabilities.

Introduction

The conflicts of the post covid age have become the accelerating laboratories for the AI-enabled transformations of warfare, which are qualitatively different from prior such transformations. The innate practices of decision-making during a conflict, which were the exclusive domain of human judgment, are now being infiltrated by specialised AI tools. Today, AI-enabled kill chain systems introduced to battlefield intelligence are compressing the decision cycle from days to minutes. These are the systems where a few steps of a traditional kill chain have been either heavily assisted or completely automated using specialised AI tools. The major escalations of post-COVID years, most notably the Russia-Ukraine war, present a striking study of wartime innovation and adaptation. This war, beginning with the relentless and diversifying use of unmanned systems of all kinds, has now evolved to integrate AI through Small Language Models (SLMs) for target identification and engagements. A similar but more intense example of such application of AI tools has recently come into the limelight, where the Israel Defence Forces (IDF) has operationalised an AI-based kill chain system against the Hamas terrorists in Gaza post the October 7 attack.[1] The AI tools, specifically designed and trained for embedding with the various steps of the kill chain from spotting a threat to neutralising it, have seen, according to unverified reports, a full-scale deployment in this

conflict. Although it has raised serious concerns over accountability and high collateral damage, it has also presented a capability demonstration of such AI tools in the field. The three names of AI tools that have made insistent claims to be used during the Israel-Gaza conflict are ‘Lavender’, ‘Habsora’ (‘the gospel’ in Hebrew) and ‘Where’s Daddy’. The IDF, through its official press release, has denied the claims of the use of such AI tools, stating that they do not “employ AI to autonomously select targets for attack” but for mere intelligence analysis.[2] Since these systems signify a fundamental shift by replacing humans in a kill chain, they are altering the debate from questioning their use to the scale of consequences (humanitarian) acceptable to the actors using them.

Considering India’s geopolitical environment, internal security scenario and global turmoil amid raging conflicts in West Asia, these developments in the domain of AI appear vital to India’s strategic interests. The volatile security environment around India, while sub-conventional to hybridised internal and external threat actors remain persistent, a sophisticated AI-enabled ISR platform and kill chain systems may drastically boost its counter posture. The algorithmic warfare capabilities are structuring a new arms race among emerging powers, and India, being a pivotal player in the region, cannot afford to be left out. Within the context, defence establishments and key stakeholders face a consequential set of questions: How is the character of modern conflicts being reshaped by AI kill chain systems? What military advantages do they confer against hybrid threat actors? And critically, where does India stand in its own readiness to develop, deploy, or defend against such systems?

This research article has explored this development and analysed the conditions where AI-enabled kill chain systems have been claimed to be used and have proven effective against a clustered enemy. It offers a detailed technical and operational analysis of AI-enabled kill chain systems, the tools used by Israel, and their claimed effectiveness. The article has examined these AI tools by tracing how each system functions within the F2T2EA framework (Find, Fix, Track, Target, Engage, Assess). This article pitches into the ongoing debate, interrogating whether these emerging disruptive technologies are finally going to put state actors a step ahead against the non-state actors proficient in non-conventional/hybrid means of warfare. Finally, but most centrally, the paper

addresses India, assessing the current state of AI integration, deployment, policy, and challenges. Through this assessment, this article has identified critical gaps in India's AI integration readiness against similar threats. Based on the systematic evaluation of AI kill chain architecture in use, this study proposes a framework of strategic imperatives to guide Indian defence modernisation in this domain.

Understanding the AI-Enabled Kill Chain: Concepts and Architecture

A military kill chain refers to a structured sequence of tactical manoeuvres designed to achieve a strategic objective, which typically involves identifying, tracking, targeting, and eliminating an enemy threat. It was conceptualised during World War II as a systematic framework for decision-making. The initial form of a kill chain, often referred to as the 'traditional kill chain', involved four F's: find, fix, fight, and finish. It provides a foundational structure for a kill chain, whose evolution then becomes a function of technologies of the era and the evolving nature of threats.[3] To that end, by the late 1990s, the US military doctrine evolved this basic chain into steps that conformed to the advances in precision-guided munitions and air power of that time, such as Find, Fix, Track, Target (FFTT). This approach was matured in the 1991 Gulf War within the doctrine of "shock and awe", adding a dimension of psychological impact on the enemy's will to fight.[4] Post 9/11 engagements of the US in Afghanistan, the new sub-conventional threat paradigm led to its further evolution into "find, fix, track, target, engage, assess" (F2T2EA). This framework, codified by the US Air Force, remains doctrinally and technologically central, absorbing the contemporary advancements in joint targeting.

The architecture of the WW-II kill chain was rooted in industrial warfare, where aerial reconnaissance, strategic bombing, and the introduction of radars were its key enablers. It was completely human-centric, linear, and slow in execution, taking sometimes months to engage the enemy. The Cold War era takes a conceptual leap in cross-domain generalisation of the concept with the introduction of the OODA Loop (Observe--Orient--Decide--Act) developed by John Boyd.[5] The deployment of AWACS/airborne radars, ISR satellites, and digital command and control (C2) evolved the targeting from a linear to a cyclic process. The F2T2EA, the current version of the kill chain, was formalised by John

P. Jumper to meet the rapid technological advancements at the beginning of the digital age.[6]

The extensive use of UAVs and satellite-based ISR by the US in the Middle Eastern conflicts conforms to this argument. This phase of the kill chain, based on the F2T2EA architecture, evolved between 2001 and 2015, converging to networked and drone-centric strikes deep inside the enemy territory. This approach has remained effective in eroding the sense of safety manifested by complex terrain among enemy forces. A morphed variant of this kill chain can be observed in counterterrorism campaigns of the US in Afghanistan, Iraq, and Yemen. In this phase of kill chain evolution, real-time ISR and strike integration have proven decisive in running a near-cyclic (continuous) kill chain; however, humans remain integral at all steps.

The AI integration in this aspect comes with the notion that in high-risk zones of foreign territory infested with seasoned guerrillas, the first three steps of the F2T2EA kill chain must be time-sensitive and risk-free. The current phase of kill chain evolution (2015-present) characterises a non-linear, distributed and machine-assisted system with varied levels of autonomy at each step. The key technologies enable such architecture involve AI/ machine learning, sensor fusion (multi-domain ISR), cloud-based command and control (C2) assistance, autonomous systems (UAVs, UUVs, UGVs) and internet of military things (IoMT). These technologies are embedded at each step of the kill chain, transforming it into an AI-enabled kill chain. In that, the first three steps, as shown in the figure below, are usually completely automated using dedicated AI tools. The figure below mentions the example of such tools used by Israel against Hamas terrorist post October 7 attack. Step one, “Find”, involves sensor-based technologies fused with an LLM trained to analyse the data collected from those sensors. Facial recognition, voice and gestures recognition, electromagnetic signature detection (quantum magnetometry-based heartbeat locator called “Ghost Murmur”, used by CIA in Iran airman rescue), etc., are a few such active examples.[7] A set of personal data trails left on open-sourced platforms such as social media posts, GPS movement data, phone records, known associations, etc., can also be used to filter out and perform identity confirmation using AI tools. The

second step uses a similar AI tool with its LLM trained to pinpoint the location by identifying buildings, industrial structures, wild terrain, etc. The Gospel system used in Gaza is designed to do exactly that, to mark buildings with exact coordinates, which is a source location of a target identified in step 1. Step 3 involves monitoring the movement of the target in and out of its designated location. Here, another example of an AI tool called Where's Daddy comes in play, which has reportedly been used in Gaza to track Hamas terrorists to their homes. The next two steps involve limited AI intervention as they leave the choice to carry out the strike in human hands, since, for now, only humans are allowed to take the life of another human.

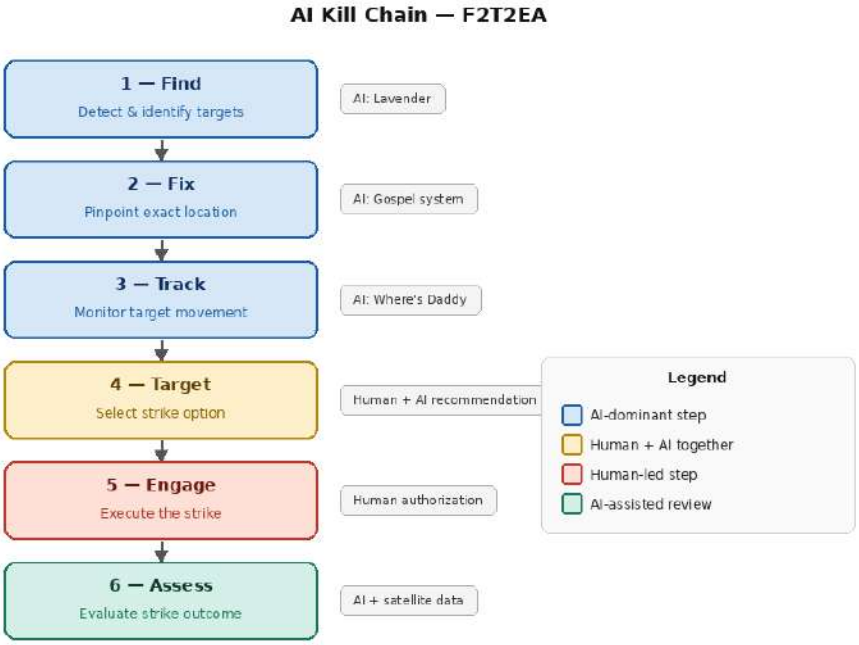


Figure 1: F2T2EA Architecture of AI-enabled kill chain with AI tools used by Israel against Hamas. **Source:** Designed by the author using the Claude AI tool.

The last step of this F2T2EA architecture-based kill chain conducts the post-strike assessments to measure the effectiveness of AI. This step also implies its cyclic nature by installing a feedback channel for the chain to learn and evolve for better accuracy.

The observed examples of such kill chain systems in place are Project Maven (launched in 2017 by the US DoD); TITAN (Tactical Intelligence Targeting Access Node); the

Advanced Battle Management System (ABMS). launched by the US Air Force;[8] AI-enabled decision dominance in Intelligentised warfare conceptualised by China; and integrated strike with AI-coordinated ISR used in the Russia-Ukraine war. Israel's deployment of a highly sophisticated AI-assisted targeting system in Gaza has been further discussed in detail in the following section.

Case Studies: AI Kill Chain Systems in Active Conflict

The all-encompassing impact of accelerating AI integration in the weapons of war has already begun to take shape. The countries like the US and Israel, which have consistently depended on cutting-edge technologies to maintain their military supremacy, have taken this obsession to a new level. The deployment of an AI-enabled kill chain using AI tools, namely Lavendar, the Gospel, and Where's Daddy, by the Israel Defence Forces in Gaza has emanated two shockwaves moving in opposite directions. The most spoken and visible shockwave is of humanitarian concerns over massive unaccounted-for deaths of Palestinians under the guise of collateral damage.[9] The other wave is rather silent but has penetrated deep inside the strategic dome of global militaries. This wave has made the strategic planners and military generals apprehensive of the uncharted territory that AI has dragged the warfare into. Although the introduction of Israel's AI kill chain came after the October 7 terrorist attack by Hamas, an analysis of events and initiatives taken before this suggests long-term planning and a strategic foresight that goes far beyond any new threats the world has seen yet. Thus far, the official IDF sources emphasise that their AI kill chain is essentially a "human-controlled process"; they do not clarify whether there were humans in control during their operations in Gaza and, if so, how such high unaccounted fatalities occurred.[10]

To trace back the evolution of this AI kill chain, one must look at the foundation needed for each subsystem and how that foundation was acquired. The three AI tools reportedly used have been developed with the help of an American software company called Palantir Technologies (PLTR).[11] For these AI tools to work with a certain level of accuracy, there is a need for a Large Language Model (LLM) trained on billions of parameters to analyse a specific data type. In Israel, such LLMs were developed in-house under the supervision

of Unit 8200 (an Intelligence Corps unit of IDF), which called on the army reservists with professional working experience in companies like Google, Microsoft and Meta.[12] Now, these LLMs need a colossal amount of data to train their algorithms, and in the case of Israel, companies like Fifth Dimension (an AI-based track and surveillance technology provider since 2017, founded in 2014 by a Mossad member)[13] and AnyVision (an advanced AI-based facial recognition and identification), have been collecting and feeding data to machine learning since 2017-18.[14] The Israeli government has installed thousands of such 'AI cameras' within an integrated surveillance architecture where data inputs from all sources are collected and analysed to cross-check/verify specific intelligence outputs. This large quantity of data needs to be stored and remain accessible through cloud servers, which, in Israel's case, have been provided by Google, Meta and Microsoft under Project Nimbus and Azure.[15] This whole architecture has been consistently calibrated and supervised by the Unit 8200 of IDF, suggesting a unified approach with a long-term strategic vision in action.

Lavender

In contrast, Lavender uses its cross-referencing intelligence database to generate a "suspicion score" from multiple data sources such as phone calls, social media activities, and images captured through surveillance cameras and drones.[16] It works as a fully automated kill list generator, also termed as the "Target Factory" of the IDF by a few sources. It maintains a smart, correlational database, a digital file of each suspected individual with hundreds of attributes. Lavender itself does not declare someone a target, but it provides an analysis of a suspect, which is then run through 'identification criteria' (specialised criteria created to identify a Hamas member) to confirm whether the suspect is a member or not.

The Gospel

The Gospel, also known as 'Habsora', identifies and makes a list of buildings where frequent terrorist sightings have been recorded, using data collected from satellites, drones, cameras, cyber intelligence, phone intercepts, body cams, human intelligence,

and other aerial and ground ISR conducted in the region. This tool is limited to providing information on ‘objects’ and not humans; thus, it generates a list of sites, which is then matched with the list of people identified through the Lavender. Gospel has been trained on data gathered from IDF’s long-run ‘predictive policing’ campaigns, technologically enabled by an Israeli company called “Fifth Dimension” and Palantir of the US. The AI tool assigns priority scores to assessed sites based on various data criteria such as the proximity of the site to known command centres, frequency of terrorist activities, and buildings/hideouts used for rocket launches or storage.[17]

Where’s Daddy

The third tool, called “Where’s Daddy”, tracks the cell phone signals of the target and traces them back to their home, thus confirming their identity and clearing the way for a lethal strike.[18] It tells the current location of an individual and updates it in real time to enable time-sensitive decisions to be made. The technology triangulates the location of an individual through mobile-phone metadata (IMSI-catcher-style data, cell-tower triangulation, etc.), vehicle movements, checkpoints, drone and CCTV-based surveillance data, etc., and after coordination with other tools, it gives a geospatial estimation of the location as an output.[19]

These three tools alone have reportedly identified homes, tunnels, and movements of over 40,000 members of Hamas in weeks. In the first month of its operations, the IDF has struck more than 15000 locations. A sequence of processes that used to take a year to identify 50 targets at most has now contracted to 100 in a day, says the head of the IDF, Aviv Kochavi.[20] This technological feat, even though criticized for its accuracy and humanitarian concerns, remains unprecedented and radical in the domain of ISR processing and kill chain automation.

All three tools have been designed to track and identify members of Hamas and Palestinian Islamic Jihad (PIJ). Another tool developed by the same Unit 8200, called “Depth of Wisdom”, is also a similar endeavour of the IDF specifically designed to map Gaza’s tunnel network. This whole system indicates a level of penetration that AI has

achieved against a non-conventional yet persistent threat, similar to what India deals with at its northwestern and northeastern borders. Palantir's Gotham is another such AI model used by the US Department of Defence, the UK government, and intelligence communities of many of their allies. Gotham connects and synthesises a huge variety of data sources to generate real-time situational awareness and course of action.[21]

India's Defence AI Landscape: Ambitions and Realities

AI, now recognised as an Emerging Disruptive Technology (EDT) in defence by the US, EU, and NATO through their official documents, has a bright green signal to penetrate deep inside military domains all around the world.[22] India, considering AI as a transformative force, took its first dedicated initiative in 2018 with a task force established under the Department of Defence Production (DDP) called "Strategic Implementation of AI for National Security and Defence". Based on the recommendation of this task force, in 2019, the foundation of the Defence AI Council (DAIC) and a Defence AI Project Agency (DAIPA) formalised India's AI journey in the defence sector. Since then, different departments under the MoD have launched numerous initiatives, roadmaps, campaigns, and symposiums, awaiting the AI-led transformations, similar to those seen in the US, China, and Israel. In the last five years (2020-25), India's defence innovation ecosystem has come up with many promising AI-based solutions, supported by initiatives such as iDEX and IndiaAI.[23]

India, through its coordinated initiatives between the DRDO, government, and private industrial entities, has been able to procure certain credible defensive systems such as Akashteer (AI-enabled air defence system), Sudarshan Chakra (AI-assisted defence architecture), etc. Moreover, a strong emphasis on building a consortium of startups in this segment through various support systems, most notably iDEX, has been a big success. At its core, India's policy and structural initiatives in the domain of Military AI (MAI) seek to integrate AI in its multi-domain operations with a compressed decision-action loop through indigenous capabilities.[24] However, in comparison to the AI architecture witnessed in action by the IDF, India remains a few steps behind in starting as a beginner-level player. Nonetheless, it is only fair to accept that current AI systems in

action, emerging through the large consortium of startups, do offer a glimpse of hope. The AI-based Intrusion Detection System (AI-IDS) deployed for smart border management, AI-enabled C2ISR systems helping in preventing cross-border infiltration and CT/CI operations, and the Maritime Information Management and Analysis Centre (IMAC), enhancing maritime domain awareness, deserve a mention in this regard.[25]
In a broader sense of comparison, China's military-civil fusion strategy enables a smooth transfer of AI innovations from commercial laboratories to operational military use. At the same time, the January 2026 directive issued by the United States Department of War, calling for AI systems without vendor-imposed ethical constraints, indicates a rapid move toward fewer limitations in capability development.[26] Taken together, these trends may encourage a global race where strategic competition outweighs safety and human oversight, placing middle powers in a difficult position as they try to advance technologically while maintaining responsible governance.[27]

Despite significant resource constraints, India retains a notable advantage. The 2024 Evaluating Trustworthy AI (ETAI) Framework, introduced by the DRDO, reflects a systematic effort to embed safety, reliability, and robustness at the core of military AI.[28] In doing so, it outlines a structured governance approach that is more formally articulated than comparable efforts in the United States or China. However, world leaders are now openly emphasising "rapid adoption of AI for military dominance", India's self-imposed compulsion to act as a role model in this evolving domain may keep it behind and comfortable.

India, at the beginning of its AI transformation, faces a persistent gap between data and doctrine. The lack of an integrated, tri-service data architecture constrains progress toward Joint All-Domain C2 capabilities. Moreover, AI adoption has largely remained limited to areas such as autonomous systems and logistics, with comparatively less emphasis on intelligence analysis, decision support, cyber operations, and information warfare.[29]

These gaps create big hurdles in erecting India's AI counter/defence against the evolving sub-conventional and hybrid threats in the contested border areas. In a broad sense, gaps in India's defence AI ambitions and realities are successively dependent, first, on a lack of funding and, then, as a result, the absence of data infrastructure and hardware manufacturing capabilities and thus no dedicated indigenous AI models that can be tuned to address evolving needs. Comparing AI budgets for defence-related developments with other countries like the US and China is meaningless for now, since India's seriousness towards this swiftly emerging domain is still too humble, and comparing AI spending only validates this further.

Strategic Imperatives for India

During a recent two-day Ran Samvad conference held on 9-10 April 2026, which was attended by CDS Gen Anil Chauhan along with many other senior military officers from all three services, the creation of an AI-enabled kill chain came up many times. The consensus was achieved that, while technology may automate the decision loop to some extent, the human element must remain in war decision-making.[30]

The AI-enabled kill chain or an AI-assisted system that can effectively shorten the decision loop in a high-stakes and rapidly evolving threat scenario is a necessity in India's diverse threat landscape. The threat of cross-border and hinterland terrorism growing and morphing as a function of radicalisation or Islamic fundamentalism has remained an enduring challenge. The protracted insurgencies destabilising strategically sensitive areas in the northeast and the external actors and factors nurturing it are now more than a mere internal security issue. There are lags in India's intelligence apparatus, structural or systematic; if it can't be overhauled soon, it must be provided with an extra arm. The AI-enabled technologies can be that arm and more. To that end, an AI framework needs to be installed with unrestricted access to resources under the Joint Intelligence Committee (JIC). Since developing a specialised in-house LLM for strictly military applications will require training on structured and classified intelligence data. Moreover, India's LLM must have a 'shape and behaviour' which is best suited to its security environment. Because of that, an Indian military LLM must evolve around the

stakeholders who have the best understanding of India's threat-security landscape. As the development of AI-enabled systems should be under JIC, its deployment authority can be given to the Chief of Defence Staff (CDS), who can effectively ensure that the three forces within the AI-assisted intelligence lifecycle. This 'two arm's structure will act as a person firing a handgun, where one will remain focused on pulling the trigger while the other will support to counter the recoil while ensuring accuracy. A command force to oversee the execution of the AI kill chain can be established on the model of India's Strategic Forces Command (SFC) under the CDS. A similar group of intelligence officers with technical expertise and professional experience in the domain can be employed to oversee the development and efficiency of the kill chain, under the JIC.

To acquire an AI-enabled kill chain, India needs a heavy investment in creating a 'parallel data architecture', a dedicated successive stream of LLMs and AI tools designed for specific needs in neutralising a wide array of threats. Such data architecture may involve parallel development of 1) a structured surveillance data collection system from strategic installation of sophisticated sensor-based surveillance devices across the border areas and in the disturbed and sensitive regions like Jammu and Kashmir and 2) a state-of-the-art secure and integrated indigenous in-house cloud-based data storage and server facility. In March 2024, under the India AI mission, the cabinet approved a massive budget of ₹10,371.92 crore to be spent over the next 5 years, along with a facility of 38,000 GPUs (to process data and for machine learning).[31] In the civilian AI domain, it is a significant step; however, in the defence sector, the annual AI-centric budget allocation is only ₹100 crore, as per the Chandrasekaran Committee's recommendations.[32] This amount will not be enough by a long margin for making any significant AI infrastructure in the defence-specific domain. The second step would be to bring the best minds of the country together to build a series of LLMs tailored to accommodate a futuristic threat foresight. This will need a GPU infrastructure connected to the in-house cloud database. India's ongoing cloud initiatives, such as the MeghRaj National Cloud, could be a start but may not be enough, considering the scale of data needed for an accurate AI machine. The last step would be to create various AI tools, as per the security needs, consistently evolving to

absorb new threat dimensions, and are highly accurate, to keep the collateral to a minimum.

Having an effective AI-enabled kill chain can offer many strategic and tactical advantages to India's security forces. An effective demonstration of such a kill chain against the cross-border terrorists can very well create a deterrence from Pakistan ever trying to use terrorism as a tool of diplomacy.

Conclusion

The paper, through a case study analysis, demonstrates that the use of AI in warfare can take extreme turns, enabling a technologically advanced military to dominate a sub conventional contested theatre. AI-enabled kill chain systems used by the IDF represent a structural transformation in the logic of warfare, beyond mere technological enhancements, compressing decision cycles and blurring the boundaries between tactical execution and strategic intent. At the cost of profound ethical, legal, and escalation risks, the Israeli case illustrates both the operational advantages of speed, precision, scale, and low cost of warfare. For India, following this development through blind imitation or cautious stagnation may not work in the long run, but a quick and calibrated adaptation addressing the complex spectrum of hybrid threats will go a long way. To that end, India's path must be locked onto building its indigenous and mission-oriented AI capabilities, taking it as a mission supervised by the highest of authorities. These capabilities must remain, through their evolution, anchored in doctrinal clarity and a robust data ecosystem.

The framework suggested in this paper must be built with an integrated approach, inviting and incorporating inputs from all key stakeholders involved in keeping India secure and assertive.

DISCLAIMER

The paper is the author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS, the Defence forces, or the Government of India. The author certifies that the article is original in content, unpublished, and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

Endnotes

[1] Eadon, Yvonne M. "LLMs, Autonomous Weapons, and Human Rights | Annenberg." Official University Website. University of Pennsylvania, Annenberg School for Communication, 2025. https://www.asc.upenn.edu/research/centers/milton-wolf-seminar-media-and-diplomacy.
[2] The IDF's Use of Data Technologies in Intelligence Processing. IDF Press Releases: Israel at War. Israel Defense Forces, 2024. https://www.idf.il/en/mini-sites/idf-press-releases-israel-at-war/june-24-pr/the-idfs-use-of-data-technologies-in-intelligence-processing-published-june-18-2024/.
[3] Dziak, Mark. "Kill Chain - EBSCO Research." EBSCO, 2024. https://www.ebsco.com/research-starters/computer-science/kill-chain.
[4] Ruiz, Ashley. "The Future of War: Kill-Chain Supremacy and Ukraine's Lessons." Journal of Strategic Security 18, no. 4 (2025): 53–63. https://doi.org/10.5038/1944-0472.18.4.2592.
[5] Grant, Tim, and Bas Kooter. Comparing OODA and Other Models as Operational View C2Architecture. June 13, 2005.
[6] "Innovation That Matters | Ultra I&C." Company Website. How Ultra I&C's Solutions Are Improving the F2T2EA Kill Chain Model, February 8, 2023. https://www.ultra-ic.com/blog/how-ultra-ic-s-solutions-are-improving-the-f2t2ea-kill-chain-model/.
[7] Gupta, Aman. "What Is 'Ghost Murmur'? The Secret CIA Heartbeat Tracker Used to Find Downed American Pilot in Iran." Mint, April 8, 2026. https://www.livemint.com/technology/tech-news/what-is-ghost-murmur-the-secret-cia-heartbeat-tracker-used-to-find-downed-american-pilot-in-iran-11775630423998.html.
[8] AFP. "AI at War I What to Know about Project Maven." Technology. The Hindu, April 6, 2026. https://www.thehindu.com/sci-tech/technology/ai-at-war-l-what-to-know-about-project-maven/article70828735.ece.

[9] Questions and Answers: Israeli Military's Use of Digital Tools in Gaza | Human Rights Watch. September 10, 2024. https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-of-digital-tools-in-gaza.
[10] Schmitt, Michael N. "Israel – Hamas 2024 Symposium - The Gospel, Lavender, and the Law of Armed Conflict." Lieber Institute West Point, June 28, 2024. https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/.
[11] Gray, Chris Hables. "AI at War." In AI, Sacred Violence, and War—The Case of Gaza, edited by Chris Hables Gray. Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-81501-0_4. Chapter 4, P87.
[12] Qandeel, Mais, and Özgün Erdener Topak. "Genocidal Surveillant Assemblage in Palestine: A Socio-Legal Analysis." Journal of Genocide Research, October 8, 2025, 1–22. https://doi.org/10.1080/14623528.2025.2567372.
[13] Gray, Chris Hables. "AI at War." In AI, Sacred Violence, and War—The Case of Gaza, edited by Chris Hables Gray. Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-81501-0_4.
[14] Lunden, Ingrid. "AnyVision, the Controversial Facial Recognition Startup, Has Raised $235M Led by SoftBank and Eldridge." TechCrunch, July 7, 2021. https://techcrunch.com/2021/07/07/anyvision-the-controversial-facial-recognition-startup-has-raised-235m-led-by-softbank-and-eldridge/.
[15] Xavier, John. "How Israel Used Azure to Monitor Palestinians | Explained." World. The Hindu, September 28, 2025. https://www.thehindu.com/news/international/how-israel-used-azure-to-monitor-palestinians-explained/article70103052.ece.
[16] Darati, Sayid R. "From Productive Force to Destructive Force: Digital Colonialism in Palestine." News & Analysis. Bianet, October 7, 2025. https://bianet.org/yazi/from-productive-force-to-destructive-force-digital-colonialism-in-palestine-312332.
[17] Schmitt, Michael N. "Israel – Hamas 2024 Symposium - The Gospel, Lavender, and the Law of Armed Conflict." Lieber Institute West Point, June 28, 2024. https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/.
[18] Hall, Wynton. "AI Warfare Is Here in the Form of Quadcopters and High-Tech Drones, NYPost." News & Analysis. NewYork Post, March 15, 2026. https://nypost.com/2026/03/15/us-news/ai-warfare-is-here-in-the-form-of-quadcopters-and-high-tech-drones/.
[19] Iraqi, Amjad. "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza." +972 Magazine, April 3, 2024. https://www.972mag.com/lavender-ai-israeli-army-gaza/.
[20] Gray, Chris Hables. "AI at War." In AI, Sacred Violence, and War—The Case of Gaza, edited by Chris Hables Gray. Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-81501-0_4. Chapter 4, P86.
[21] Dobler, Yannik. "Palantir: A Software That Safes and Takes Lives." Digital Innovation and Transformation, November 30, 2022. https://d3.harvard.edu/platform-digit/submission/palantir-a-software-that-safes-and-takes-lives/.
[22] Singh, Thangjam K., and Deepak Tiwari. "Disruptive Technologies in Strategic Affairs Threats and Preparedness for India." Comparative Strategy 44, no. 4 (2025): 460–72. https://doi.org/10.1080/01495933.2025.2504854.
[23] Press, Information Bureau. "Transforming India with AI." Government of India. Press Information Bureau, PIB Headquaters, December 30, 2025. https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=2209737.
[24] Saini, Gaurav. India's Approach to Military AI: Strategy, Governance, and Challenges. Geopolitcs and International Security Program Series. The Council for Strategic and Defense Research (CSDR), 2026. https://csdronline.com/wp-content/uploads/2026/02/CSDR_Feb-26_Indias-Approach-to-Military-AI-1.pdf.

[25] Mishra. “Artificial Intelligence (AI) in Defence Modernisation.” Business Analytic. KPMG, KPMG, June 23, 2025. https://kpmg.com/in/en/blogs/2025/06/artificial-intelligence-in-defence-modernisation.html.
[26] “Artificial Intelligence Strategy for the Department of War.” MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP. SECRETARY OF WAR, June 2026. https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF.
[27] Saini, Gaurav. India’s Approach to Military AI: Strategy, Governance, and Challenges. Geopolitcs and International Security Program Series. The Council for Strategic and Defense Research (CSDR), 2026. https://csdronline.com/wp-content/uploads/2026/02/CSDR_Feb-26_Indias-Approach-to-Military-AI-1.pdf.
[28] PIB Headquaters. “Framework & Guidelines to Integrate Trustworthy AI into Critical Defence Operations Unveiled.” Government of India. Press Information Bureau, October 17, 2024. https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=2065847.
[29] Ibid
[30] Express, News Service. “Role of Humans in AI Dictated War Decisions, Reflections on West Asia Conflict and Operation Sindoor Feature at Second Joint Indian Defence Leaders Summit | Bangalore News - The Indian Express.” News & Analysis. Indian Express, April 11, 2026. https://indianexpress.com/article/cities/bangalore/role-of-humans-in-ai-dictated-war-decisions-reflections-on-west-asia-conflict-and-operation-sindoor-feature-at-second-joint-indian-defence-leaders-summit-10631007/.
[31] Press, Information Bureau. “Transforming India with AI.” Government of India. Press Information Bureau, PIB Headquaters, December 30, 2025. https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=2209737.
[32] Hooda, Lt. Gen. Deependra Singh. “Implementing Artificial Intelligence in the Indian Military.” Delhi Policy Group (New Delhi, India), no. DPG Policy Briefs (February 2023). https://www.delhipolicygroup.org/.