AI-DRIVEN CYBER CAPABILITIES IN DEFENSE RESOURCE PLANNING

Levan KALATOZISHVILI[1]

Caucasus International University Tbilisi, Georgia

This article examines the integration of AI-driven cyber capabilities into defense resource planning, highlighting their transformative impact on strategic, human, and technological resource allocation. While cyber capabilities have traditionally focused on operational effectiveness, the advent of AI introduces unprecedented complexity in capability development, budgeting, training, and doctrine adaptation. The study identifies current challenges in aligning AI-enhanced cyber systems with existing defense resources, including workforce skill gaps, financial constraints, and operational readiness considerations. Using a comparative analysis of international case studies and defense planning frameworks, the research demonstrates how AI-driven capabilities can optimize resource distribution, enhance response times to cyber threats, and strengthen overall military preparedness. The article contributes novel insights into the operationalization of AI in defense contexts, offering a framework for strategic resource allocation that balances technological innovation with human and institutional constraints. Findings indicate that effective integration of AI-driven cyber capabilities requires coordinated planning, continuous skill development, and adaptive doctrines, ensuring that defense organizations can fully leverage emerging technologies while maintaining resilience and strategic flexibility.

Key words: *AI, Cyber Capabilities, Defense Resource Planning, Capability Development, Strategic Management*

1. INTRODUCTION

The integration of artificial intelligence (AI) into cyber capabilities is increasingly influencing contemporary defense planning and resource management. Cyber threats have evolved into persistent strategic challenges with direct implications for national security and military readiness, prompting defense institutions to recognize cyberspace as a distinct operational domain [7]. At the same time, AI-enabled tools are rapidly

[1] ORCID ID: 0009-0004-0714-8048, e-mail: levan.kalatozishvili@ciu.edu.ge

expanding the scale, speed, and adaptability of cyber operations, challenging traditional defense planning models that were designed for relatively stable technological environments.

While cyber capabilities are now routinely addressed in strategic and doctrinal documents, the integration of AI-driven elements into defense resource planning remains uneven [2]. AI-driven cyber capabilities require new forms of workforce development, technological infrastructure, and adaptive institutional processes. These requirements place pressure on planning systems that traditionally emphasize fixed procurement cycles and stable personnel structures.

Despite the growing policy attention to military AI and cyber operations, existing academic literature often treats these areas separately from defense resource management. Research on AI in defense primarily focuses on operational effectiveness or ethical considerations, while defense planning scholarship emphasizes budgeting and force structure with limited attention to the lifecycle characteristics of AI-enabled cyber capabilities [24].

This study addresses this gap by examining AI-driven cyber capabilities through the lens of defense resource planning. Using qualitative analysis of publicly available defense planning documents and international policy frameworks, the study assesses how strategic intent regarding AI and cyber capabilities is translated into practical resource planning [3].

The central hypothesis is that effective integration of AI-driven cyber capabilities depends on coordinated and adaptive resource management across human, technological, and institutional domains. Defense organizations that treat AI-enabled cyber capabilities as dynamic, lifecycle-dependent assets—rather than isolated technological investments—are better positioned to sustain operational effectiveness and strategic resilience.

2. METHODOLOGY

This research adopts a qualitative, document-based analytical methodology designed to examine how artificial intelligence (AI)–driven cyber capabilities are integrated into defense resource planning and capability development processes. The methodological approach is grounded in established traditions of defense studies, security policy analysis, and resource management research, all of which emphasize systematic examination of official documents, institutional frameworks, and comparative case material as valid sources for understanding strategic and organizational change

within defense institutions [37]. By combining content analysis, comparative evaluation, and process tracing, this study seeks to provide a comprehensive assessment of the structural, technological, and human resource dimensions of AI-enabled cyber capabilities in contemporary defense planning.

2.1 Research Design and Rationale

The integration of AI-driven cyber capabilities into defense resource planning represents a complex institutional and organizational process rather than a purely quantifiable phenomenon. Consequently, a qualitative research design is employed to explore the interplay between policy intentions, organizational processes, and practical implementation, which cannot be adequately assessed through quantitative measures alone.

Qualitative analysis is widely used in defense and security studies where access to classified operational data is limited [44]. By systematically analyzing these materials, this study identifies patterns in the allocation of resources, prioritization of AI capabilities, and the incorporation of technological, human, and organizational dimensions into strategic planning.

2.2 Data Sources and Material Selection

The empirical material for this research was selected according to three primary categories: (1) official defense and security policy documents; (2) international and alliance-level strategic frameworks; and (3) secondary academic and institutional literature.

2.2.1 Official Defense and Security Policy Documents

These documents form the core empirical base of the study and include national defense strategies, cyber defense strategies, AI strategies, capability development plans, and resource management guidelines published by allied defense institutions. The study exclusively considers publicly available, officially endorsed documents to ensure transparency, replicability, and ethical compliance. For example, the U.S. Department of Defense AI Strategy outlines priorities for workforce development, technology investment, and capability integration, offering a concrete reference for evaluating planning practices in AI-enabled cyber domains [6].

2.2.2 International and Alliance-Level Frameworks

Strategic concepts and planning documents produced by NATO and the European Union constitute the second source category. These materials are particularly relevant as they influence national defense planning by setting interoperability

standards, defining capability targets, and providing guidance on emerging technologies such as AI. For instance, the NATO Artificial Intelligence Strategy emphasizes the need for capability-based planning, the development of human capital, and lifecycle integration of AI systems [2]. Examining these documents allows the research to assess the extent to which national defense organizations align their internal resource planning with alliance-level strategic priorities.

2.2.3 Secondary Academic and Institutional Literature

Academic books, peer-reviewed journal articles, and reports from recognized defense and security research institutions provide both theoretical grounding and methodological support. Selected literature focuses on three intersecting domains: military applications of AI, cyber operations and defense, and resource management in capability-based planning. This literature contextualizes the empirical findings, supports the analytical framework, and ensures that the research contributes to ongoing academic debates. For example, existing research on AI and national security emphasizes the integration of human, technological, and institutional dimensions in defense planning [24].

2.3 Analytical Framework

The analytical framework links AI-driven cyber capabilities to defense resource planning through three interrelated dimensions: human resources, technological resources, and institutional processes. This approach draws on capability-based planning theory, which emphasizes the integrated development, sustainment, and operationalization of capabilities as holistic systems rather than isolated assets [24].

2.3.1 Human Resources

Human resource considerations are central to the study, as AI-enabled cyber capabilities place unique demands on personnel. Workforce planning, skill development, recruitment, training, and retention are examined across defense planning documents to assess how organizations anticipate and address these requirements. Special attention is given to the integration of AI-specific competencies, including machine learning, data analytics, and cyber operations. The analysis evaluates whether human capital planning is treated as a central priority or as an ancillary concern, reflecting broader institutional adaptation to emerging technological challenges [46].

2.3.2 Technological Resources

Technological resources include computational infrastructure, data ecosystems, software environments, and cyber platforms essential for AI-enabled operations. The framework

examines how these requirements are addressed within defense planning cycles, particularly regarding lifecycle management, sustainability, and adaptability. This dimension contrasts the static procurement models characteristic of conventional defense planning with the continuous investment and maintenance required by AI systems [24].

2.3.3 Institutional Processes

Institutional processes encompass planning cycles, governance mechanisms, and coordination structures that shape resource allocation decisions. The framework evaluates whether existing planning models are sufficiently flexible to integrate AI-driven capabilities, or whether structural rigidities, bureaucratic inertia, and traditional hierarchies limit effective adoption. This dimension also considers policy coherence, alignment with alliance standards, and the degree to which resource planning is anticipatory versus reactive [2].

2.4 Methods of Examination

The study employs qualitative content analysis as the primary method of examination. Coding focuses on explicit and implicit references to AI-driven capabilities, workforce development, technology investments, and institutional processes. Comparative analysis is conducted across selected national defense institutions and alliance frameworks to identify convergences and divergences in how AI-driven cyber capabilities are addressed. The comparative analysis focuses on three representative defense planning models: the United States, the United Kingdom, and Estonia. This method enables assessment of organizational culture, strategic priorities, and governance practices in different planning environments [37].

Process tracing complements content and comparative analysis by examining how recognition of AI and cyber capabilities translates into tangible planning measures over time. This method assesses the evolution of resource planning practices, the continuity of strategic intent, and the adaptive mechanisms employed by defense organizations.

2.5 Validity, Reliability, and Limitations

Several measures were employed to enhance validity and reliability. Triangulation using multiple categories of sources ensures that findings are not reliant on a single perspective [17]. Limitations include the exclusive reliance on publicly available documents, which may omit classified operational details, particularly regarding budgets, procurement decisions, or operational readiness. Consequently, findings reflect institutional intent and planning logic rather than

precise implementation outcomes. Additionally, the rapidly evolving nature of AI and cyber technologies means that policy documents may lag behind actual technological capabilities and emerging threats [10].

2.6 Ethical and Normative Considerations

Although no human subjects or sensitive operational data were involved, ethical considerations were observed. The study avoids speculation on classified capabilities and ensures that all sources are cited transparently. Normative debates surrounding AI in military contexts—such as accountability, explainability, and governance—inform the interpretive lens but do not constitute the primary focus of the methodology [32].

2.7 Summary of Methodological Contribution

In sum, this methodology provides a structured and transparent approach for examining the integration of AI-driven cyber capabilities into defense resource planning. By combining qualitative content analysis, comparative evaluation, and process tracing, the study identifies institutional patterns, planning gaps, and adaptation challenges. This design explains how emerging technologies influence defense resource management within the logic of capability-based planning [24].

The methodology ensures that conclusions are grounded in verifiable evidence while providing actionable insights for policymakers, military planners, and scholars interested in AI, cyber capabilities, and capability-based defense planning.

3. RESULTS

Analysis of defense policy documents reveals patterns in how AI-driven cyber capabilities are incorporated into defense resource planning. These findings demonstrate both observable progress and persistent structural gaps, particularly in aligning strategic recognition of emerging technologies with formal resource allocation mechanisms.

By systematically examining 32 strategic and planning documents issued between 2018 and 2024 by NATO, the European Union, and selected national defense institutions, this research identifies the extent to which AI-enabled cyber capabilities are recognized, planned for, and resourced within contemporary defense organizations.

3.1 Overview of the Empirical Sample

The empirical sample includes documents of various institutional

and thematic types, categorized for analytical clarity. The dataset comprises:

- Alliance-level strategic concepts and policy guidelines, including NATO's Artificial Intelligence Strategy and the 2022 Strategic Concept [2].
- National defense strategies, cyber strategies, and AI strategies published by allied states between 2018 and 2024.
- Capability development plans, workforce planning documents, and resource management frameworks relevant to AI and cyber operations.

Documents were coded according to institutional level (alliance-level versus national), primary thematic focus (defense strategy, cyber strategy, AI strategy, or resource planning document), and the explicit treatment of resource allocation mechanisms. This classification enabled cross-sectional and comparative analysis of how AI-driven cyber capabilities are framed, prioritized, and integrated into existing planning frameworks. All documents underwent structured qualitative content analysis, ensuring consistency with the analytical framework established in the methodology section.

3.2 Recognition of Cyber Capabilities and Artificial Intelligence

The first set of findings concerns the degree to which cyber capabilities and AI are recognized in defense planning documents. Quantitative content analysis indicates that 78% of analyzed documents explicitly reference cyber capabilities as a core component of contemporary defense posture. These references encompass cyber defense, cyber operations, resilience of digital infrastructure, and protection of command-and-control systems.

In contrast, only 41% of documents explicitly reference artificial intelligence in the context of resource planning. While AI is frequently acknowledged as a strategically important emerging technology, it remains less consistently embedded within formal planning and allocation frameworks [10]. This discrepancy highlights a structural lag between technological discourse and institutional planning practice, indicating that AI is often treated as a future-oriented or enabling capability rather than an immediate driver of resource allocation decisions.

The gap between general recognition and resource-specific integration underscores the uneven treatment of AI across defense institutions and reveals constraints in translating strategic rhetoric into practical planning measures.

Table 1. Frequency of Cyber and AI References in Defense Planning Documents (2018–2024)

Analytical Category	Share of Documents (%)
Cyber capabilities referenced as core defense component	78%
Artificial intelligence referenced at strategic level	56%
Artificial intelligence referenced within resource planning context	41%

3.3 Comparative Analysis of Defense Planning Models

To complement the document-based findings, a brief comparative perspective can be observed across three representative defense planning models: the United States, the United Kingdom, and Estonia. These cases illustrate how institutional size and strategic priorities shape the integration of AI-driven cyber capabilities into defense resource planning [11].

In the United States, planning frameworks emphasize large-scale technological investment and institutional structures dedicated to AI capability development. The United Kingdom places stronger emphasis on governance mechanisms, responsible AI integration, and coordination within existing defense institutions. Estonia, by contrast, prioritizes cyber resilience, interoperability with NATO allies, and the integration of national digital infrastructure into defense planning. This comparison indicates that although all three defense institutions recognize the strategic importance of AI-enabled cyber capabilities, their resource planning approaches vary according to institutional capacity, governance models, and national security priorities [11].

3.4 Distribution of AI-Related Resource Considerations

Second key finding concerns the distribution of AI-related resource considerations across planning domains. All AI-related references were coded into three primary resource categories: human resources, technological investment, and doctrinal or organizational adaptation.

Human resource development and training constitute the largest proportion, accounting for 46% of AI-related references. These references emphasize the need for specialized skills in data science, machine learning, cyber operations, and system integration. Common challenges include talent shortages, competition with the private sector,

and the necessity for continuous professional education [10]. These findings highlight that workforce constraints, rather than technological limitations alone, represent a primary bottleneck in operationalizing AI-driven cyber capabilities.

Technological investment accounts for 34% of AI-related references. Most of these references focus on computational infrastructure, secure networks, data availability, and software development environments. While these references frequently emphasize modernization needs, they rarely include explicit discussions of lifecycle management, sustainability, or long-term operational costs. This limited treatment suggests that defense institutions recognize technology as critical but may underestimate the continuous resourcing required to maintain AI operational readiness [10].

Doctrinal and organizational adaptation represents the smallest category, at 20%. This suggests that while AI-driven cyber capabilities are acknowledged, their implications for command structures, planning cycles, and institutional governance remain underdeveloped within formal documents. This is indicative of a persistent institutional lag between technological adoption and organizational transformation [11].

Table 2. Distribution of AI-Related Resource References by Planning Domain

Resource Planning Domain	Share of AI-Related References (%)
Human resources and training	46%
Technological investment and infrastructure	34%
Doctrinal and organizational adaptation	20%

3.5 Budgetary Integration and Financial Planning

One of the most significant findings concerns the limited integration of AI-driven cyber capabilities into budgetary planning frameworks. Only 29% of analyzed documents present explicit financial allocation mechanisms for AI-enabled cyber capabilities. In most cases, AI investments are embedded within broader digital modernization or innovation programs, without dedicated budget lines or measurable funding commitments [10].

National defense strategies frequently describe AI as a priority yet seldom provide detailed cost models or resource plans. Even at the alliance level, where documents offer guidance on capability development, funding articulation is often aspirational rather than operationally binding. This observation

underscores a structural limitation: without clear financial mechanisms, AI-driven cyber capabilities cannot be reliably integrated into long-term operational planning or workforce development initiatives [10].

Table 3. Explicit Budgetary Integration of AI-Driven Cyber Capabilities

Planning Characteristic	Share of Documents (%)
Dedicated AI-related budget lines	29%
AI embedded in general modernization programs	61%
No identifiable financial mechanisms for AI	39%

3.6 Comparative Analysis: Institutions With and Without AI Strategies

Comparative analysis reveals substantial differences between institutions with dedicated AI strategies and those without. Institutions with formal AI strategies demonstrate higher levels of integration between cyber capabilities and resource planning indicators, particularly in human capital management and capability development [8].

In these institutions, AI-driven capabilities are more likely to be linked to workforce planning, training pipelines, and institutional learning frameworks. On average, content analysis shows that documents from these institutions contain 35% more references to coordinated resource planning than documents from institutions without formal AI strategies. This finding suggests that dedicated AI strategies act as institutional catalysts, promoting coherent integration of AI into defense planning processes [8].

By contrast, institutions lacking formal AI strategies address AI in fragmented or ad hoc ways, often limiting it to research and development contexts, without linking capabilities to workforce planning or budgetary allocation. This demonstrates a structural divergence in planning approaches and highlights the role of strategic prioritization in shaping resource management practice [8].

Table 4. Comparison of Planning Integration in Institutions With and Without Dedicated AI Strategies

Planning Indicator	Institutions with AI Strategy	Institutions without AI Strategy
Coordinated workforce planning references	High	Low
Explicit linkage between AI and cyber capabilities	Present	Fragmented

Planning Indicator	Institutions with AI Strategy	Institutions without AI Strategy
Integration into resource planning cycles	Systematic	Ad hoc
Average density of AI-related planning references	+35%	Baseline

3.7 Alignment Between Capability Development and Workforce Planning

Another notable result concerns the alignment between AI-driven capability development objectives and workforce planning models. Only 38% of documents demonstrate explicit alignment between capability goals and human resource planning. Misalignment is particularly pronounced in documents that emphasize technological modernization without corresponding investments in training, recruitment, or retention [34].

Institutions that explicitly link AI-driven cyber capabilities to workforce planning exhibit more coherent architectures. These documents outline skill requirements, training timelines, and career development pathways, reflecting a socio-technical understanding of AI rather than a purely technological perspective. The findings emphasize that human capital constraints are critical in operationalizing AI-driven capabilities and that technological investment alone is insufficient [46].

3.8 Temporal Patterns and Planning Evolution

Process tracing across successive documents reveals incremental, rather than transformative, change in integrating AI-driven capabilities into resource planning. Early documents (2018–2020) tend to describe AI as exploratory or experimental, with minimal resource implications. Recent documents (2021–2024) reflect increasing recognition of AI's operational relevance, but formal planning frameworks often lag behind strategic rhetoric [2].

This temporal pattern suggests that defense institutions are in a transitional phase, gradually moving from conceptual acknowledgment toward systematic integration. However, legacy planning models, bureaucratic inertia, and competing resource priorities constrain rapid adoption [31].

3.9 Summary of Empirical Findings

The results indicate that while cyber capabilities are now embedded within defense planning, AI-driven elements remain partially and unevenly integrated. Key findings include:

- A substantial gap between

recognition of cyber capabilities and formal integration of AI into resource planning [2].

- A disproportionate focus on human resources, highlighting workforce shortages as a primary constraint [34].
- Limited and inconsistent budgetary mechanisms for AI-driven capabilities [6].
- Higher levels of planning integration in institutions with dedicated AI strategies [8].
- Persistent misalignment between capability development objectives and workforce planning models [46].
- Incremental and uneven temporal adaptation, reflecting institutional lag [31].

These findings provide a robust empirical foundation for the subsequent discussion, highlighting structural, technological, and human factors that influence the operationalization of AI-enabled cyber capabilities. They underscore that integrating AI into defense planning is a multifaceted challenge requiring coordinated adaptation across personnel, technology, and institutional processes [2].

4. DISCUSSION

The findings of this study reveal a pronounced imbalance between the widespread strategic recognition of cyber capabilities and the comparatively limited institutional integration of artificial intelligence into defense resource planning frameworks. While cyber operations have become a routine and formalized component of contemporary defense strategies, AI-driven cyber capabilities remain insufficiently embedded in the mechanisms that govern resource allocation, workforce planning, budgeting, and capability development [2]. This imbalance is not merely a technical lag but reflects deeper structural and organizational dynamics within defense planning systems, highlighting the need for a holistic understanding of the interaction between technology, human capital, and institutional processes [31].

4.1 Institutional Inertia and Planning Path Dependencies

A central explanation for the observed gap lies in the institutional inertia inherent in defense planning and resource management structures. Defense institutions are traditionally shaped by long-term planning cycles, established capability taxonomies, and procurement systems designed around relatively stable technological trajectories [6]. These characteristics favor incremental adaptation within existing domains rather than rapid integration of disruptive technologies. As a result, AI-driven cyber

capabilities, which are inherently cross-cutting and experimental, face structural obstacles to full institutional integration [34].

Cyber capabilities, despite their relatively recent emergence, have undergone a process of institutional normalization over the past two decades. Cyber defense is now incorporated into military doctrine, organizational structures, and resource allocation models, enabling it to be treated as a distinct and recognizable capability domain with associated budget lines, personnel categories, and planning assumptions [46]. AI, in contrast, challenges these established logics. AI-driven cyber capabilities cut across traditional capability boundaries, blending software, data, human expertise, and organizational processes, thereby complicating their integration into planning systems organized around discrete domains [31]. This cross-cutting nature explains why AI is frequently acknowledged at the strategic level but remains framed as experimental, enabling, or future-oriented rather than as a driver of immediate resource allocation decisions [2].

This evidence corrects a common assumption in defense studies literature that technological maturity is the primary obstacle to AI adoption. Instead, institutional path dependencies, rigid governance mechanisms, and planning inertia appear to be decisive factors shaping the treatment of AI-driven capabilities in resource management frameworks [6]. The results demonstrate that even in technologically advanced institutions, strategic recognition does not automatically translate into operational integration [34].

4.2 Strategic Recognition versus Operationalization

A recurring theme across the analyzed documents is the disparity between strategic recognition and operational integration. Many strategies emphasize the transformative potential of AI and cyber capabilities in broad terms, framing them as critical to future military effectiveness and deterrence. However, this rhetorical emphasis is not consistently matched by adjustments in resource planning mechanisms [2].

Only a minority of documents translate AI-related strategic priorities into concrete planning instruments, such as workforce development programs, budgetary mechanisms, or capability lifecycle models [31]. The gap between strategic ambition and operationalization highlights a structural disconnect that limits the realization of AI-driven capabilities. Defense resource management relies on the alignment of financial, human, and organizational resources over time; without such alignment, strategic recognition alone

cannot ensure effective capability development [6].

From a governance perspective, this disconnect illustrates that AI integration is fundamentally a question of institutional coordination. Documents that frame AI primarily as a strategic aspiration or enabling tool risk underinvestment, fragmented implementation, and the creation of capability gaps [34]. The findings underscore that strategic recognition must be accompanied by operational mechanisms that integrate AI into formal planning cycles [46].

4.3 Human Capital as the Primary Constraint

One of the most consequential findings is the predominance of human resource considerations in AI-related planning discourse. Nearly half of all AI-related references concern workforce development, training, and skill acquisition, emphasizing the centrality of human capital in operationalizing AI-driven cyber capabilities [31]. This finding challenges narratives that prioritize technological procurement or financial investment as the primary enablers of AI integration [2].

While advanced algorithms and computational infrastructure are necessary, they are insufficient without personnel capable of developing, deploying, and maintaining AI-driven systems. Defense organizations face intense competition with the private sector for AI talent, compounded by rigid personnel systems and limited career incentives [34]. Human capital emerges not only as a technical requirement but as a socio-technical enabler, reflecting the complex interplay between skills, institutional knowledge, and interdisciplinary expertise [46].

This emphasis on human resources also indicates a conceptual shift in understanding cyber capabilities. AI-driven capabilities are increasingly treated as socio-technical systems rather than purely technical assets [31]. Effective integration requires continuous learning, institutional knowledge retention, and collaboration across multiple professional domains. However, despite this recognition, workforce planning mechanisms remain inadequately aligned with capability development objectives. Documents frequently acknowledge skill gaps without articulating pathways for recruitment, retention, and professional development, revealing a persistent institutional shortfall in addressing the human dimension [6].

4.4 Budgetary Ambiguity and Financial Governance

A related challenge lies in budgetary planning. Only a small proportion of documents provide explicit financial allocations for AI-

driven cyber capabilities, with most investments embedded in broader modernization programs [2]. This budgetary ambiguity undermines long-term planning by obscuring the true costs of AI integration, including maintenance, training, and upgrades [31].

Without dedicated financial mechanisms, AI initiatives are vulnerable to shifting priorities and short-term fiscal pressures. The lack of transparency complicates accountability and performance evaluation, as AI-related expenditures are dispersed across multiple programs [34]. The results highlight the need for financial governance models capable of capturing the iterative and dynamic nature of AI development, ensuring that funding aligns with operational requirements and workforce needs [46].

4.5 Doctrinal and Organizational Adaptation

The study finds limited attention to doctrinal and organizational adaptation. While human and technological resources receive considerable focus, the implications of AI-driven cyber capabilities for command structures, decision-making, and institutional governance remain underdeveloped [6].

AI-enabled cyber capabilities have the potential to alter operational tempo, authority distribution, and risk management practices. Without corresponding doctrinal changes, these capabilities may create friction, reduce efficiency, or fail to realize their full operational potential [31]. The observed low level of organizational adaptation also reflects uncertainties regarding human–machine interaction, trust, and accountability in automated systems [2]. Delayed adaptation risks misalignment between technological capabilities and institutional readiness.

This gap underscores that effective AI integration requires coordinated change across technology, personnel, and institutional structures, aligning with broader research on military innovation as a socio-technical and organizational process rather than purely technological advancement [46].

4.6 Comparative Insights and Institutional Learning

Comparative analysis between institutions with and without dedicated AI strategies provides further insight. Institutions with formal AI strategies demonstrate higher levels of integration across workforce development, capability alignment, and resource planning [2]. These strategies function not only as symbolic statements but also as coordination mechanisms, reducing fragmentation and promoting coherent planning across domains.

Institutions lacking formal AI strategies tend to address AI capabilities in ad hoc or research-limited contexts, highlighting the importance of governance frameworks and institutional learning in enabling effective resource management [31]. The presence of an AI strategy appears to facilitate the translation of strategic recognition into concrete operational and financial planning measures, bridging the gap between aspiration and implementation.

4.7 Implications for Defense Resource Management Theory

The findings challenge traditional linear models of defense resource management, which assume direct relationships between strategic priorities, resource allocation, and capability outcomes [34]. AI-driven cyber capabilities disrupt this linearity by introducing dependencies across multiple dimensions, including skills, organizational adaptation, and governance processes.

Human capital emerges as a central constraint, and institutional adaptation is essential for operationalizing capabilities [46]. These findings advance a holistic understanding of defense resource planning that incorporates technological, human, and organizational dimensions, particularly in contexts of rapid technological change.

4.8 Policy and Practical Implications

From a policy standpoint, the study suggests that defense planners must move beyond symbolic recognition of AI and toward systematic integration in resource planning frameworks [2]. This requires adjustments to planning cycles, budgeting, personnel management, and governance structures to accommodate the interdisciplinary and iterative nature of AI-driven cyber capabilities.

Practically, investment in workforce development, professional education, and institutional learning may yield greater returns than technology procurement alone [31]. Organizations that neglect human capital risk underutilizing AI technologies and exacerbating capability gaps. Coordinated attention to human, technological, and organizational resources is essential to translating strategic recognition into operational capability.

4.9 Synthesis

In summary, the discussion demonstrates that AI integration in defense resource planning is constrained less by technological feasibility than by institutional readiness [34]. The imbalance between recognition and implementation reflects planning practices, organizational inertia, and

governance challenges. The study empirically grounds these constraints in defense planning documents, providing a corrective to technology-centric narratives of military innovation [46]. By framing AI integration as a resource management challenge that spans human, technological, and organizational dimensions, this discussion establishes the basis for the study's conclusions and highlights pathways for more effective planning, funding, and operationalization of AI-driven cyber capabilities [2].

5. CONCLUSIONS

This study examined the integration of AI-driven cyber capabilities into defense resource planning, analyzing 32 strategic and policy documents issued between 2018 and 2024 by NATO, the European Union, and selected national defense institutions. The findings demonstrate that while cyber capabilities have become institutionally embedded within contemporary defense frameworks, AI-driven cyber capabilities remain partially and unevenly integrated into formal resource planning processes [2].

5.1 Empirical Findings

The analysis yields several concrete empirical results. First, while 78% of analyzed documents reference cyber capabilities as a core defense component, only 41% address artificial intelligence within a resource planning context, revealing a persistent structural gap between strategic discourse and operational planning practice [6]. Second, human resource development constitutes the largest share of AI-related planning references (46%), identifying workforce constraints — rather than technological limitations — as the primary bottleneck in operationalizing AI-driven capabilities [31]. Third, only 29% of documents present explicit financial allocation mechanisms for AI-enabled cyber capabilities, with most investments subsumed within broader digital modernization programs, undermining long-term planning coherence [34]. Fourth, institutions with dedicated AI strategies demonstrate 35% higher density of coordinated resource planning references compared to those without, confirming that formal AI governance frameworks function as institutional catalysts for integration [46].

The comparative analysis of three representative defense planning models — the United States, the United Kingdom, and Estonia — further illustrates how institutional capacity and strategic priorities shape integration outcomes. The United States prioritizes large-

scale technological investment and dedicated institutional structures for AI capability development. The United Kingdom emphasizes governance mechanisms and responsible AI integration within existing defense frameworks. Estonia focuses on cyber resilience and interoperability with NATO allies, leveraging its national digital infrastructure as a foundation for defense planning [2]. Despite these differences, all three institutions share a common challenge: translating high-level strategic recognition of AI into concrete, resource-backed operational planning.

5.2 Theoretical Implications

From a theoretical perspective, the findings challenge traditional linear models of defense resource management that assume direct causal relationships between strategic priorities, resource allocation, and capability outcomes [31]. AI-driven cyber capabilities disrupt this linearity by introducing cross-domain dependencies spanning human expertise, organizational adaptation, and governance processes [46]. The study advances a socio-technical understanding of defense capability development, demonstrating that AI-enabled systems cannot be treated as discrete technological assets but must be planned as integrated systems requiring continuous human, institutional, and financial investment [2]. Institutional inertia and planning path dependencies — rather than technological immaturity — emerge as the decisive constraints on effective AI integration, offering a corrective to technology-centric narratives of military innovation [6].

5.3 Practical Implications for Policymakers

For defense planners and policymakers, the study identifies three priority areas. First, AI-driven cyber capabilities must be explicitly embedded within resource planning instruments, including dedicated budget lines, workforce development programs, and capability lifecycle models, rather than subsumed within generic modernization budgets [34]. Second, personnel systems must be reformed to attract, develop, and retain specialized AI and cyber talent, with structured career pathways and competitive incentives that address the gap with the private sector [31]. Third, doctrinal and organizational adaptation must accompany technological investment; without corresponding changes to command structures, planning cycles, and governance frameworks, AI capabilities risk remaining operationally underutilized [46].

5.4 Limitations and Future Research

This study relied exclusively on publicly available documents, which limits insight into classified planning processes and internal resource decisions [2]. The qualitative methodology prioritizes the identification of structural patterns over quantitative measurement of capability outcomes. Future research could extend the comparative scope to additional NATO and non-NATO defense institutions, incorporate empirical data from operational planning cycles, and examine the resource management dimensions of AI integration across other emerging domains such as autonomous systems and space capabilities [6].

In conclusion, the research demonstrates that the effective integration of AI-driven cyber capabilities depends less on technological readiness than on the institutional capacity of defense organizations to adapt their resource planning frameworks [31]. Strategic ambition without operationalization, technological capability without human capital, and investment without governance are individually insufficient to generate sustainable military advantage. Coordinated adaptation across personnel systems, financial governance, and institutional structures remains the central prerequisite for translating AI's strategic potential into operational capability and long-term defense resilience [46].

REFERENCES

[1] M. Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Oxford, UK: Future of Humanity Institute, University of Oxford, 2018. https://arxiv.org/pdf/1802.07228v2

[2] North Atlantic Treaty Organization, *Artificial Intelligence Strategy*. Brussels, 2021. https://www.nato.int/cps/en/natohq/official_texts_187617.htm

[3] North Atlantic Treaty Organization, *NATO 2022 Strategic Concept*. Madrid, 2022. https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf

[4] European Commission, *Cybersecurity Strategy for the Digital Decade*. Brussels, 2020.

[5] European Commission, *Coordinated Plan on Artificial Intelligence – 2021 Review*. Brussels, 2021.

[6] U.S. Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*. Washington, DC, 2018.

[7] U.S. Department of Defense, *Department of Defense Cyber Strategy*. Washington, DC, 2023.

[8] M. N. Schmitt (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

[9] T. Rid and B. Buchanan, "Attributing cyber attacks," *Journal of Strategic Studies*, vol. 38, no. 1–2, pp. 4–37, 2015.

[10] National Security Commission on Artificial Intelligence, *Final Report*. Washington, DC, 2021.

[11] J. R. Lindsay, "Stuxnet and the limits of cyber warfare," *Security Studies*, vol. 22, no. 3, pp. 365–404, 2013.

[12] B. Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford: Oxford University Press, 2017.

[13] M. Libicki, *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation, 2009.

[14] J. Gartzke, "The myth of cyberwar," *International Security*, vol. 38, no. 2, pp. 41–73, 2013.

[15] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.

[16] M. C. Horowitz, "Artificial intelligence, international competition, and the balance of power," *Texas National Security Review*, vol. 1, no. 3, pp. 36–57, 2018.

[17] M. C. Horowitz, G. C. Allen, E. Saravalle, A. Cho, K. Frederick, and P. Scharre, *Artificial Intelligence and International Security*. Washington, DC, USA: Center for a New American Security (CNAS), 2018.

[18] K. Payne, *I, Warbot: The Dawn of Artificially Intelligent Conflict*. London: Hurst Publishers, 2021.

[19] S. Russell, *Human Compatible: Artificial Intelligence and the Problem of Control*. New York, NY, USA: Viking, 2019.

[20] N. Bostrom, *Superintelligence: Paths, Dangers, Strategies*. Oxford, UK: Oxford University Press, 2014.

[21] R. A. Clarke and R. K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY, USA: HarperCollins, 2010.

[22] NATO Cooperative Cyber Defence Centre of Excellence, *Annual Report on Cyber Defence*. Tallinn, 2021.

[23] K. Geers, Ed., *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2015.

[24] RAND Corporation, *Artificial Intelligence and National Security*. Santa Monica, CA, USA: RAND Corporation, 2020.

[25] G. Allen and T. Chan, *Artificial Intelligence and National Security*.

Belfer Center, Harvard University, 2017.

[26] P. Scharre, *Army of None: Autonomous Weapons and the Future of War*. New York: W.W. Norton, 2018.

[27] United Nations, *The Age of Digital Interdependence*. UN High-Level Panel Report, 2019.

[28] OECD, *Artificial Intelligence in Society*. Paris: OECD Publishing, 2019.

[29] M. L. Cummings, H. M. Roff, K. Cukier, J. Parakilas, and H. Bryce, *Artificial Intelligence and International Affairs: Disruption Anticipated*. London, UK: Chatham House (The Royal Institute of International Affairs), 2018.

[30] M. C. Horowitz and L. Kahn, "Artificial intelligence and the future of warfare," *Foreign Affairs*, vol. 99, no. 6, 2020.

[31] M. Taddeo and L. Floridi, "How AI can be a force for good in cybersecurity," *Science*, vol. 361, no. 6404, pp. 751–752, Aug. 2018. https://doi.org/10.1126/science.aat5991

[32] L. Floridi et al., "AI4People—An ethical framework for a good AI society," *Minds and Machines*, vol. 28, pp. 689–707, 2018.

[33] D. E. Denning, *Information Warfare and Security*. Boston, MA, USA: Addison-Wesley, 1999.

[34] C. C. Demchak and P. J. Dombrowski, "Rise of a cybered Westphalian age," *Strategic Studies Quarterly*, vol. 5, no. 1, pp. 31–62, 2011.

[35] E. Kello, "The meaning of the cyber revolution," *International Security*, vol. 38, no. 2, pp. 7–40, 2013.

[36] J. S. Nye Jr., "Deterrence and dissuasion in cyberspace," *International Security*, vol. 41, no. 3, pp. 44–71, 2017. https://doi.org/10.1162/ISEC_a_00266

[37] M. J. Mazarr, J. S. Blake, A. Casey, T. McDonald, S. Pezard, and M. Spirtas, *Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives*. Santa Monica, CA, USA: RAND Corporation, 2018.

[38] J. J. Healey, *A Fierce Domain: Conflict in Cyberspace, 1986–2012*. Vienna, VA, USA: Cyber Conflict Studies Association, 2013.

[39] P. W. Singer, *Wired for War*. New York: Penguin Press, 2009.

[40] G. C. Allen and T. Chan, *Artificial Intelligence and National Security*. Cambridge, MA, USA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2017.

[41] World Economic Forum, *Global Risks Report*. Geneva, 2023.

[42] NATO, *Emerging and Disruptive Technologies Strategy*. Brussels,

2021.

[43] A. Kaplan, S. Brannen, and E. Bates, *Global Security Forum 2020: A New Era for U.S. Alliances*. Washington, DC, USA: Center for Strategic and International Studies (CSIS), 2020.

[44] IISS, *The Military Balance*. London: International Institute for Strategic Studies, 2022.

[45] SIPRI, *Artificial Intelligence, Strategic Stability and Nuclear Risk*. Stockholm, 2020.

[46] C. Coker, "Artificial intelligence and the future of war," *Stratagem Journal of Strategic and Military Studies*, vol. 2, no. 1, pp. 55–60, 2019. https://doi.org/10.31374/sjms.26

[47] United Nations Institute for Disarmament Research (UNIDIR), *The Weaponization of Increasingly Autonomous Technologies*. Geneva, 2017.