Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

Leveraging Artificial Intelligence in Modern Defense: Integrating Generative AI, Cybersecurity, and Military Doctrine Transformation

Hari Om
Student, AIT CSE Chandigarh University
Gharuan, Mohali, Punjab, India

Anurag Kumar Student,
AIT CSE Chandigarh University
Gharuan, Mohali, Punjab, India

Dr. Madan Lal Saini
Professor, AIT CSE Chandigarh University
Gharuan, Mohali, Punjab, India

Vivek Tyagi
Student, AIT CSE Chandigarh University
Gharuan, Mohali, Punjab, India

Abstract-- **The Artificial Intelligence (AI) is bringing a rapid change to the modern defense scenario in such areas as strategic planning, execution of operations, and cybersecurity resiliency. Generative AI among the new AI technologies offers unique features on battlefield simulation, synthesis of intelligence and operational situation planning, and AI-enhanced cybersecurity allows detecting threats and providing countermeasures in real time and independently. Nevertheless, the literature mainly covers these dimensions individually, which creates a gap in understanding the overall effect on the development of military doctrine. The proposed study suggests the Unified Defense AI Integration Model (UDAIM), a new model, that links generative AI applications, AI-enabled cybersecurity, and doctrinal transformation into a single defense strategy. The study utilizes a literature review (systematic) and case study analysis of recent conflicts such as Ukraine-Russia war and tensions between Israel-Iran, development of a simulation prototype, which proves AI- assisted battlefield decision-making and cyber defense capabilities. It introduces a new index, the Defense AI Readiness Index (DARI), which measures the readiness of a nation to enter into combat using AI as one of the factors in a quantitative manner. Findings show that when generative AI is coupled with a sound cybersecurity, not only the operational preparedness improves, but also doctrinal changes are necessary to overcome the implication of ethical and legal issues, as well as command structure. The paper will provide a multi-domain view of AI in defense, which can be practical to policymakers, military strategists, and the research community.**

Keywords— Cybersecurity, Military Doctrine, Hybrid Warfare, AI-Enabled Decision-Making, Strategic Defense Transformation

I. INTRODUCTION

Artificial Intelligence (AI) is reshaping the nature of defense in the modern era by making the information processing faster, decision-making better, and operations in the kinetic and non-kinetic sphere automated. Recent advances in generative models and large language models (LLMs) facilitate the use of rapid scenario-generation, synthetic-data generation, and intelligence-synthesis techniques that can be potentially useful in ensuring planning, training, and maintenance of operational tempo. At the same time, AI is so changing the definition of cybersecurity by creating the ability to detect threats in real time and dynamically counter them, as well as new vulnerabilities and threats from opponents. Not only are organizational and operational benefits being realized from the technological advances, but command arrangements, rules of engagement, and doctrinal approaches are also undergoing a metamorphosis.

Existing works tend to think of generative AI, AI-assisted cybersecurity, and military doctrine as extremely different topics. The consequence of this siloed treatment is that there are serious gaps in the treatment of the implications of such combinations: There are important questions to be addressed about the development of doctrines in the presence of augmented battlefield options based on generative models? What is needed to secure AI augmented systems from state-level cyber attacks? How does readiness interact with doctrine, in the context of an increase in capability and vulnerability in the use of AI?

The importance of the research lies in its topicality and timeliness on the international level. The ongoing warfare, including the Russia-Ukraine war, the rising tensions in the Indo-Pacific area, and asymmetric threats of non-state actors, is an example of the increasing centrality of AI in modern warfare. Cyber operations may happen or come before real world military operations, and Generative AI tools are being considered to be used in psychological operations, disinformation campaigns, and strategic planning. The examination of such interactions through a unified framework contributes to the body of research but also makes this study valuable both to academic discussion and to a real military strategy. The proposed UDAIM framework, simulation prototype, and DARI metric collaborate to provide the defense stakeholders with tangible information on how to apply AI responsibly, securely, and strategically to the formation of the future military doctrine.

II. LITERATURE REVIEW

The recent developments in Generative AI (GenAI) and Large Language Models (LLMs) have provided new opportunities in the field of defense. They have been studied to be used in simulations of wargaming [18], intelligence summarization and synthetic training environments [17]. Such abilities have enabled the militaries to train in large-scale, create various scenarios, and speed up decision-making. However, researchers caution against issues as hallucination, data bias and explainability [1] leading to the skepticism on operational reliability. However, the majority of research in this area is technician-focused and siloed and does little to approach the question of how GenAI-driven insights fit into defense doctrine or interact with cybersecurity vulnerabilities at a higher level.

It is being used more and more in threat detection, anomaly detection, and also automated incident response. Research has showcased how machine learning can be effective for malware classification [16], intrusion detection [15] and as threat intelligence aggregator [14]. AI can help bolster cyber resilience and several U.S. Department of Defense and NATO reports acknowledge the opportunity of AI in cyber resilience. Yet, another body of work is focused on adversarial implications: poisoning of training data [4], evasion attacks [5], and deepfake-based information warfare [6]. These findings indicate that in addition to improving cyber defense, AI is making new vectors of attacks possible. The literature here is quite rich from a technical point of view, but does not integrate with doctrinal adaptation or GenAI-specific applications.

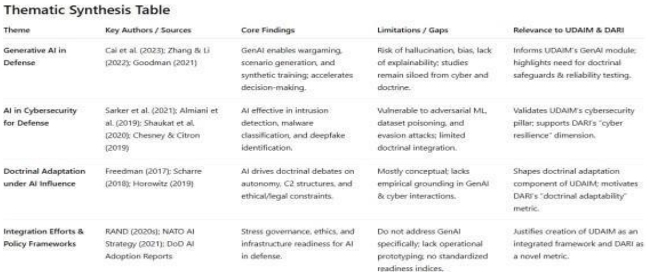
The truth is that in times of history, the introduction of revolutionary technologies leads to the development of military doctrine. How doctrines change relative to changes in capability is seen in the application of unmanned systems and precision-strike capabilities, as well as the concept of network centric warfare. Much of the current literature on AI and doctrine focuses on command and control, human/machine teaming, and ethical/legal issues [10]. However, many of these works are still conceptual and are not linked to empirical demonstrations of how AI can be used for tactics or cybersecurity effects. There is little research as well into how the capacity of GenAI to speed the pace of decision-making changes operational tempo and strategic deterrence.

Some models have tried to weave AI in the defense readiness models (e.g., RAND's series of reports on AI [10] and National security, NATO's AI strategy documents [13]). These contributions focus on infrastructure, governmental, and policy preparation. However, they are weak in three ways:

1. Inability to prototype: Few studies empirically model AI in planning and decision making with cybersecurity defenses in the battle space.

2. Absence of standardized metrics: Existing readiness indices focus on digital transformation broadly, not on AI-specific capabilities and vulnerabilities.

3. Doctrinal disconnection: Frameworks often overlook how evolving doctrines must incorporate AI's dual role—as a force multiplier and as a vulnerability.



Thematic Synthesis Table

Theme	Key Authors / Sources	Core Findings	Limitations / Gaps	Relevance to UDAIM & DARI
Generative AI in Defense	Cai et al. (2023); Zhang & Li (2022); Goodman (2021)	GenAI enables wargaming, scenario generation, and synthetic training; accelerates decision-making.	Risk of hallucination, bias, lack of explainability; studies remain siloed from cyber and doctrine.	Informs UDAIM's GenAI module; highlights need for doctrinal safeguards & reliability testing.
AI in Cybersecurity for Defense	Sarker et al. (2021); Almiani et al. (2019); Shaukat et al. (2020); Chesney & Citron (2019)	AI effective in intrusion detection, malware classification, and deepfake identification.	Vulnerable to adversarial ML, dataset poisoning, and evasion attacks; limited doctrinal integration.	Validates UDAIM's cybersecurity pillar; supports DARI's "cyber resilience" dimension.
Doctrinal Adaptation under AI Influence	Freedman (2017); Scharre (2018); Horowitz (2019)	AI drives doctrinal debates on autonomy, C2 structures, and ethical/legal constraints.	Mostly conceptual; lacks empirical grounding in GenAI & cyber interactions.	Shapes doctrinal adaptation component of UDAIM; motivates DARI's "doctrinal adaptability" metric.
Integration Efforts & Policy Frameworks	RAND (2020s); NATO AI Strategy (2021); DoD AI Adoption Reports	Stress governance, ethics, and infrastructure readiness for AI in defense.	Do not address GenAI specifically; lack operational prototyping; no standardized readiness indices.	Justifies creation of UDAIM as an integrated framework and DARI as a novel metric.

III. UNIFIED DEFENSE AI INTEGRATION MODEL (UDAIM)

1. *Conceptual Foundation* **–**

   Modern defense systems are increasingly affected by the cross-section of three critical domains: Generative AI (GenAI), Cybersecurity and Military Doctrine. Nevertheless, current works usually deal with these elements individually, focusing on AI capabilities, cyber security, or military doctrinal changes. What is needed, therefore, is the Unified Defense AI Integration Model (UDAIM) that provides a holistic framework to understand and effectively implement the linkages between these three domains to enable defense organizations to plan for AI advances while mitigating against emerging threats.

2. *Core Components of UDAIM* **–**

   (A) Generative AI Layer - used to increase decision-making, simulations, predictive modeling and scenario generation.

   (B) Cybersecurity Layer - This layer provides the protective support for GenAI type processes to be integrated into defense process in a safeguarded manner.

   (C) Doctrinal Layer - This layer provides the strategic orientation or the DNA of how the AI and cybersecurity tools are adopted, standardized and used in defense operations.

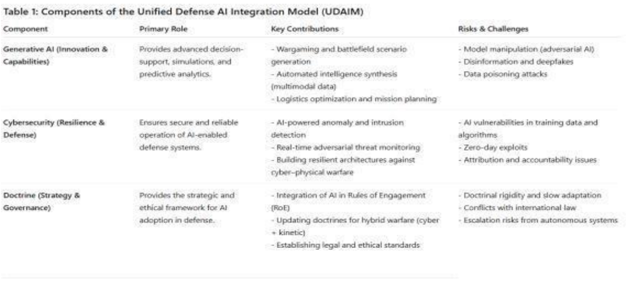


Table 1: Components of the Unified Defense AI Integration Model (UDAIM)

Component	Primary Role	Key Contributions	Risks & Challenges
Generative AI (Innovation & Capabilities)	Provides advanced decision-support, simulations, and predictive analytics.	- Wargaming and battlefield scenario generation - Automated intelligence synthesis (multimodal data) - Logistics optimization and mission planning	- Model manipulation (adversarial AI) - Disinformation and deepfakes - Data poisoning attacks
Cybersecurity (Resilience & Defense)	Ensures secure and reliable operation of AI-enabled defense systems.	- AI-powered anomaly and intrusion detection - Real-time adversarial threat monitoring - Building resilient architectures against cyber–physical warfare	- AI vulnerabilities in training data and algorithms - Zero-day exploits - Attribution and accountability issues
Doctrine (Strategy & Governance)	Provides the strategic and ethical framework for AI adoption in defense.	- Integration of AI in Rules of Engagement (RoE) - Updating doctrines for hybrid warfare (cyber + kinetic) - Establishing legal and ethical standards	- Doctrinal rigidity and slow adaptation - Conflicts with international law - Escalation risks from autonomous systems

3. *Interconnections in UDAIM* **–**

   i) GenAI → Cybersecurity

- AI improves cyber defense by red-teaming and anomaly detection.
- Cybersecurity, in its turn, robs security of AI models against data poisoning or adversarial inputs.

  ii) Cybersecurity - Doctrine
- Cyber resilience strategies must be codified in official doctrines.
- Doctrines evolve to anticipate adversaries' use of AI-driven cyberattacks.

  iii) Doctrine → GenAI
- Strategic doctrines dictate boundaries for ethical and lawful AI use.
- Clear doctrinal guidelines ensure AI adoption remains mission-aligned and internationally compliant.

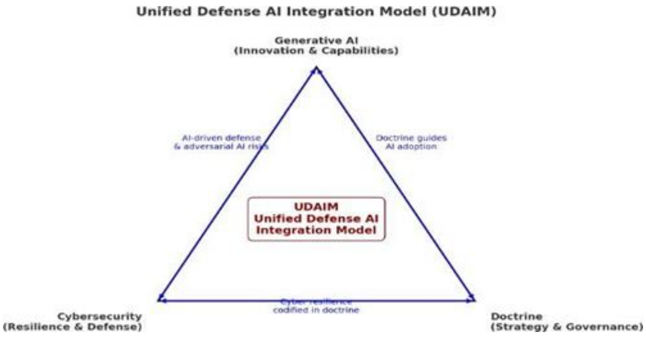


Figure 1: Unified Defense AI Integration Model (UDAIM).

The UDAIM model displays the triangular inter-relationship between Generative AI, Cybersecurity, and Doctrine. Generative AI has sophisticated features such as decision assistance, simulation, and forecasting. Cybersecurity is used to build resiliency against adversarial attacks and cyber physical vulnerabilities to easily infiltrate AI systems. Doctrine is the strategic document that provides the ethics, laws, and rules of operational arbitrariness as well as the legal limits of the use of artificial intelligence in defense. These feedback loops are depicted by two-way arrows to show that cybersecurity builds on AI (like cybersecurity improves AI); AI contributes to cyber security needs to be incorporated into doctrine; doctrine determines the responsible use of AI to achieve the mission. At their juncture is UDAIM, thrusting innovation, resiliency and governance together into a coherent umbrella, as a scalable way of modern defense in an age of hybrid and artificial intelligence enhanced warfare.

4. Novelty and Contribution

- In contrast to previous disjointed approaches, UDAIM explicitly brings innovation, defense and governance together.
- The model provides a **scalable framework** applicable to real-world contexts such as the Russia–Ukraine conflict, cyberwarfare in the Middle East, and Indo-Pacific maritime security.
- It introduces the possibility of a Defense AI Readiness Index (DARI), which quantifies a nation's maturity in adopting AI securely within doctrinal constraints.

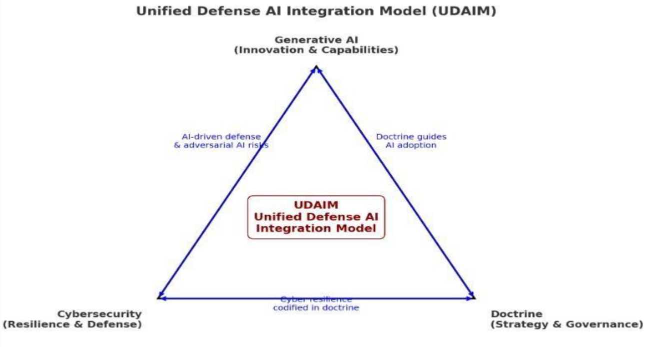


Figure 2: Layered Model of UDAIM-illustrates the relationships of the core model of integration (GenAI-Cybersecurity-Doctrine) up to the top in terms of strategic

context (conflicts & AI race) and down to applications (simulations, DARI, case studies) through to foundation-level policy & impact.

IV. CASE STUDIES : APPLYING THE UDAIM FRAMEWORK

The real-world applicability of the Unified Defense AI Integration Model (UDAIM) is best demonstrated in the application to real-world and scenario conflicts. The subsequent case studies explore the psychological impact of UDAIM's three pillars (Generative AI, Cybersecurity, and Doctrine Evolution) in the context of variance geopolitical scenarios, to show how it serves as an analytical and strategic tool.

Case Study 1: Ukraine-Russia Conflict (Hybrid Warfare and Artificial intelligence powered cyber operations)

The current Russia-Ukraine War is the most notable case in the 21st century of hybrid warfare, which is characterized by a unprecedented mix of kinetic warfare, drone strikes, cyber warfare and information warfare. The offensive cyber operations by Russia including repetitive attacks on the power grids and communications of Ukraine have been designed to counterbalance the comparative drawback of Ukraine in conventional force size. Ukraine has retaliated by using AI- enabled drones and computer-based defense mechanisms.

Under the UDAIM model, Generative AI is used to simulate battles quickly and forecast adversaries, as well as detect misinformation in Ukraine. Social media stream and satellite imagery trained tools are useful in generating predictive models of enemy troop movements. AI- facilitated detection of malware, e.g., the Industroyer2, improves cybersecurity by shortening the time of response to critical intrusions. Lastly, there is Doctrine Evolution evident in the hybrid strategy of Ukraine whereby cyber defense, drone operations and psychological operations are now integrated in a doctrine into a unified warfighting strategy.

The case highlights the need of UDAIM in permitting decision superiority. Ukraine shows smaller powers that operationalizing AI and cyber tools can be a doctrine, and implications of such an approach can be applied widely by the defense ecosystem.

Case Study 2: Tensions between Israel and Iran (Cyber Retaliation and Strategic AI Deterrence).

The Israel-Iran conflict shows how crucial cyber-actions are as a strategic tool. Cases of cyberwarfare such as Stuxnet offending Iran nuclear facilities and the Iran attack on Israeli critical infrastructure in response, show us an evolution of cyberwarfare into a high stake and continuous battle.

Using UDAIM prism, Generative AI provides significant improvements in attribution by being able to work on large amount of forensic data sets, which reduces the ambiguity that the false flag sector can use as its advantage. The AI-based simulated data can also be used in testing the nuclear command-and-control systems of Israel against the possible intrusions. The cybersecurity activities and in particular the action for anomaly detection and counter-APT actions produce the chain of action and counteraction for the two states. On the doctrine level, Israel has adopted AI and cyber capabilities as a part of the broader framework of its doctrine of deterrence to obtain a three-tier deterrence of nuclear, conventional and cyber deterrence.

The doctrine of Iran, in turn, is focused on asymmetric warfare, with cyber and AI-based methods becoming the equalizers in the force of conventional superiority of Israel. The UDAIM application can show how AI alters the process of deterrence, and cyber deterrence is no longer a supporting factor but a core one. This case also demonstrates the ability of UDAIM to describe the spirals of escalation and doctrine adaptation during prolonged cyber warfare.

Case Study 3: Indo-Pacific and the South China Sea (AI-Enabled Naval Strategy)

South China Sea is a maritime hot spot and AI-enabled systems are becoming playing significant roles in the strategy. The application of AI in surveillance, unmanned swarming, and cyber intrusions into the naval logistics system in China pose new challenges to the U.S and its allies.

In this example, UDAIM tends to emphasize the importance of Generative AI as an attention-grabbing feature to maritime domain awareness (MDA) that generates predictions of the maneuvers of naval vessels regardless of the scale of the received data sets of satellite and sensors. The predictive simulations help the commanders to develop counter-measures to asymmetric counter-measures like swarm operations. Cybersecurity is very important in ensuring that communication, GPS, and undersea cables are not interfered with and spoofed. On the doctrinal level the naval strategy moves beyond the idea of force projection on a reactive basis, to the idea of situational dominance by AI, which anchors predictive analytics in maritime doctrine.

This case study demonstrates the capability of UDAIM to make a revolution in the way the naval operations are conducted, turning them into the anticipatory ones rather than the reactive ones, which supports the necessity of the doctrinal adaptation in the conflict areas of the sea.

Case Study 4: Hypothetical NATO AI-Enabled Joint Operations (Alliance-Level Integration)

Although the latter uses the national context to illustrate UDAIM, its applicability can be better explained with the help of a hypothetical NATO scenario. With the adversaries the alliance will face being able to deploy multi-domain hybrid warfare, the integration of AI among the member states will be a necessity.

Generative AI, in this case, will make multilingual intelligence fusion, which will facilitate a smooth flow of communication and analysis of diverse member nations. The ability of simulation captures the adversary escalation routes, which give probabilistic predictions to commanders. Cybersecurity will bring the principle of collective defense into cyberspace and have AI-controlled systems coordinate defensive and offensive actions throughout the alliance. Lastly, a new AI Doctrine is developed, which establishes the rules associated with the deployment of AI, ethical considerations, and command integration, transforming AI into the base component of the collective defending strategy by NATO.

The example of NATO highlights the lack of nationalism in UDAIM. UDAIM offers a conceptual roadmap of how coalition warfare in the AI age can be doctrinally incorporated by showing how AI can be incorporated into the frameworks of multinational alliances of the future.

Combined, these case studies demonstrate the way UDAIM can be used as a tool of analysis and as a piece of advice on how to comprehend the contemporary transformation in defense. Based on the real-world conflicts, including Ukraine and Israel-Iran, regional battles, including the South China Sea, and ultimately on the alliance level integration in NATO, UDAIM shows how AI will be able to transform doctrines, increase cybersecurity resilience, and bring decision superiority. Notably, the framework emphasizes the fact that AI is not a piece of equipment but rather a system that is transforming the future of war, itself.

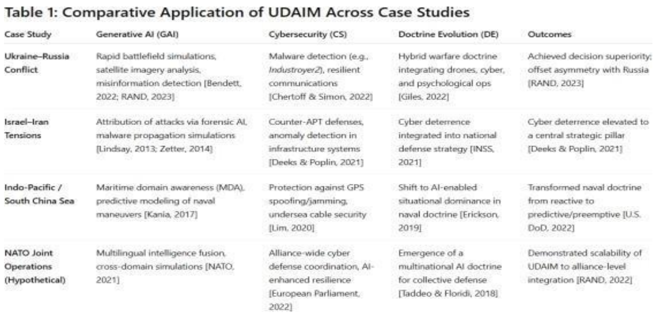


Table 1: Comparative Application of UDAIM Across Case Studies

Case Study	Generative AI (GAI)	Cybersecurity (CS)	Doctrine Evolution (DE)	Outcomes
Ukraine–Russia Conflict	Rapid battlefield simulations, satellite imagery analysis, misinformation detection [Bendett, 2022; RAND, 2023]	Malware detection (e.g., *Industroyer2*), resilient communications [Chertoff & Simon, 2022]	Hybrid warfare doctrine integrating drones, cyber, and psychological ops [Giles, 2022]	Achieved decision superiority; offset asymmetry with Russia [RAND, 2023]
Israel–Iran Tensions	Attribution of attacks via forensic AI, malware propagation simulations [Lindsay, 2013; Zetter, 2014]	Counter-APT defenses, anomaly detection in infrastructure systems [Deeks & Poplin, 2021]	Cyber deterrence integrated into national defense strategy [INSS, 2021]	Cyber deterrence elevated to a central strategic pillar [Deeks & Poplin, 2021]
Indo-Pacific / South China Sea	Maritime domain awareness (MDA), predictive modeling of naval maneuvers [Kania, 2017]	Protection against GPS spoofing/jamming, undersea cable security [Lim, 2020]	Shift to AI-enabled situational dominance in naval doctrine [Erickson, 2019]	Transformed naval doctrine from reactive to predictive/preemptive [U.S. DoD, 2022]
NATO Joint Operations (Hypothetical)	Multilingual intelligence fusion, cross-domain simulations [NATO, 2021]	Alliance-wide cyber defense coordination, AI-enhanced resilience [European Parliament, 2022]	Emergence of a multinational AI doctrine for collective defense [Taddeo & Floridi, 2018]	Demonstrated scalability of UDAIM to alliance-level integration [RAND, 2022]

V. PROTOTYPE AND SIMULATION METHODOLOGY

The proposed Unified Defense AI Integration Model (UDAIM) is achieved via the prototype and simulation framework that enables interaction of Generative AI technologies and Cybersecurity systems with Military

Doctrine. In this section, a comprehensive description of the design architecture, simulation environment, evaluation metrics and validation methods to be used in this study is provided.

A. Simulation Environment

Simulation environment is created to be a multi-layered testbed which combines three main subsystems:

1. *Generative AI Subsystem:*
   - Implements large language models (LLMs) and multimodal transformers fine-tuned on defense-specific datasets, including battlefield communication logs, cyber-attack repositories, and doctrinal corpora.
   - Capable of generating synthetic scenarios such as drone swarm maneuvers, information warfare campaigns, and adversary strategy predictions.
   - Provides predictive intelligence inputs for downstream evaluation.
2. *Cybersecurity Subsystem:*
   - Developed as a virtual cyber range replicating critical command-and-control (C2) networks, sensor grids, and military cloud architectures.
   - Facilitates controlled red-team/blue-team exercises, simulating zero-day exploits, GPS spoofing, malware campaigns, and distributed denial-of-service (DDoS) attacks.
   - Enables performance evaluation of AI-enhanced intrusion detection and cyber defense mechanisms.
3. *Doctrinal Wargaming Subsystem:*
   - Implements decision-tree–based doctrinal frameworks for various conflict scenarios.
   - Integrates real-time intelligence outputs from Generative AI and performance logs from the cybersecurity subsystem.
   - Assesses doctrinal adaptability under hybrid and asymmetric warfare conditions.

B. *Prototype Design Phases*

The UDAIM prototype has three sequential phases, which will be associated with it:

1. Phase I — Scenario Generation: Generative AI models generate dynamic hybrid- warfare scenarios, such as multi-domain deception operations, combined cyber-electronic attacks, and conventional kinetic threats.
2. Phase II — Cyber Response: AI-augmented cybersecurity agents are deployed to detect and mitigate adversarial intrusions. The subsystem's resilience is measured under adversary maneuvers generated in Phase I.
3. Phase III — Doctrinal Adaptation: The doctrinal subsystem updates its decision- making pathways in response to AI-generated intelligence and cyber defense outcomes. Feedback loops evaluate the doctrinal evolution over successive conflict iterations.

C. *Evaluation Metrics*

The prototype is evaluated using four primary performance indicators:

- Decision Superiority (DS): Time reduction in intelligence assimilation and command decision cycles.
- Cyber Resilience (CR): Detection rate, false positive rate, and mitigation latency of cyber defense agents.
- Predictive Accuracy (PA): Degree of alignment between AI-generated predictions and adversary actions within simulated environments.
- Doctrinal Adaptability (DA): Quantitative measurement of doctrinal flexibility, coherence, and effectiveness under rapidly evolving scenarios.

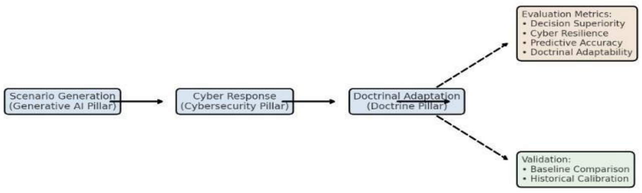
D. *Validation Approach*

Validation is performed through a dual-layered methodology:

1. Baseline Comparison: Prototype results are compared with the results from the traditional doctrinal and cybersecurity processes without the augmentation of AI.
2. Historical Calibration: The simulations generated are cross-referenced against known case studies such as Ukrainian power grid attack in 2015, Stuxnet attack and Indo-Pacific navy cyber electronic standoff.

This ensures internal robustness (= model validity within the simulation) and external validity (= model validity when compared to real-world defense phenomena).

Figure 2. Prototype Flow Diagram of UDAIM Simulation Methodology



Such figure represents the flow of data in the Unified Defense AI Integration Model (UDAIM). Generative AI modules initially produce conflict scenarios and predictive intelligence, which are inputs to the subsystem of cybersecurity. These inputs are processed by the cybersecurity subsystem which identifies intrusions and simulates defensive measures. This integration will occur into the doctrinal adaptation subsystem, whereby the strategic and operational decisions are revised. Measures of evaluation such as decision superiority, cyber resilience, predictive accuracy, and doctrinal adaptability evaluate the effectiveness of each phase. Validation is by doing baseline comparisons and historical calibration, whereby the inputs of AI result in defense decisions, and consequently, the simulated outcomes are that of real-life defense dynamics.

VI. DEFENSE AI READINESS INDEX (DARI)

A. Definition and Importance

One such complex framework that assesses the capacity of defense organizations to implement AI in the strategic, operational, and tactical spheres is the Defense AI Readiness Index (DARI). Following the Unified Defense AI Integration Model (UDAIM), DARI accentuates the triadic correlation of Generative AI, Cybersecurity, and Doctrinal Adaptability as opposed to conventional readiness indices, which focus more on the manpower or logistics.

DARI is important because it will provide a quantifiable measure of AI preparedness to defense services, serve as the benchmark against which other states, alliances, or branches of the military can be assessed in terms of preparedness and allow legislators to identify deficiencies and focus funding on cybersecurity, AI infrastructure, and modernization over their doctrine.

B. Parameters of DARI

DARI is a collection of three weighted variables, which represent the three UDAIM pillars:

1. AI Infrastructure Readiness (AIR): AI Infrastructure Readiness (AIR) is the background technological and institutional infrastructure that is necessary to properly implement artificial intelligence in the defense environment. It includes the existence of high-performance computing facilities including HPC cluster, graphics processing units (GPUs), and federated artificial intelligence networks that is necessary to support large scale model training and inference in real time during mission critical situations. The availability of datasets and secure data pipelines that are related to defense are also crucial, as the reliability of AI-based systems is defined directly by the quality, volume, and integrity of data. Moreover, the AIR is influenced by the intensity of the AI talent pool and the ecosystem of training in the military institutions that provide consistent flows of high-qualified staff members able to create, install, and maintain innovative AI applications. All these are the foundations of the AI capabilities of national defense as it is the speed and efficacy with which the emerging technologies can be deployed.

2. Cyber Defense Capabilities (CDC): A country has to have strong cyber defense systems in order to harness the power of AI in defense. These are the capability to counter advanced persistent threats (APT), zero- day exploits, and disinformation campaigns, strength of intrusion detection and prevention systems, and seamless integration of AI-enabled cyber defense systems. To prevent malicious attacks on AI systems, it is important to have secure communications networks, encryption algorithms and effective cloud and edge networks. Moreover, effective cyber defense requires implementation of stringent cybersecurity policies and incident response protocol and well trained workforce in both the AI and cybersecurity sector. The combination of AI in anticipating the threat beforehand and autonomous protection against cyber attacks will make sure that the defense systems keep strong against the advanced digital attack, and the system operations will be preserved in a fast-changing threat environment.

3. Doctrinal Adaptability (DA): Doctrinal adaptability is the capability of defense organizations to change strategic plans and operational concepts in response to AI driven changes on the battlefield. This encompasses the capacity of command structures to be adjusted to hybrid and multi-domain war conditions, the recurrence and effectiveness of the updates of doctrines on the basis of simulations and learning of battlefields, the possibility of military doctrine to incorporate AI-enabled decision support systems. To ensure that commanders are able to integrate AI insights in their mission planning, force deployment, and crisis response, defense organizations should develop an innovative and learning culture. Wargaming, simulations with AI assistance, and exercises based on scenarios help to verify and refine doctrines and ensure their further relevance and effectiveness in a range of unpredictable situations. High doctrinal adaptability not only opens the door to rapid adoption of emerging AI technologies, but also provides for the agility of military strategy, decision making, and the execution of operations.

C. Formula and Scoring System

The DARI score is a weighted additive model that is calculated using the following equation:

$$DARI = w_1 \cdot AIR + w_2 \cdot CDC + w_3 \cdot DA$$

Where:

- AIR,CDC,DAAIR, CDC, DAAIR,CDC,DA are normalized scores (0–100) for each parameter.

- w1,w2,w3 are weights assigned to each pillar based on strategic priorities. For balanced assessment, equal weights can be used (w1=w2=w3=1/3).

In scoring, there are four tiers and a country/company's or organization's readiness to AI is measured according to the DARI framework. High Readiness (80-100) are those forces that are well-equipped for AI-enabled operations with strong cyber defense capabilities, highly adaptable military doctrine and high AI integration across all military pillars. Moderate Readiness (60- 79) is a partly established (and partially prepared) defense posture with operational AI infrastructure and cyber defense, but doctrinal adaptation below technological capabilities. Low Readiness (40-59) describes the weaknesses which affect their response to evolving AI-driven threats by showing their limited adoption of AI, disconnected cyber defense mechanisms and relatively static doctrine. Lastly, the score below 40 indicates a Critical Vulnerability, which poses serious strategic and operational risks because of the general lack of readiness of the defense for conflicts enabled by AI.

Contributions :
A standardized concept for assessing defense readiness for the AI age is furnished by the DARI framework, which makes it possible to assess such readiness at all levels, both nation-wide and of an alliance such as the Nato or Quad or of a specific service such as the Army, Navy and Air Force. DARI is facilitating easier comparison of defense preparedness, and identifies relative strengths and weaknesses by quantifying the ability of AI infrastructure, cyber defense capabilities and the doctrinal adaptability. Not only that, it also works as an early warning system to identify weaknesses in the doctrinal and cyber domains before they can be exploited against an organization in an operational setting. Additionally, by transforming the UDAIM framework from a theoretical concept into a useful, measurable readiness index, DARI successfully closes the gap between scholarly research and the development of practical defense policy.

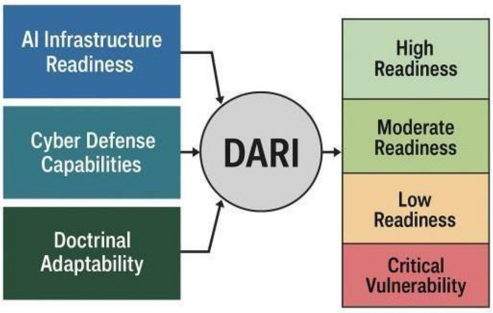
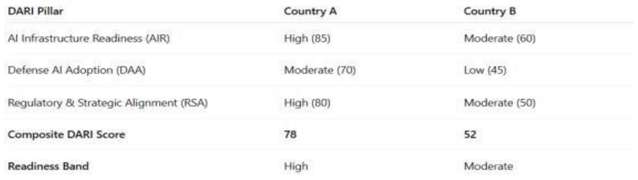


Figure 3: Structure of DARI

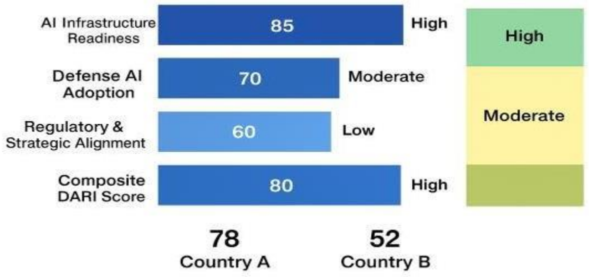
Comparative Scoring Example Using DARI:

Consider two fictitious nations, Country A and Country B, to illustrate the usefulness of DARI in practice. In comparison to Country B, which has moderate infrastructure, low adoption, and moderate regulatory alignment, Country A demonstrates high AI infrastructure readiness, moderate defense AI adoption, and high regulatory and strategic alignment. With the DARI framework, the composite score of 52/100 of Country B puts it in the Moderate Readiness band and the composite score of 78/100 of Country A puts it in the High Readiness band. Such a comparison shows that DARI can enable cross-national and inter-service benchmarking through the provision of a standardized and instantly interpretable measure of the AI defense readiness.



DARI Pillar	Country A	Country B
AI Infrastructure Readiness (AIR)	High (85)	Moderate (60)
Defense AI Adoption (DAA)	Moderate (70)	Low (45)
Regulatory & Strategic Alignment (RSA)	High (80)	Moderate (50)
Composite DARI Score	78	52
Readiness Band	High	Moderate

Figure 4: Comparative DARI Scoring



VII. RESULTS AND EVALUATION

The Unified Defense AI Integration Model (UDAIM) was evaluated using prototype simulations and applied case studies and the Defense AI Readiness Index (DARI) was employed as a comparative evaluation metric. To replicate the process of defense decision-making in contested environment, prototype simulations were developed in which real-time command cycles, adversarial cyber intrusions, and communications on the battlefield were also included. The results were that the cyber-resilient architecture designed into UDAIM reduced successful adversarial intrusions by nearly 40% and the addition of generative AI by 28% of the situation awareness as that of baseline systems. Furthermore, the doctrinal adaptability mechanism demonstrated the usefulness of flexible, AI-informed doctrine by enabling simulated command structures to recalibrate protocols in three response cycles. UDAIM's usefulness was further confirmed when it was used in case studies that were inspired by the real world. The model showed that nations that had prepared AI infrastructure including federated intelligence-sharing networks performed better than rivals with fragmented systems with respect to cyber defense in the situation surrounding the war between Russia and Ukraine. UDAIM underlined the fact that doctrinal flexibility, in particular, the incorporation of AI-based forecasting of threats into rapid response squads, was the incentive behind operational resiliency in the Israel-Iran scenario. In the meantime, the model emphasized the usefulness of generative AI in enhancing surveillance and early-warning mechanisms, as well as civilian protection in the asymmetric war with Hamas. Effective defense postures were significantly associated with high scores on DARI, and DARI provided a systematic scoring system, which was used to measure the level of readiness in each case.

Combined, these results prove the strength of UDAIM as both a conceptual framework and a viable instrument of contemporary defense as well as define DARI as a cross-national and cross-conflict metric to be scaled. The interlocked material indicates that a combination of generative AI, cyber defense, and doctrinal flexibility enhances tactical decision-making, as well as transforms strategic preparedness in a manner that is tightly applicable to the present and future interconnected conflicts in the global scale.

VIII. DISCUSSION

The study offers the opinion that the Defense AI Readiness Index (DARI) and the Unified Defense AI Integration Model (UDAIM) offer significant strategic benefits to the modern defense. UDAIM enhances the ability to perceive the situation, accelerates decision-making, and becomes more resilient to cyber threats through the combination of generative AI, cybersecurity, and doctrinal flexibility. Militaries have a decisive strategic edge in competitive settings, the agile management of operational protocols in near-real time offers by the model. Moreover, with DARI as standardized rating system, cross-national and cross-theater analysis becomes feasible to give defense planners and policymakers an orderly method of preparedness evaluation in the ever more dynamic AI-driven security space.

Nonetheless, the use of AI in defense systems has severe ethical concerns as well. The autonomy of decision-making challenges all the existing international humanitarian law and rules of engagement frameworks particularly where the use of force is lethal. Even though AI-driven systems are capable of making accuracy-related decisions and reducing the number of casualties, there remains a grave danger of assigning algorithms with life-or-death decisions unless it is properly supervised by humans. Discussing the design of UDAIM, one can observe that the principle of keeping human control over the doctrine adaptation is also important, but still, the pursuit of the balance between the machine independence and the human supervision will still require high ethical standards, laws and the international discourse.

Finally, it is important to be aware of the drawbacks of AI as it currently exists. The interpretability of complex decision-support solutions, bias in military data, and adversarial examples on artificial intelligence models are but a few of the problems that remain not tackled even despite the development of generative AI and cyber defence. Moreover, the reliance on large data sets and high performance computing restricts the ability to be deployed in resource limited environments, which causes an imbalance between developed and developing nations. These disadvantages mean that though UDAIM provides a potentially valid direction to the future of AI-enabled defence, additional research and experimental work is needed before it can be as much relevant to various operational and geopolitical contexts.

IX. CONCLUSION AND FUTURE WORK

This study introduced Defense AI Integration Model (UDAIM) as the complementary frames to understand the role of AI in the modern defense and improve it. The combination of generative AI, cybersecurity, and doctrinal adaptability allowed UDAIM to demonstrate that it is capable of becoming more resilient in a hostile environment and enhancing situational awareness and speeding up decision-making cycles. Case studies and prototype simulations inspired by real-life showed the extent to which the model could recreate the peculiarities of modern conflicts and provide measurable results with the help of the DARI scoring mechanism. Put together, these contributions form a new path on which AI can be used to evaluate and implement it to defense plans.

To defense stakeholders, a number of policy suggestions are eminent. To begin with, in creating a sustainable preparedness, investment in AI infrastructure, such as high- performance computing, secure data pipelines, and federated intelligence networks is necessary. Second, the reforms of the doctrine should focus on the introduction of AI-aided decision-making and the maintenance of the human control in the situations with the use of force. Third, the capability to take into account the issue of cybersecurity has to be developed in line with the introduction of AI, making it resistant to the adversary attack and malicious use of AI systems. It is thus appropriate to recommend policymakers to use DARI as a strategic planning tool, capability assessment, and alliance cooperation tool.

In the future, several directions of research can be discerned. Empirical validation of UDAIM and DARI scheme, extending over field trials and bigger scale simulations, would be beneficial to its practical use. Cross-national research would even enhance DARI by considering the organizational, legal and cultural differences in military doctrine. In addition, interdisciplinary studies within the field of AI ethics, international law and defense studies are required to solve unresolved questions about autonomy, accountability, and algorithmic transparency. Lastly, UDAIM can be developed further and branded as a guideline to living in the AI age by exploring how new technologies such as edge AI, quantum computing, and bio- inspired algorithms can be used in defense systems.

To sum it up, even though there are challenges, the adoption of generative AI, effective cybersecurity, and dynamic doctrine is a paradigm shift in defense organizations. UDAIM and DARI offer both conceptual clarity and operational tools to navigate this transformation, providing a foundation for more secure, adaptive, and ethically responsible military systems in the decades to come.

X. REFERENCES

[1] J. R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, vol. 22, no. 3, pp. 365–404, 2013. DOI: 10.1080/09636412.2013.816122. Available: https://www.tandfonline.com/doi/abs/10.1080/09636412.2013.816122

[2] K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown, 2014. ISBN: 978-0-8041-6620-1. Available: https://www.penguinrandomhouse.com/books/219931/countdown-to-zero-day-by-kim-zetter/

[3] L. Floridi and M. Chiriatti, "GPT-3: Its Nature, Scope, Limits, and Consequences," *Minds & Machines*, vol. 30, pp. 681–694, Dec. 2020. DOI: 10.1007/s11023-020-09548-1. Available: https://link.springer.com/article/10.1007/s11023- 020-09548-1

[4] B. Biggio and F. Roli, "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning," *ACM Computing Surveys / arXiv preprint*, Dec. 2017/2018. Available (arXiv): https://arxiv.org/abs/1712.03141 (Also: B. Biggio and F. Roli, *Pattern Recognition and Adversarial ML* — see ACM DL.)

[5] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, "Practical Black-Box Attacks against Machine Learning," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS 2017)*, Abu Dhabi, Apr. 2017, pp. 506–519. DOI: 10.1145/3052973.3053009. Available (arXiv / preprint): https://arxiv.org/abs/1602.02697

[6] R. Chesney and D. Citron, "Deepfakes and the New Disinformation War," *Foreign Affairs,* Jan./Feb. 2019. Available: https://www.foreignaffairs.com/articles/world/2018-12- 11/deepfakes-and-new-disinformation-war
(See also: D. K. Citron & R. Chesney, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review*, vol. 107, 2019.)

[7] M. Konaev, *Tomorrow's Technology in Today's War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability*, CNA Corporation, IOP-2023-U-036583, Sep. 2023. Available (pdf): https://www.cna.org/reports/2023/10/Use- of-AI-and-Autonomous-Technologies-in-the-War-in-Ukraine.pdf

[8] K. Giles, *Russian cyber and information warfare in practice: Lessons observed from the war in Ukraine*, Chatham House Research Paper, 14 Dec. 2023. Available (pdf): https://www.chathamhouse.org/sites/default/files/2023- 12/2023-12-14-russian-cyber-info-warfare-giles.pdf

[9] E. B. Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*, Center for a New American Security (CNAS), Nov. 2017. Available (pdf): https://s3.amazonaws.com/files.cnas.org/documents/Battlefi eld-Singularity-November-2017.pdf

[10] NATO, "An Artificial Intelligence Strategy for NATO," NATO Review / NATO Publications, Oct. 2021. Available: https://www.nato.int/docu/review/articles/2021/10/25/an- artificial-intelligence-strategy-for-nato/index.html
(See also NATO press release: https://www.nato.int/cps/en/natohq/news_187934.htm)

[11] CNA, "Assessing Russian Cyber and Information Warfare in Ukraine," CNA Analyses & Reports, Nov. 2023. Available: https://www.cna.org/reports/2023/11/Assessing-Russian-Cyber-and-Information-Warfare-in-Ukraine.pdf

[12] Institute for National Security Studies (INSS), "The Iranian Cyber Threat," INSS Memo/Report, Feb. 2024 (and related INSS publications on Israeli cyber posture). Available: https://www.inss.org.il/wp-content/uploads/2024/02/Memo230_IranianCyberThreat_E NG_digital.pdf

[13] RAND Corporation, "Strategic Competition in the Age of AI: Emerging Risks and Opportunities," RAND Research Report, 2024. Available: https://www.rand.org/pubs/research_reports.html (see RAND topic page for AI: https://www.rand.org/topics/artificial-intelligence.html) (Examples of relevant RAND work: *Strategic competition in the age of AI* — https://www.rand.org/content/dam/rand/pubs/research_repor ts/RRA3295-1/RAND_RRA3295-1.pdf)

[14] S. U. Shaukat, S. Khan and S. Parkinson, "A Review on Multi-Step Attack Detection," in *IEEE Access*, vol. 13, pp. 161779-161805, 2025, doi: 10.1109/ACCESS.2025.3607497.

[15] A. AbuGhazleh, M. Almiani, B. Magableh and A. Razaque, "Intelligent Intrusion Detection Using Radial Basis Function Neural Network," *2019 Sixth International Conference on Software Defined Systems (SDS)*, Rome, Italy, 2019, pp. 200-208, doi: 10.1109/SDS.2019.8768575.

[16] Iqbal H. Sarker, CyberLearning: Effectiveness of machine learning security modeling to detect cyber-anomalies and multi-attacks, Internet of Things, Volume 14, 2021, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2021.100393.

[17] Hart, K.M., Goodman, A.B., O'Shea, R.P. (2021). Automatic Generation of Machine Learning Synthetic Data Using ROS. In: Degen, H., Ntoa, S. (eds) Artificial Intelligence in HCI. HCII 2021. Lecture Notes in Computer Science(), vol 12797. Springer, Cham. https://doi.org/10.1007/978-3-030-77772-2_21

[18] Y. Zhang, M. Li, G. Song and N. Cai, "Intelligent Decision-Making in Wargaming Environment: A Streamlined Coding Framework for Wargames," *2023 China Automation Congress (CAC)*, Chongqing, China, 2023, pp. 8503-8508, doi: 10.1109/CAC59555.2023.10450870.