IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 February 2024, accepted 8 March 2024, date of publication 18 March 2024, date of current version 2 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3378735

TOPICAL REVIEW

Harnessing ICT-Enabled Warfare: A Comprehensive Review on South Korea's Military Meta Power

SANG JIN OH[1], (Member, IEEE), SANG KEUN CHO[2], AND YONGSEOK SEO[1]

[1]Moon Soul Graduate School of Future Strategy, Korea Advanced Institute of Science and Technology (KAIST), Yuseong-gu, Daejeon 34141, Republic of Korea
[2]Korea Advanced Institute of Science and Technology (KAIST), Yuseong-gu, Daejeon 34141, Republic of Korea

Corresponding author: Yongseok Seo (manoa@kaist.ac.kr)

ABSTRACT Major countries around the world are leveraging information and communications technology (ICT), such as artificial intelligence, big data, cloud computing and cybersecurity, to strengthen their militaries. These technological advancements are driving the changes in weapon systems, strategies, and tactics. In 2021, the South Korean Ministry of National Defense introduced the concept of ''military meta power'' to describe the power generated in the cognitive military domain utilizing ICT. This concept is significant in that it differentiates between cognitive and physical military power, emphasizing the importance of the cognition-based power in future warfare. Additionally, the concept consolidates various cognitive military capabilities, including AI capability, cyber capability, space capability, and C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance), into a unified ICT-generated power. This study aims to contribute to the literature on ''military meta power'' by providing a comprehensive overview of its characteristics, composition, and attributes. To achieve this objective, the research begins with an exploration of the philosophical insights on technology related to ICT, followed by a comprehensive review of the perspectives of existing academic papers. Finally, this study provides an in-depth analysis of various military strategies.

INDEX TERMS Military meta power, the extension theory of technology, military cognitive capability, ICT, AI, data.

I. INTRODUCTION

In the realm of modern warfare, major nations are rapidly advancing their military capabilities by leveraging sophisticated information and communications technology (ICT), including artificial intelligence (AI), big data, cloud computing, cybersecurity, and advanced networks [1], [2], [3], [4], [5]. This is leading to the automation and unmanned operation of weapon systems, as well as profound changes in military strategies and tactics [6], [7], [8], [9], [10], [11]. This paper initiates its exploration by addressing a fundamental question: how can military power generated by ICT be precisely defined? Given the transformative nature of these technologies and their significant impact on military power [12], defining this phenomenon is important.

In this context, we focus on the 'Defense Vision 2050' published by the South Korean Ministry of National Defense (MND) in November 2021. The ministry presented a new concept of 'military meta power' to describe military power generated in the cognitive domain based on ICT [13]. In parallel, the ministry named traditional physical military power as 'military hard power [13].' The South Korean ministry's separation 'ICT-driven military power in the cognitive domain' from 'traditional physical military power' highlights the distinct nature of these two types of power. The differentiation aligns with the ministry's effort to identify the characteristics of emerging military power based on ICT.

Making a distinction between 'power in the cognitive domain' and 'power in the physical domain' stems from the philosophical exploration of the relationship between humans and technology, as evident in 'the extension theory of technology [14], [15], [16], [17], [18].' Advocated by scholars like Ernst Kapp and Marshall McLuhan, this theory proposes that tools and machines extend and amplify human physical and cognitive capabilities [14], [15], [17]. This concept becomes intuitively apparent when we consider examples: basic tools

The associate editor coordinating the review of this manuscript and approving it for publication was Paulo Mendes.

such as hammers enhance our physical abilities, whereas advanced instruments like microscopes and computers augment our sensory and cognitive capacities [16]. Notably, McLuhan argues that electric technology externally enhances human cognitive functions [17], forming a theoretical foundation for this study, which investigates the implications of ICT-enabled warfare on military cognitive capabilities.

In the cognitive domain, numerous studies have been conducted on ICT-based military capabilities up to this point. These studies have mainly focused on AI capability [8], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], cyber capability [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], space capability [9], [36], [41], [42], [43], and 'command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) [44], [45], [46], [47].' These investigations have undoubtedly yielded valuable insights. However, a tendency to analyze the military applications narrowly within these isolated areas often overlooks the broader impacts of these technologies on military operations, which are essential for comprehending the full facets of these military capabilities.

Furthermore, some studies have distinguished AI from other ICT and emphasized the differences [27], [48]. This perspective overlooks the essential interconnectedness of these technologies in practice. AI isn't simply a separate entity; it relies heavily on other ICT components like cloud computing, communications networks, and the Internet of Things (IoT) to function effectively. This is particularly the case for the military, which requires real-time information sharing and analysis of data generated on a wide range of battlefields. This interconnectedness of ICT is crucial for the effective real-time operation of AI in military contexts.

Recognizing the interdependent and complementary nature of these ICT components is central to our research. By adopting a holistic perspective, we aim to delve into the intricate cognitive aspects of ICT-based military capabilities. This approach prioritizes not just understanding individual technologies in isolation, but appreciating how their convergence enhances military cognitive functions. Such an understanding is vital for a complete appreciation of the cognitive dynamics at play in modern military capabilities.

In the context of ICT, this study reviews and synthesizes the various academic research and military strategies, and analyzes the various military capabilities associated with ICT to define and explore the concept of the newly emerging military power. Through these efforts, we aim to develop a comprehensive framework for understanding the cognitive aspects of ICT-based military power, offering valuable insights for both military policy makers and scholars.

II. RESERCH FRAME

This study aims to provide a comprehensive framework for understanding the concept of 'military meta power,' a new type of military power introduced by the South Korean MND. The South Korean ministry introduced the concept of military meta power in its 'Defense Vision 2050,' which defines it as military power generated by ICT. Military meta power is distinct from physical military power (military hard power), as described below [13].

'Military meta power' is the emerging cognitive force in the military, powered by the rapid adoption of advanced technologies such as AI, big data, and hyper-connected networks. It represents an expanding sphere of influence that transcends traditional constraints of time and space, enabled by real-time data exchange and intelligent analysis.

'Military hard power' embodies the tangible force of the military, characterized by the destructive capabilities, precision, and durability. This includes the collective strength of weapon systems, equipment, supplies, and personnel.

The South Korean MND's definition of cognitive military power based on ICT has various implications, potentially reshaping decision-making processes and blurring traditional battlefield boundaries. To delve into these implications, this study reviews relevant philosophical insights, existing academic research, and various military strategies. It aims to elucidate the composition, structure, and characteristics of the emerging military power driven by ICT.

This study explores the concept of 'military meta power' through a four-stage approach. First, it investigates 'the technology extension theory,' which posits that technology extends and amplifies human capabilities in both domains: 'physical through mechanical principles' and 'cognitive through electronic ones' [14], [16], [17]. This foundational principle provides the philosophical framework for differentiating between physical and cognitive military power, forming the basis for a deeper understanding of their roles in future warfare.

Second, this study reviews existing academic research on the various military capabilities developed through the application of ICT. Through this review, it was confirmed that academic research is being conducted with a tendency to focus on four key areas: AI capability, cyber capability, space capability, and C4ISR. These studies provide valuable insights into the meaning of ICT-enabled military capabilities in each area.

Third, this study takes a comprehensive approach to examine ICT-based military power, extending beyond the boundaries of existing academic research. It introduces a novel framework for military power composition that integrates all key ICT-enabled military capabilities. To achieve this, we meticulously examined a selection of publicly available military strategies, ultimately focusing on 14 strategies released by the U.S. military [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62]. Our choice of U.S. strategies "is based on three key factors. (1) The U.S. military has publicly released a rich and diverse set of ICT-related strategies across various fields, offering a comprehensive foundation for this analysis. (2) By focusing on strategies from a single entity, the U.S. military, we ensure greater internal consistency and coherence in the policies examined. (3) It is noteworthy that nations tend to share similar approaches and global technological standards when employing ICT for

TABLE 1. Examined U.S. military strategic documents related to ICT.

	Documents	Publication Year
1	Summary of the 2018 Department of Defense (DoD) Artificial Intelligence Strategy	2018
2	US DoD Responsible Artificial Intelligence Strategy and Implementation Pathway	June 2022
3	Summary of 2023 Cyber Strategy of DoD	2023
4	DoD Cyber Workforce Strategy 2023 - 2027	Mar. 2023
5	DoD Zero Trust Strategy	Nov. 2022
6	DoD Identity, Credential, and Access Management (ICAM) Strategy	Mar. 2020
7	Defense Space Strategy - Summary	June 2020
8	DoD Digital Modernization Strategy	July 2019
9	DoD C3 Modernization Strategy	Sep. 2020
10	DoD Cloud Strategy	Dec. 2018
11	US Army Cloud Plan	Oct. 2022
12	DoD Software Modernization Strategy	Feb. 2022
13	DoD Electromagnetic Spectrum Superiority Strategy	Oct. 2020
14	DoD Data Strategy	Sep. 2020

military purposes. Therefore, the strategies of the U.S. military serve as a valuable reference point with broader global relevance. The strategies analyzed are presented in Table 1.

To unveil the composition of ICT-based cognitive military power, we delved into U.S. military strategies through the prism of military data life cycle – the processes of data generation, transmission, processing, and interpretation. By scrutinizing how these data processes interact within these strategies, we demonstrated that seemingly disparate cognitive capabilities are intricately interconnected, forming a singular, coherently linked structure. This revelation underpins our proposition: ICT-based military power is not a mosaic of distinct parts, but rather a unified force.

Fourth, the South Korean military proposed the concept of 'military meta power' as the embodiment of ICT-driven capabilities, and identified four attributes of this power: interaction, integration, analytics, and agility. This study synthesizes the South Korean military's framework, academic research, and various military strategies to provide specific delineations of these attributes in the context of the cognitive military power.

III. THE EXTENSION THEORY OF TECHNOLOGY

The relationship between humans and technology has been a subject of philosophical inquiry for centuries. The extension theory of technology, a prominent school of thought in technology philosophy, argues that technology extends human capabilities [14], [18]. The extension theory posits that tools and machines extend the capabilities of the human body and mind outward [15]. This argument provides an intuitive logic in the context of "hammers extend human arm capabilities, microscopes extend human eye capabilities, and computers extend human brain capabilities [16]." This thesis provides important insights into the exploration of how technology, including ICT, affects military power.

In particular, Marshall McLuhan's view that "electric technology extends and enhances human cognitive function after the emergence of electric technology [17]" is the main theoretical basis of this paper. In this study, we examined military cognitive capabilities that are formed by extending human cognitive capabilities using electric technology, namely ICT.

The idea that technology is an extension of the human body originated with Aristotle [14]. Aristotle argued that "the body is our natural tool [63]." Since then, the tools that humans use have expanded from naturally-made to human-made. In 1870, Ralph Waldo Emerson proposed that human body serves as a source that stimulates technological progress. He argued that "the human body is the magazine of inventions, the patent-office, where are the models from which every hint was taken. All the tools and engines on earth are only extensions of its limbs and senses [64]." Emerson's perspective highlights the human body as the origin and inspiration for human inventions.

Building upon this foundational concept, German philosopher Ernst Kapp, in 1877, offered a profound interpretation. He proposed that not just simple artefacts, but even complex technologies can be understood as "projections" of human organs [15]. This theory of "projection," defined as an "externalization of an interior," positions human organs as the archetypes for artificial tools and instruments [18]. Kapp conceptualized the human organism as the "Original Form [15]," akin to Plato's views, and argued that all technological artifacts are essentially extensions of this original form. His work advanced our understanding of the human-technology relationship. He contended that humans "project" their organs into external forms, which in turn, amplify and reinforce bodily functions [15]. This concept is exemplified in how tools like hammers, bows, catapults, automobiles, airplanes, and rockets not only extend but also enhance human physical capabilities.

Marshall McLuhan, one of key figures in the technological expansion theory, built upon Kapp's foundational ideas. With the emergence of ICT, McLuhan shifted the focus to electric media. He posited that 'During the mechanical ages we had extended our bodies in space. Today, after more than a century of electric technology, we have extended our central nervous system itself in a global embrace, abolishing time and space as far as our planet is concerned [17].' McLuhan's contribution was pivotal as he transitioned from Kapp's attention on 'the bodily function' to a focus on 'the cognitive function.'

He argued that the cognitive functions of the central nervous system, which control media like sight and hearing, cannot be adequately explained by mechanical principles alone [17]. Instead, McLuhan viewed electric media as a new tool that extends the information processing capabilities of the human central nervous system. He famously described humans in the electric age as organisms that "wear their brains outside their skulls and their nerves outside their

TABLE 2. Research frame.

Stage	RESEARCH SUBJECTS	Research Focus and Approach
1	Academic literature related to the Extension Theory of Technology	Based on a philosophical approach that differentiates technological impacts on cognitive and physical domains, we recognize ICT's impact on cognitive military capabilities
2	Academic literature and 14 U.S. military strategies related to ICT	Classifying ICT-enabled military cognitive capabilities, and summarizing their characteristics.
3	14 U.S. military strategies related to ICT	By analyzing the U.S. military strategies according to the military data life cycle (generation, transmission, processing, and interpretation), we confirm that military cognitive capabilities are interlinked and operate in a coordinated manner.
4	South Korean 'Defense Vision 2050', Academic literature, and 14 U.S. military strategies, related to ICT	As a holistic structure, we examine ICT-enabled cognitive military power (military meta power) and specifically identify it's four attributes (interaction, integration, analytics, and agility).

hides [17]," highlighting the profound impact of electric technology on human cognition.

This theoretical trajectory from Kapp to McLuhan provides a significant foundation for our study, particularly in understanding how technologies extends and enhances not just physical, but also cognitive military capabilities. In the context of ICT-enabled military capabilities, McLuhan's perspective resonates with the way advanced algorithms, data processing machines, and interconnected networks serve as cognitive enhancements, augmenting and amplifying the ability to gather, process, and utilize information for improved military operations.

Our study places particular emphasis on Marshall McLuhan's assertion that the emergence of electric technology significantly enhances and extends human cognitive functions. McLuhan's pioneering idea is a central concept in our investigation of military cognitive capabilities.

IV. TECHNOLOGY EXTENSION AND MILITARY COGNITIVE CAPABILITIES

Before delving into the examination of military cognitive capabilities, it's necessary to establish a foundation by considering their origin: human cognitive functions. Cognitive psychologist Kim M. Kiely succinctly defines these functions as "mental processes involved in acquiring knowledge, manipulating information, and reasoning, encompassing domains like perception, memory, learning, attention, decision-making, and language abilities [65]."

The human brain, a marvel of complexity, governs an orchestra of functions and reasoning processes throughout the body. From thought and memory to emotions, motor skills, and sensory perception (vision, touch, etc.), it acts as the central command, processing and interpreting electrical and chemical signals through a vast network of nerves. Linked to this intricate system is the nervous system, consisting of the brain, spinal cord, nerves, and sensory organs – our organic interface with the world, enabling us to perceive, learn, and make judgments.

It is within this framework that we explore military cognitive capabilities, which result from projecting and augmenting human cognitive functions into the national defense sector through advanced ICT.

A. MILITARY COGNITIVE CAPABILITIES

In delineating military cognitive capabilities, our study primarily reviewed the 14 U.S. military strategic documents and academic papers related to ICT, as outlined in the research frame (section II). We summarized and categorized these strategic documents (Appendix A) and systematically reviewed academic papers (Appendix B) into cohesive conceptual categories, fostering a structured understanding of different military cognitive capabilities. As shown in Table 3, this analysis yielded the identification of four primary capabilities, each representing a crucial aspect of ICT's role in military operations: AI capability, cyber capability, space capability, and C4ISR. These categories not only encompass specific strategies but also, importantly, resonate with current academic discourse in military technology.

This categorization serves as a valuable starting point for further research in this study. This study examines these military capabilities, drawing insights from extensive academic research to synthesize and elaborate on their characteristics. We posit that AI capability, cyber capability, space capability, and C4ISR are integral to the core pillars of ICT-based military capabilities, each contributing distinctively to the modernization and efficacy of military operations.

1) AI CAPABILITY

The foundational work of American neurosurgeon Warren McCulloch and logician Walter Pitts in 1947, which aimed to replicate brain neural networks in computational models, marked the inception of AI [66]. Since then, AI's trajectory has been punctuated by periods of progress and hurdles [67], ultimately culminating in its present status as a transformative force across diverse areas, including the military. The evolution of AI has been propelled by three key factors: the

TABLE 3. Classification of military capabilities based on U.S. military strategies.

U.S. Strategic Documents	Military Capabilities
• Summary of the 2018 DoD Artificial Intelligence Strategy • US DoD Responsible Artificial Intelligence Strategy and Implementation Pathway	AI Capability
• Summary of 2023 Cyber Strategy of DoD • DoD Cyber Workforce Strategy 2023 – 2027 • DoD Zero Trust Strategy • DoD Identity, Credential, and Access Management (ICAM) Strategy	Cyber Capability
• Defense Space Strategy – Summary	Space Capability
• DoD Digital Modernization Strategy • DoD C3 Modernization Strategy • DoD Cloud Strategy • US Army Cloud Plan • DoD Software Modernization Strategy • DoD Electromagnetic Spectrum Superiority Strategy • DoD Data Strategy	C4ISR

availability of big data, advancements in machine learning approaches and algorithms, and significant increases in computing power [4]. In the military context, AI is now widely acknowledged as a "game changer [68]."

Within the military sphere, AI transcends its role as a mere weapon system and acts as an ultimate enabler [19], amplifying the capabilities of existing armaments. On a tactical level, AI automates and refines the functions of various weapon platforms, bolstering the efficiency and precision of military operations [8], [29]. Prime examples include the Royal Wingman [69], an unmanned combat air vehicle designed to cooperate with manned aircraft, and the Sea Hunter [70], autonomous anti-submarine vessel. Additionally, sophisticated swarming weapon systems orchestrate collective action among multiple drones [71], [72], [73].

Strategically, AI serves as a decision-support system for military commanders, synthesizing and interpreting data from disparate sources to deliver comprehensive situational awareness [6], [8], [28], [74]. Its signal processing prowess encompasses imagery analysis, radio frequency interpretation, and acoustic intelligence, contributing vital insights for operational decision-making. The sheer breadth of AI applications, from multilingual communication and terrain analysis to 3D modeling, substantially enhances the military's information processing and interpretation capabilities, laying the foundation for more informed and adaptable strategic planning [75], [76], [77]. The continuous integration of AI into command and control systems further underscores its growing importance in minimizing operational risks and bolstering military strategic planning and execution [78].

2) CYBER CAPABILITY

Warfare has transcended the familiar physical realms of land and air, venturing into the intricate and artificial domain of cyberspace [30], [79], [80]. This new battlefield dimension is characterized by its artificial construct and inherent complexity [34], [81]. As defined by the U.S. military's strategic command, cyberspace is "a global domain within the information environment, consisting of an interconnected network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, embedded processors, and controllers [82]."

In cyberspace, the rapid processing of data at electronic speeds underscores its critical time-sensitive nature, as emphasized by Rain Ottis and Peeter Lorents [30]. The speed and scope of cyber operations were vividly demonstrated in 2003 by the SQL Slammer worm, which affected over 750,000 systems worldwide in a span of minutes [83].

Cyber warfare has evolved into a key strategic area in modern military tactics, targeting a nation's critical information infrastructure, and psychological resilience. This form of warfare manifests in various tactics such as sabotage aimed at disrupting infrastructure, espionage for acquiring confidential information, and subversion to create societal unrest [31]. These cyber-attacks are carried out by both state-sponsored and independent entities for political motives or as part of hybrid warfare strategies, posing threats not only during active conflicts but also in peacetime [84].

The increasing dependence on digital systems in military and civilian sectors has led to "paradoxically increasing digital vulnerability [85]," highlighting escalating challenges in maintaining security and integrity within the expanding cyber landscape. This aspect of modern warfare necessitates ongoing research and development in cybersecurity measures to safeguard against evolving threats and maintain strategic advantage in the digital era.

3) SPACE CAPABILITY

Beyond Earth's atmosphere, space capabilities play a crucial role in modern military operations, encompassing functions like surveillance, reconnaissance, information gathering, navigation support, and communication. Advanced satellite technologies serve as force multipliers, amplifying the effectiveness of diverse military assets across domains, from ground forces and naval fleets to aircraft and missile systems [86].

A prime example of this transformative impact is the Global Positioning System (GPS), developed by the United States in the 1970s. GPS revolutionized military operations by providing near-instantaneous and precise positioning, navigation, and timing (PNT) information, enabling seamless coordination across various domains. Similarly, military communication satellites, a vital cog in the C4ISR system, ensure secure and comprehensive communication networks crucial for global operations [87].

Furthermore, technological advancements in satellite-based optical and radio detection have dramatically enhanced intelligence gathering capabilities, both in volume and quality. Earth observation satellites are indispensable for strategic military surveillance, enabling close monitoring of enemy activity and nuclear facilities [87]. Beyond weather forecasting, meteorological satellites also contribute to military resource management, logistics, and operational planning, showcasing their versatility for military planning purposes [88].

Recognizing the pivotal role of outer space in securing strategic advantage, achieving space superiority has become a focal point in contemporary defense strategies, both during peacetime and in times of heightened military tension. This underscores the evolution of space technology from a supporting component to an essential element of modern military capabilities and strategic planning.

4) C4ISR

C4ISR plays a fundamental role in modern military operations, empowering commanders with enhanced situational awareness and collapsing the response time between threat detection and engagement [47]. This integrated system acts as the battlefield's central nervous system [89], facilitating seamless communication and coordinated action across diverse military units, ensuring self-synchronization and decisive operations [90].

C4ISR has been closely tied to the development of network-centric warfare (NCW), a strategic concept that seeks to efficiently utilize battlefield information by leveraging advanced ICT [45], [91], [92], [93], [94]. It has undergone continuous evolution with a singular focus: achieving information superiority in the battlefield. Its effectiveness as a force multiplier was prominently displayed during the Gulf War (1990-1991) [95], where it dramatically enhanced situational awareness and, in conjunction with precision-guided munitions and stealth technology, significantly elevated combat performance and operational coordination [44], [96].

To grapple with the ever-increasing complexity of modern warfare, C4ISR systems are constantly adapting to integrate cutting-edge advancements in information processing and data management. These systems seamlessly aggregate and analyze vast data streams from a network of sensors deployed across land, sea, air, and space domains. The advent of cloud computing has proven crucial in tackling this 'big data,' providing essential digital storage and processing capabilities [93]. Furthermore, the integration of AI into C4ISR systems holds immense promise for augmenting decision-making processes and revolutionizing battlefield information analysis [29], [97], [98].

By functioning as the military's "nervous system [89]," C4ISR allows the "muscle" components, including troops and weapon systems, to function effectively. Its relentless advancement mirrors the dynamic nature of military strategy and underscores the pursuit of technological superiority in the ever-evolving landscape of warfare.

This section synthesizes the fundamental attributes of AI capability, cyber capability, space capability, and C4ISR, informed by in-depth literature review. A key finding is that these capabilities serve as critical enablers in modern warfare, enhancing the efficiency and effectiveness of conventional military assets without directly applying physical force [19], enabling integrated coordination of various military organizations and assets to optimize operational efficiency and overall effectiveness. At the heart of these capabilities lies their inherent connection to cyberspace, a realm governed by electronic principles that facilitate rapid data processing [80]. These capabilities transform data into actionable intelligence, offering strategic advantages in military operations.

This study further explores the common characteristics of these cognitive military capabilities, examining how their combined application and synergy form a holistic military operational framework. This integrated approach underscores the importance of advanced ICT in redefining traditional military strategies and tactics, emphasizing the transformative impact on the adaptability of modern military forces.

V. ORGANIZING MILITARY COGNITIVE CAPABILITIES

In our study, we propose that military cognitive capabilities function not as isolated units but in a coordinated and interconnected manner, much like the complex workings of the human nervous system. The key to our analysis is understanding the pivotal role of data in integrating these capabilities.

In the context of military operations, data functions like the biological signals in the human nervous system. Data flows through diverse information and communication systems, propelled from battlefield sensors, transferred and centralized in dedicated hubs, and processed rigorously to align with strategic directives. Ultimately, this dynamic circulation culminates in actionable intelligence, extracted through careful interpretation. We delineate this dynamic journey as the "data life cycle," which encompasses four stages: (1) data generation, where raw information is captured from various battlefield's sensory outposts; (2) data transmission, ensuring the uninterrupted flow of data through communication channels; (3) data processing, where raw data is gathered, refined and aligned with strategic objectives; and (4) data interpretation, the final alchemy where actionable insights are extracted, ready to guide decisive action.

By focusing on this data-centric perspective, this analysis elucidates how different facets of military cognitive capabilities – such as AI capability, cyber capability, space capability, and C4ISR – integrate to operate as a unified structure. This approach highlights the synergistic and complementary interaction of these capabilities, providing a deeper understanding of their collective impact on enhancing military strategy and operational efficiency.

In our research, we conducted a comprehensive review of 14 strategic documents from the U.S. military. Our aim was to identify how these documents address the four distinct stages of the data life cycle. We meticulously examined all strategic documents to identify the military policies and technological elements that are relevant to the data life cycle. To better understand the overall structure, we organized these elements as keywords into a table (Appendix C), focusing on the technological components. Our analysis of these strategic documents revealed valuable insights into policies and technological components across all four stages of the data life cycle: data generation, transmission, processing, and interpretation. This analysis revealed that these strategic policies are fundamentally interconnected.

A. ORCHESTRATING MILITARY COGNITIVE CAPABILITIES

Our study posits that military cognitive capabilities, like the intricate workings of the human nervous system, function not in isolation but in a coordinated and interconnected manner. The data itself becomes the linchpin in our analysis. Our analysis of 14 strategic documents from the U.S. military, viewed through the lens of the data life cycle, provided valuable findings. The following is a comprehensive summary of the military policies and technological elements presented in the reviewed strategy documents, organized according to the data life cycle, based on Table 9 in Appendix C.

1) DATA GENERATION: SENSING THE BATTLEFIELD AND BEYOND

In the initial phase of data generation, military operations leverage a comprehensive array of advanced sensors, devices, and military platforms. These sensing technologies are strategically integrated into a variety of platforms, including terrestrial vehicles, aircraft, naval ships, submarines, and satellites, as well as advanced cyber infrastructure systems. They are deployed across all operational domains—land, sea, air, space, and cyberspace—to ensure a thorough surveillance and data collection coverage.

These devices are equipped to detect and capture a broad spectrum of data types. They gather information in diverse formats such as high-resolution images, acoustic sound waves, radio frequency signals, and chemical signals. This versatility enables comprehensive environmental assessment, crucial for informed decision-making in military operations.

Beyond the immediate tactical requirements of the battlefield, the scope of data generation extends to encompass non-tactical aspects of military operations. This includes the collection and analysis of data for purposes like military base management, personnel training programs, and overall military administration. The data generated in these contexts is vital for operational planning, resource allocation, and the continuous improvement of military management systems.

This detailed approach to data generation, characterized by its multi-domain and multi-format capabilities, reflects the complexity and technological sophistication of contemporary military operations. It underscores the strategic importance of diverse and robust data management methods. Effective military data management forms the bedrock of military intelligence and operational efficiency.

2) DATA TRANSMISSION: BRIDGING THE BATTLEFIED

During the data transmission phase in military operations, a wide range of communication methods are employed to efficiently transmit collected data to designated data hubs. The selection of these methods is carefully tailored based on the geographic location of the data source and the specific requirements for transmission capacity.

The array of communication methods includes advanced wireless communication systems for short to medium distances. These systems notably comprise cutting-edge 5G networks, which offer high-speed data transmission capabilities, and other wireless platforms operating across various bands of the electromagnetic spectrum (EMS). These technologies ensure rapid and secure data exchange, crucial in dynamic military environments.

For longer distances and global communication needs, sophisticated satellite communication systems are utilized. This includes traditional satellites and CubeSats, the latter offering a more agile and cost-effective solution for certain applications. These satellite systems play a critical role in ensuring uninterrupted data flow, especially in remote or challenging operational theaters.

Additionally, high-capacity transmission systems like optical fiber networks and Passive Optical Networks (PON) are integral for handling large volumes of data with minimal latency. These systems are essential in situations demanding rapid transmission of high-resolution data over substantial distances.

For tactical and field-level operations, specialized unit-level communication systems are deployed. These tactical communication systems are designed to provide reliable and secure communication channels, essential for coordination and command in local military operations.

Throughout all these communication methods, the implementation of standardized internet protocols (All-IP, IPv6) is a cornerstone policy. This ensures seamless interoperability between various communication systems, enabling a cohesive and integrated network for data transmission within the military infrastructure.

3) DATA PROCESSING: BEYOND BITS AND BYTES

In the critical data processing phase of military operations, a combination of cloud systems and specialized platforms are strategically utilized to manage and analyze the data transmitted from various sources. Cloud technology plays a central role in this phase, integrating extensive computing resources to ensure efficient and scalable data processing. This cloud-based infrastructure is key to handling the immense volumes of data, which is characteristic of contemporary military operations.

Within this framework, specialized platforms are deployed for AI and machine learning (ML) applications, alongside platforms dedicated to big data analytics. These platforms are tailored to meet diverse operational needs, ranging from real-time intelligence analysis to strategic planning and decision support. By leveraging the power of AI and ML algorithms, these platforms extract actionable insights from vast datasets – a vital process for informed decision-making in dynamic military environments.

Additionally, the platforms for big data analysis are designed to process and interpret large-scale data sets, enabling military strategists to identify patterns and trends that might otherwise be obscured in the volume of information. This capability is crucial for strategic forecasting and operational readiness.

Looking towards the future, the potential integration of quantum computing into military data processing systems is a development of considerable interest. Quantum computing promises to exponentially accelerate data processing capabilities, potentially transforming the landscape of military data analysis. This advancement could lead to significant enhancements in the speed and accuracy of decision-making processes, offering a substantial strategic advantage in military operations.

4) DATA INTERPRETATOIN: FROM CHAOS TO CLARITY

In the fourth and vital phase of data interpretation within military operations, the processed data undergoes a transformation into actionable intelligence. This critical phase employs sophisticated AI/ML (Artificial Intelligence/Machine Learning) analytics, complemented by advanced analysis techniques and visualization tools. The primary goal here is to distill vast amounts of raw data into coherent, actionable insights that are crucial for strategic and tactical decision-making.

AI/ML analytics play a pivotal role in this phase, utilizing cutting-edge algorithms to analyze complex data sets. These algorithms are capable of identifying patterns and trends that are not immediately apparent, offering predictive insights that are invaluable for military strategists. The advanced analysis techniques applied here go beyond traditional data processing, encompassing complex statistical methods and predictive modeling to enhance the understanding of potential scenarios and outcomes.

Visualization techniques are also integral to this phase, converting complex data sets into understandable graphical representations. These visualizations aid in conveying intricate information in an accessible manner, facilitating easier interpretation and quicker decision-making.

The data interpretation process supports a wide array of critical military functions. It enhances Command & Control systems by providing commanders with timely and data-driven insights. It supports decision-making processes with predictive analytics, contributes to situational awareness by offering a clearer picture of the operational environment, and aids in logistics planning. Moreover, it plays a significant role in modeling and simulation (M&S) exercises, war-gaming, live virtual construct (LVC), base management, healthcare applications, and the automation of various processes.

A key aspect of this phase is the real-time sharing of the analysis results. This ensures that all component commands within the military structure are synchronized, operating with the same updated and accurate information. Such real-time information dissemination is crucial in maintaining operational cohesion and ensuring the effectiveness of military strategies.

B. CYBER SECURITY

In addition to the core stages of the data life cycle, comprehensive cyber security is an essential aspect of military operations, as detailed in Appendix C. This capability encompasses a wide range of protective measures, designed to safeguard every aspect of the military's digital infrastructure. These measures extend from the data itself to a variety of critical components including devices, network facilities, data processing centers, and AI/software packages. Cyber security measures are meticulously integrated across all four stages of the data life cycle to protect data and critical components.

Cyber security in military operations is multifaceted, encompassing both offensive and defensive strategies. The defensive aspect is particularly critical, involving robust measures to protect against external cyber-attacks that can compromise data integrity and operational security. The defense measures include advanced encryption techniques, firewalls, intrusion detection systems, and continuous monitoring protocols to detect and neutralize threats. Additionally, cyber capability addresses the challenges posed by potential internal misuse. This involves establishing stringent access controls, conducting regular audits, and implementing insider threat detection systems to prevent unauthorized access or manipulation of military information.

The integration of offensive cyber operations is equally vital, where proactive measures are taken to disrupt or neutralize potential cyber threats. This includes developing capabilities for cyber espionage, information warfare, and the ability to deploy countermeasures against adversarial cyber activities.

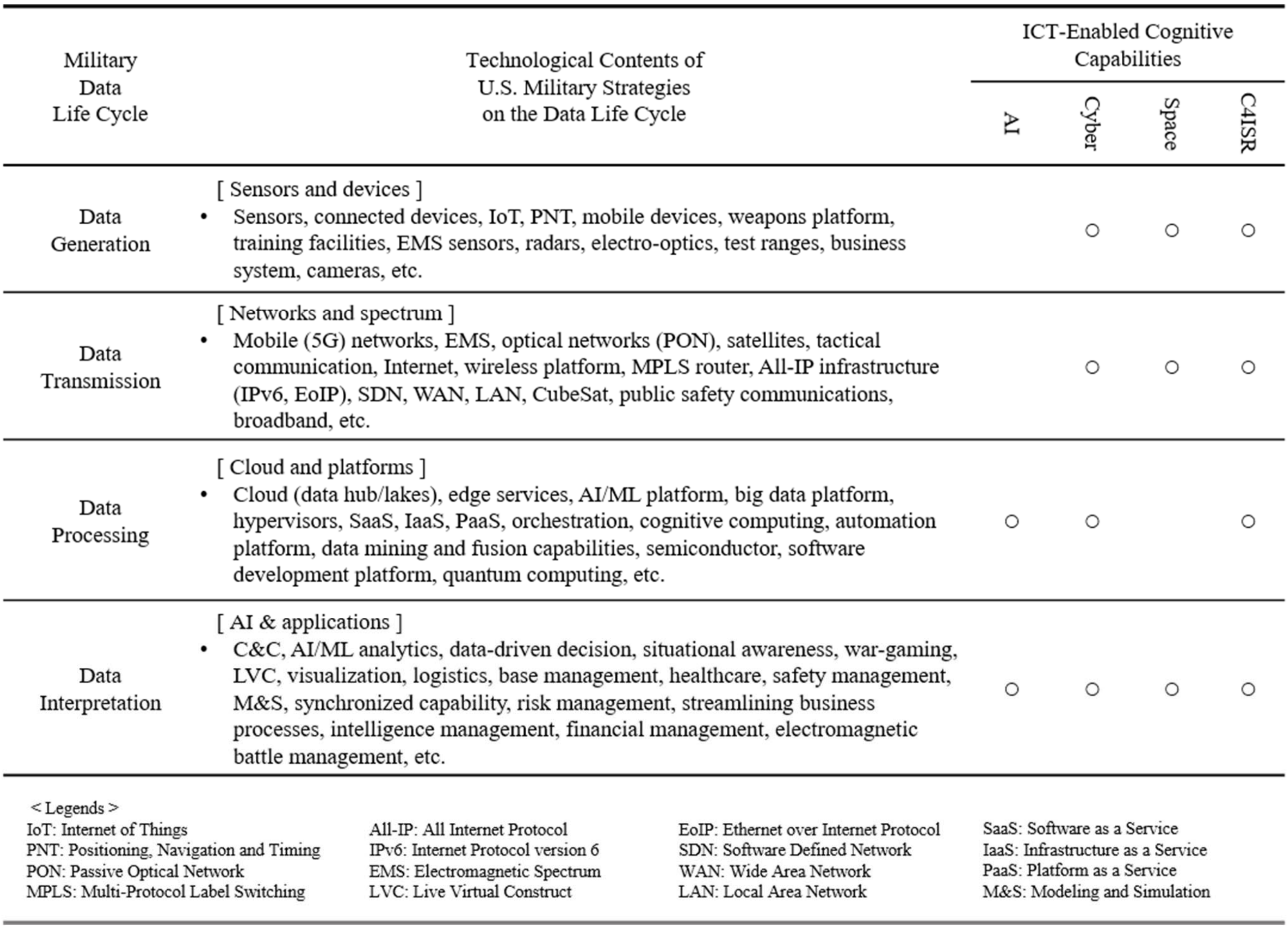
Overall, by incorporating a comprehensive zero-trust approach for the security of data, devices, network, application, and user, military cybersecurity emphasizes an enhanced architecture that requires robust verification procedures against all potential threats.

C. STRUCTURING MILITARY COGNITIVE CAPABILITIES

In our comprehensive analysis, we examined the contents of 14 strategic U.S. military documents, as listed in Appendix C. To present the findings concisely and avoid redundancies, we summarized the relevant information, which resulted in the creation of Table 4. This table presents an overview of the interplay between the data life cycle and various military cognitive capabilities. It systematically illustrates how AI capability, cyber capability, space capability, and C4ISR integrate and function across each phase of the data life cycle—encompassing data generation, transmission, processing, and interpretation.

Table 4's layout clearly illustrates the relationship between data life cycle stages and military cognitive capabilities by comprehensively incorporating technological components. This correlation highlights the complex and interconnected nature of these capabilities in modern military warfare. Their interwoven relationships are crucial for both ensuring efficient operations and gaining strategic advantage.

TABLE 4. The relationship between military cognitive capabilities and data life cycle from a technological perspective.



Military Data Life Cycle	Technological Contents of U.S. Military Strategies on the Data Life Cycle	ICT-Enabled Cognitive Capabilities			
		AI	Cyber	Space	C4ISR
Data Generation	[Sensors and devices] • Sensors, connected devices, IoT, PNT, mobile devices, weapons platform, training facilities, EMS sensors, radars, electro-optics, test ranges, business system, cameras, etc.		○	○	○
Data Transmission	[Networks and spectrum] • Mobile (5G) networks, EMS, optical networks (PON), satellites, tactical communication, Internet, wireless platform, MPLS router, All-IP infrastructure (IPv6, EoIP), SDN, WAN, LAN, CubeSat, public safety communications, broadband, etc.		○	○	○
Data Processing	[Cloud and platforms] • Cloud (data hub/lakes), edge services, AI/ML platform, big data platform, hypervisors, SaaS, IaaS, PaaS, orchestration, cognitive computing, automation platform, data mining and fusion capabilities, semiconductor, software development platform, quantum computing, etc.	○	○		○
Data Interpretation	[AI & applications] • C&C, AI/ML analytics, data-driven decision, situational awareness, war-gaming, LVC, visualization, logistics, base management, healthcare, safety management, M&S, synchronized capability, risk management, streamlining business processes, intelligence management, financial management, electromagnetic battle management, etc.	○	○	○	○

< Legends >

IoT: Internet of Things	All-IP: All Internet Protocol	EoIP: Ethernet over Internet Protocol	SaaS: Software as a Service
PNT: Positioning, Navigation and Timing	IPv6: Internet Protocol version 6	SDN: Software Defined Network	IaaS: Infrastructure as a Service
PON: Passive Optical Network	EMS: Electromagnetic Spectrum	WAN: Wide Area Network	PaaS: Platform as a Service
MPLS: Multi-Protocol Label Switching	LVC: Live Virtual Construct	LAN: Local Area Network	M&S: Modeling and Simulation

Our analysis of strategic U.S. military documents reveals the intricate interconnectedness of military cognitive capabilities through various stages of the data life cycle. This interconnectedness is systematically visualized in Fig. 1, which maps technological elements from Table 4 onto the data life cycle stages. Furthermore, Fig. 1 also incorporates the flow of Command and Control (C&C) from the cognitive power structure to operational domains. This C&C flow diagrammatically illustrates how decisions made in the cognitive domain trigger responses in the physical domain of military operations.

Fig. 1 illustrates the integrated structure of military cognitive capabilities based on ICT. This comprehensive visualization serves as the foundation for presenting the concept of 'military meta power.' In this study, we conceptualize 'military meta power' as an integrated entity, unifying diverse ICT-based cognitive capabilities under a single operational framework. This approach is further substantiated by our review of the South Korean MND's Defense Vision Document. The vision reinforces the paradigm of the cognitive military power as an essential construct in modern military strategy and operations.

VI. DEFINING ICT-ENABLED COGNITIVE MILITARY POWER

South Korea's MND, through its 'Defense Vision 2050' unveiled in November 2021, introduces 'military meta power' and 'military hard power' as distinct yet complementary elements of national defense [13]. This innovative approach acknowledges the ongoing transformation of the battlefield into a multi-dimensional arena. It envisions an operational environment that not only encompasses traditional domains such as land, sea, and air but also incorporates outer space, the realms of cyberspace, and even the human psyche [13]. This concept envisions a future battlefield where weaponized technology transcends traditional geographical domains, extending into the digital battlefield of cyberspace and human psychological realm.

In particular, the South Korean military strategists foresee a critical juncture—a 'singularity on the battlefield'—where the rapidity and intricacy of military operations will outpace human cognitive capacities. To address this evolving landscape, the strategy emphasizes the development of 'military meta power.' This new form of military strength is predicated on harnessing cutting-edge technologies such as

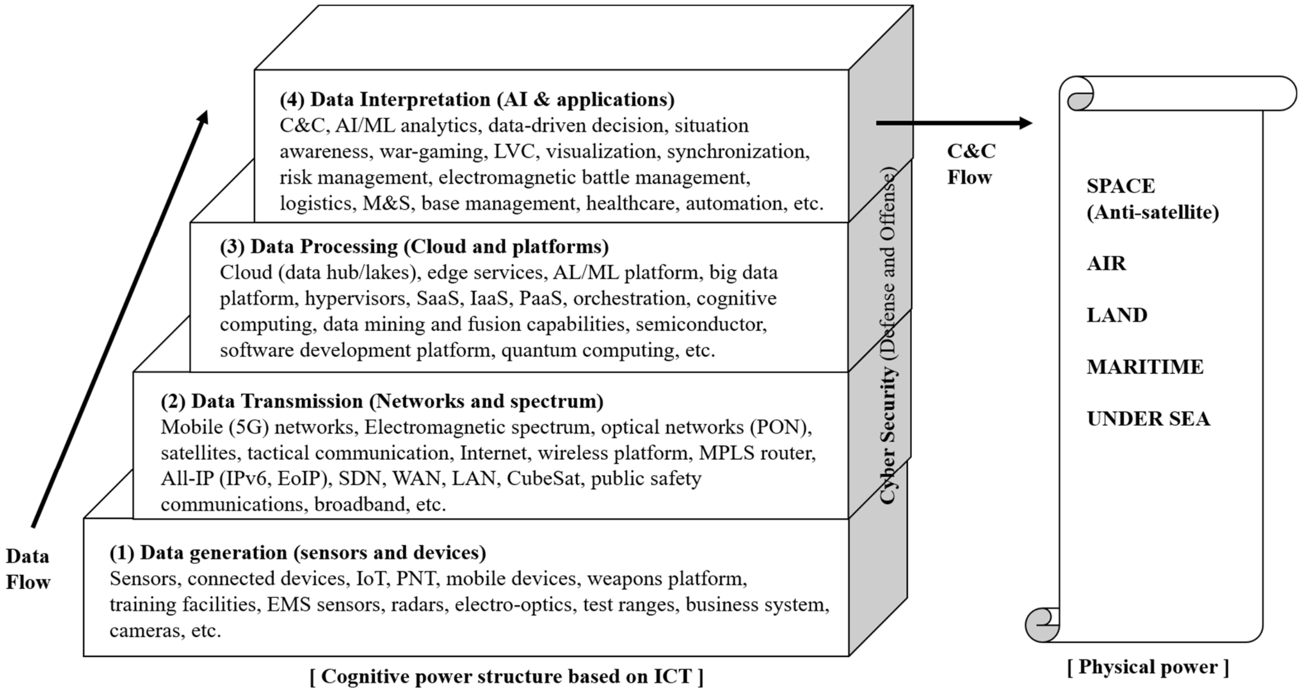

(4) Data Interpretation (AI & applications)
C&C, AI/ML analytics, data-driven decision, situation awareness, war-gaming, LVC, visualization, synchronization, risk management, electromagnetic battle management, logistics, M&S, base management, healthcare, automation, etc.
(3) Data Processing (Cloud and platforms)
Cloud (data hub/lakes), edge services, AL/ML platform, big data platform, hypervisors, SaaS, IaaS, PaaS, orchestration, cognitive computing, data mining and fusion capabilities, semiconductor, software development platform, quantum computing, etc.
(2) Data Transmission (Networks and spectrum)
Mobile (5G) networks, Electromagnetic spectrum, optical networks (PON), satellites, tactical communication, Internet, wireless platform, MPLS router, All-IP (IPv6, EoIP), SDN, WAN, LAN, CubeSat, public safety communications, broadband, etc.
(1) Data generation (sensors and devices)
Sensors, connected devices, IoT, PNT, mobile devices, weapons platform, training facilities, EMS sensors, radars, electro-optics, test ranges, business system, cameras, etc.
Cyber Security (Defense and Offense)
Data Flow
C&C Flow
SPACE (Anti-satellite)
AIR
LAND
MARITIME
UNDER SEA
[Cognitive power structure based on ICT]
[Physical power]

FIGURE 1. The comprehensive structure of military cognitive capabilities based on data life cycle.

AI, Big Data, and hyper-connected networks. It focuses on leveraging these technologies for instantaneous data sharing and in-depth analysis, thereby fostering advanced cognitive military capabilities crucial for real-time strategic decision-making [13].

This shift in perception reflects the South Korean military's strategic response to the asymmetric threats. These threats are primarily from North Korea's capabilities in nuclear and cyber warfare. This situation underscores the urgency of advancing cognitive military strength. The concept of 'military meta power' is central to this approach. 'Military meta power' emphasizes the development of sophisticated command and control systems. Also, it highlights the importance of integrated air defense systems, unmanned combat systems, and integrated future space capability. Advanced electromagnetic capability and efficient defense administration systems are equally crucial. All these elements, backed by proactive cyber capabilities, are essential for the country's effective Multi-Domain Operations. This highlights the increasing significance of technology-driven cognitive power in modern warfare [13].

Moreover, the South Korean military outlines four cardinal attributes that define 'military meta power': interaction, integration, analytics, and agility [13]. These attributes encapsulate the essence of this emergent power, highlighting the importance of dynamic interaction between different military elements, seamless integration of technologies and strategies, analytical depth in processing vast amounts of data, and agility in adapting to rapidly changing combat scenarios. Collectively, these attributes underscore the pivotal role of enhanced cognitive abilities, crucial for effectiveness in modern warfare's complex dynamics.

The South Korean strategy emphasizes preparing for a future battlefield, a 'singularity,' where rapid technological advancements and complex operational environments will demand enhanced cognitive capabilities. The term 'military meta power' encapsulates this paradigm shift, focusing on leveraging high-technology to augment military strategies and operations.

A. ATTRIBUTES OF MILITARY META POWER

Understanding 'military meta power' and its transformative potential for future military capabilities is crucial. This study synthesizes insights from diverse sources—including the South Korean MND's defense vision, U.S. military strategic documents, and relevant academic papers— to explore key aspects of four critical attributes: interaction, integration, analytics, and agility. By investigating these attributes, we offer a detailed understanding of their roles and implications in enhancing the strategic and operational military efficiency in the era of advanced technology.

1) INTERACTION

Interaction in the context of cognitive military power is pivotal for streamlined military operations. It encompasses the rapid exchange of data across the military hierarchy, facilitating both top-down and bottom-up communication. This dynamic interaction, crucial for adapting to real-time battlefield changes, fosters a state of 'self-synchronization,' thereby accelerating the pace and effectiveness of mission execution [91], [92].

Moreover, the realm of interaction extends beyond human-to-human communication, encompassing interactions between humans and machines, as well as autonomous machine-to-machine dialogues. In mixed manned-unmanned operational scenarios, human operators engage with unmanned systems via advanced human-machine interfaces, a process often referred to as 'man on the loop.' This interaction enables prompt human responses based on machine-provided intelligence. In contrast, in fully automated weapon systems, where human oversight is minimal ('man out of loop'), machine-based interactions prevail, ensuring seamless execution of pre-defined missions. However, for critical strategic decisions or sensitive operations, the integration of human judgment ('man in the loop') remains indispensable [26].

This diverse spectrum of interaction implies that, despite technological advancements, 'War is a human endeavor [99].' Technology can amplify and enable, but the human element – ingenuity, courage, and adaptation – remains at the core.

2) INTEGRATION

Integration plays a vital role in maximizing military effectiveness by synthesizing data across diverse battlefield domains. This process involves aggregating and analyzing data from multiple sources, forging a comprehensive picture of the operational environment. Such a unified representation of the battlefield is instrumental in enhancing decision-making accuracy and operational efficiency.

The 'System of Systems' concept underlines this integrated operation, focusing on the harmonious orchestration of diverse military components [100], [101]. This coordination is key to leveraging new combat capabilities, ensuring that all elements contribute effectively to the overall military goal. In line with this, Multi-Domain Operations emphasizes the necessity for commanders at every level to have a holistic view of the battlefield [102]. This approach requires commanders to integrate information from land, sea, air, space, and cyber domains to make informed strategic and tactical decisions.

Such integrated operations, which align different tactical actions under unified strategic themes, are crucial for achieving success in complex military scenarios [103]. By integrating scattered and diverse data from the battlefield, the military is better equipped to develop and execute sophisticated strategies and tactics. This comprehensive approach to data integration is not just about aggregating information; it's about transforming it into actionable intelligence that can decisively influence the outcome of military operations.

3) ANALYTICS

Analytics, a cornerstone of modern military strategy, is predominantly driven by AI and advanced analytical software. This technology marks a significant departure from traditional analysis tools, constrained by static rules. AI, in contrast, dynamically learns from data, enabling adaptive and autonomous problem-solving.

In tactical military operations, AI's role is transformative. It equips weapon systems with capabilities like sophisticated enemy identification and execution of precision strikes, thereby elevating combat effectiveness. Strategically, AI's ability to absorb and interpret data from varied environments allows it to formulate and suggest optimized strategies and tactics. This adaptability is particularly crucial in addressing the dynamic challenges of modern warfare.

The battlefield often presents scenarios of high complexity and intense pressure, where human decision-makers may encounter cognitive and physical limitations [6], [8], [26]. AI, unfettered by these human constraints, excels in processing complex, rapidly evolving battlefield information [6]. Its analytical prowess supports commanders by providing diverse, actionable solutions, thereby reducing the cognitive load and enhancing decision-making efficiency in critical military operations.

4) AGILITY

Agility in information technologies is a critical characteristic, particularly relevant in the military context. It empowers rapid interaction, integration, and analytics, essential for swift response to evolving operational scenarios. This agility is in harmony with the OODA Loop concept, formulated by John Boyd. The OODA Loop—Observe, Orient, Decide, and Act—is a process that encapsulates the rapid and cyclic decision-making essential in dynamic environments [104]. In military operations, the ability to swiftly progress through this cycle can paralyze adversaries whereas enhancing friendly forces' strategic initiatives.

This agility is most conspicuous in the realm of cyber warfare, a domain where speed is as critical as strategy. Agility here refers to the capacity to quickly adapt and respond to non-kinetic threats, such as cyberattacks, deep fakes, and misinformation campaigns [26]. The rapid and often covert nature of these threats necessitates an equally swift and informed response. Utilizing AI and sophisticated analysis software, defense systems can rapidly detect early signs of cyber intrusions or misinformation, allowing for the timely deployment of countermeasures. This property not only mitigates potential damage but also strengthens overall cybersecurity posture. These points effectively illustrate the critical role of agility in contemporary military strategy.

The concept of 'military meta power,' intricately weaving together the attributes of interaction, integration, analytics, and agility, is the bedrock of modern military strategy. This multifaceted power acts as the "ultimate connector," effectively bridging diverse military elements across various domains, thereby fostering seamless interaction. Its role as a "force multiplier [86], [95], [105]" is evident in its ability to integrate disparate data streams, synthesizing a coherent and comprehensive understanding of the battlefield. This integration is instrumental in sharing a unified operational picture, facilitating coordinated joint operations, and significantly enhancing the efficacy of military maneuvers [19], [105].

Beyond its role as a connector and integrator, the cognitive military power subtly but substantially amplifies the capabilities of physical-force-based military armament. The power acts as a "potential enabler [19], [105]," where its intelligent and autonomous systems augment the performance of traditional weaponry, subtly enhancing their effectiveness without directly exerting physical force. This characteristic represents a paradigm shift in military technology, where the cognitive dimension of power complements and reinforces the physical dimension.

Moreover, this emerging form of military power operates with the rapidity and efficiency of modern electronic technology, establishing itself as a 'proactive assistant' in contemporary warfare. Its rapid processing and analysis capabilities enable early detection of threats, providing military strategists with timely and actionable insights. This proactive nature ensures that military operations stay ahead of potential challenges, offering strategic solutions in real-time. In the information age, these capabilities redefine the landscape of military operations.

VII. ADAPTING MILITARY META POWER AND DISCUSSION

The concept of 'military meta power' is crucial for policymakers, scholars, and defense communities seeking to enhance military capabilities by leveraging advanced ICT. Military meta power embodies the integration of diverse capabilities in multiple military domains, including AI, cyber, space, and C4ISR, forming a key foundation for technological innovation in military operations. The following points are essential considerations for the development, construction, and operation of military meta power.

A. HOLISTIC APPORACH FOR COGNITIVE MILITARY POWER

In the context of optimizing widely spread information and communication systems, adopting a holistic view of military ICT infrastructure is crucial. Efficiently integrating and effectively operating distributed systems that produce and process vast amounts of diverse data presents a significant challenge. This necessitates a comprehensive understanding of the various systems involved, coupled with organized participation and coordination across all stakeholders.

A comprehensive and balanced design is essential for the cognitive military system, especially due to the internalization of wartime-critical ICT infrastructure into military organization. The design must ensure seamless orchestration of diverse systems and optimizes data flow throughout entire data lifecycle (generation, transmission, processing, and interpretation) to prevent detrimental bottlenecks, particularly during wartime when external resources are unavailable.

Across both strategic and tactical battlefields, comprehensive data collection and processing are essential for the military operations. In strategic theaters with large geographical areas, ICT systems for real-time communication and seamless data processing are critical for informed decision making. Even in tactical operations focused on specific areas, like enemy identification and precision strikes, collecting operational results centrally is crucial. Whereas real-time data collection might not be feasible in this case, analyzing these data together allows for system upgrades and continuous performance improvements.

Additionally, the holistic approach of cognitive military power also helps to avoid trial and error that can occur when systems are developed from individual perspectives. The concept guides military strategists to focus on creating systems that work well together (interoperability), can be tailored to meet diverse military needs (flexibility), and can evolve with technological advancements (scalability). In today's rapidly changing technological landscape, the concept encourages the adoption of ICT solutions that are not only advanced but also versatile and future-proof.

For instance, standardizing data formats and communication protocols ensures seamless information exchange between disparate military systems. This is a crucial cog in the machinery of coordinated battlefield actions. The adaptability extends further, with ICT systems designed to flexibly adapt to changes in demand, such as those in operational situations, organizational structures, tasks, and information sharing scope. Finally, in light of the rapid pace of technological evolution, military ICT systems must be designed to incorporate new technologies and features with scalable system architecture. The approaches to technological innovation are key to driving not only advancements in technology-based structures, but also in shaping more effective organizational structures and doctrinal principles in modern military strategy [106], [107].

B. PSYCHOLOGIC IMPACT AND RESPONSIBILITY

The concept of 'military meta power' holds substantial implications for both the academic and defense communities, particularly in its potential impact on the psychology and decision-making processes of military commanders. Historically, whereas the introduction of nuclear weapons revolutionized military strategy and transformed the nature of warfare, their influence on the psychological aspects of strategic decision-making was not as significant [8]. Even in scenarios involving nuclear-armed powers, strategic choices largely remained within the realm of human psychology [8]. However, the emergence and advancement of ICT have brought a paradigm shift. The cognitive military power, enabled by ICT advancements, is poised to play an increasingly influential role in shaping strategic decision-making [25], [26]. This shift suggests a move from purely human-centric decision processes to a human-machine collaborative structure where technology significantly informs and influences the cognitive aspects of military strategy and leadership.

The emergence of "military meta power" marks a significant shift in the nature of warfare, characterized by the integration of advanced information technologies that enhance human cognitive abilities. This phenomenon resonates with the extension theory of technology, which posits that technological advancements serve as extensions of

TABLE 5. Comparative framework of human cognitive system and ICT-enabled cognitive military structure.

	Human Cognitive System	ICT-Enabled Cognitive Military Structure
Upper Concepts	Nervous System	Military meta power
Cognitive Capabilities	Acquisition of knowledge, manipulation of information, reasoning, etc.	AI capability, Cyber capability, Space capability, and C4ISR
Medium	Biological signals, electrical and chemical	Data
Sub-Components	Brain, spinal cord, nerves and sensory organ	AI, Cloud, Big data technology, IoT, 5G, networks, spectrum, cyber security, SW platform, sensor, space communications, etc.

human capabilities. Reflecting aspects of human cognitive functions, including perception, learning, decision-making, and language processing, the concept of the cognitive military power embodies the theory's principle, encompassing a range of activities, such as real-time battlefield awareness through sensors, seamless communications for efficient coordination, and data analysis for informed decision-making. These functions not only enhance operational effectiveness but also hold profound implications for the psychological aspects of military activities, potentially influencing the way commanders perceive threats, assess situations, and ultimately make critical decisions in dynamic battlefield environments.

To illustrate this parallel between the elements of the human nervous system and aspects of military meta power, we present Table 5. This comparison helps conceptually evaluate how military capabilities, powered by ICT, align with human cognitive faculties. In Table 5, we juxtapose the upper concepts, cognitive capabilities, mediums, and sub-components of the human nervous system and the cognitive military power.

The potential impact of the cognitive military power on the decision-making processes of human commanders is a topic of ongoing debate [8], [25], [108]. This discussion has gained momentum with the advent of advanced large-scale AI technologies, triggered by the release of ChatGPT in November 2022, sparking conversations around the viability of Artificial General Intelligence (AGI) and its associated opportunities and challenges [109], [110]. This issue becomes particularly critical in the defense sector, where cognitive military power could fundamentally influence battlefield decision-making, possibly involving significant loss of human lives and extensive damage to property.

During warfare, human strategic decision-making is often constrained by human cognitive biases such as heuristics and groupthink [6]. Machines, in contrast, are not bound by these human limitations and continuously improve their algorithms through learning [6]. However, reliance on machines for decision-making is not without its pitfalls. When machines operate beyond the predefined human criteria or encounter errors in human-set goals, they can lead to generating erroneous outcomes [111], such as misidentifying friendly forces as enemies or escalating conflicts due to faulty risk assessments [25], [26]. This scenario introduces a new dimension of uncertainty and risk [111]. Exploring mechanisms for human-machine collaboration in strategic decision-making, alongside robust safeguards against machine errors, will be crucial to mitigating these risks and leveraging the potential of military meta power in a responsible and efficient manner.

AI algorithms are being applied to a wide range of tasks, such as decision-making and autonomous weapons, due to their capacity for rapid learning and adaptation. However, it is possible that these systems may deviate from human intentions, leading to unforeseen consequences and ethical dilemmas. This phenomenon underscores the crucial need for establishing robust technological and procedural guidelines rooted in human oversight. This study proposes a framework for developing the cognitive military power that prioritizes human control, and accountability throughout the design, deployment, and use phases. By embedding these principles into this emerging power, we can mitigate the risks of unintended consequences and ensure its responsible application in accordance with human intentions.

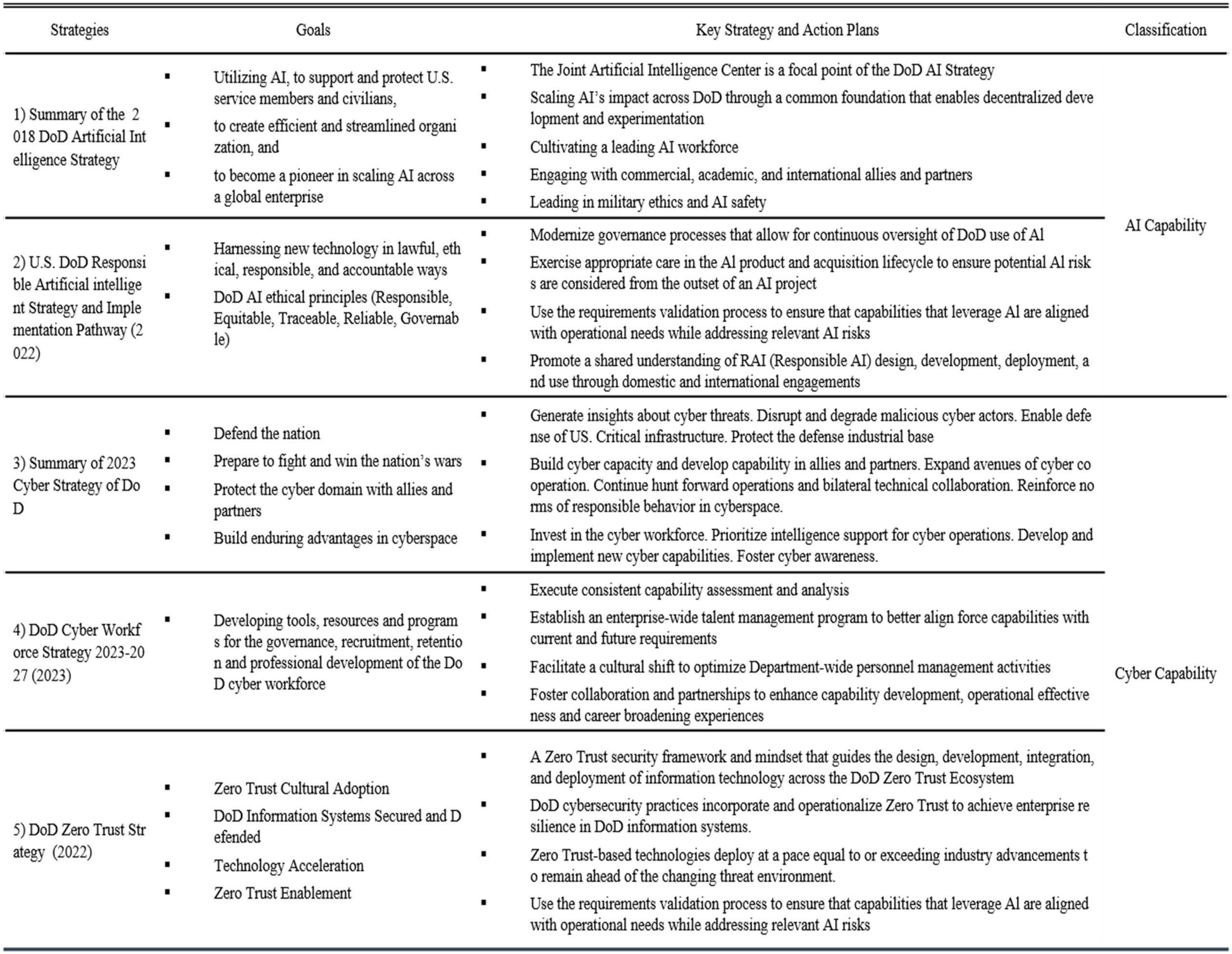
Given the profound influence of cognitive military power on future warfare, open and comprehensive discussions are critical to ensure its development and deployment remain aligned with human values. These discussions should be informed by an ethical framework that prioritizes transparency, accountability, and risk mitigation in R&D, safeguarding against potential biases and unintended consequences as these technologies evolve. Robust ethical principles are not simply desirable, but rather essential for managing the profound impacts of integrating advanced cognitive capabilities into military strategies.

VIII. CONCLUSION

This study conducted a thorough investigation of the role of emerging information and communications technologies, such as AI, big data, cloud computing, cybersecurity, and advanced networking, in shaping military cognitive capabilities. Anchored within 'the extension theory of technology,' which views these technologies as augmentations of human cognitive abilities [17], we studied the implications of 'military meta power' to investigate the qualitative shift in military power that occurs through the use of ICT.

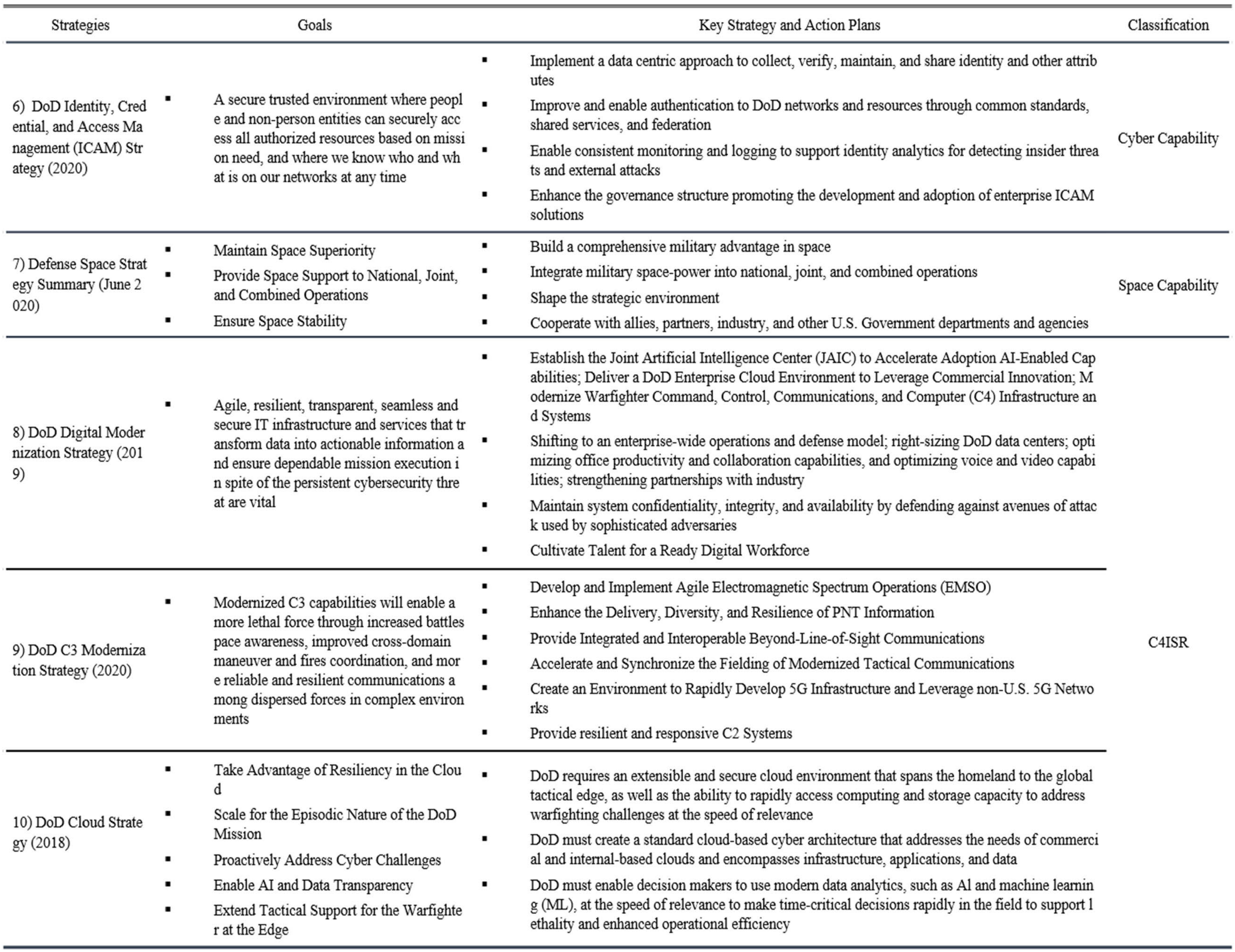
The concept of military meta power, released in South Korea's Defense Vision 2050 (2021), echoes the importance of cognitive capabilities in military strategy, particularly in the context of a dynamic and an increasingly complex multi-domain battlefield. Our comprehensive review of strategic military documents identified four key areas of military cognitive capabilities: AI capability, cyber capability, space capability, and C4ISR. Our further analysis revealed these capabilities are interlinked, functioning synergistically much like the human nervous system, leading

TABLE 6. Summary of U.S. military strategies related to ICT.



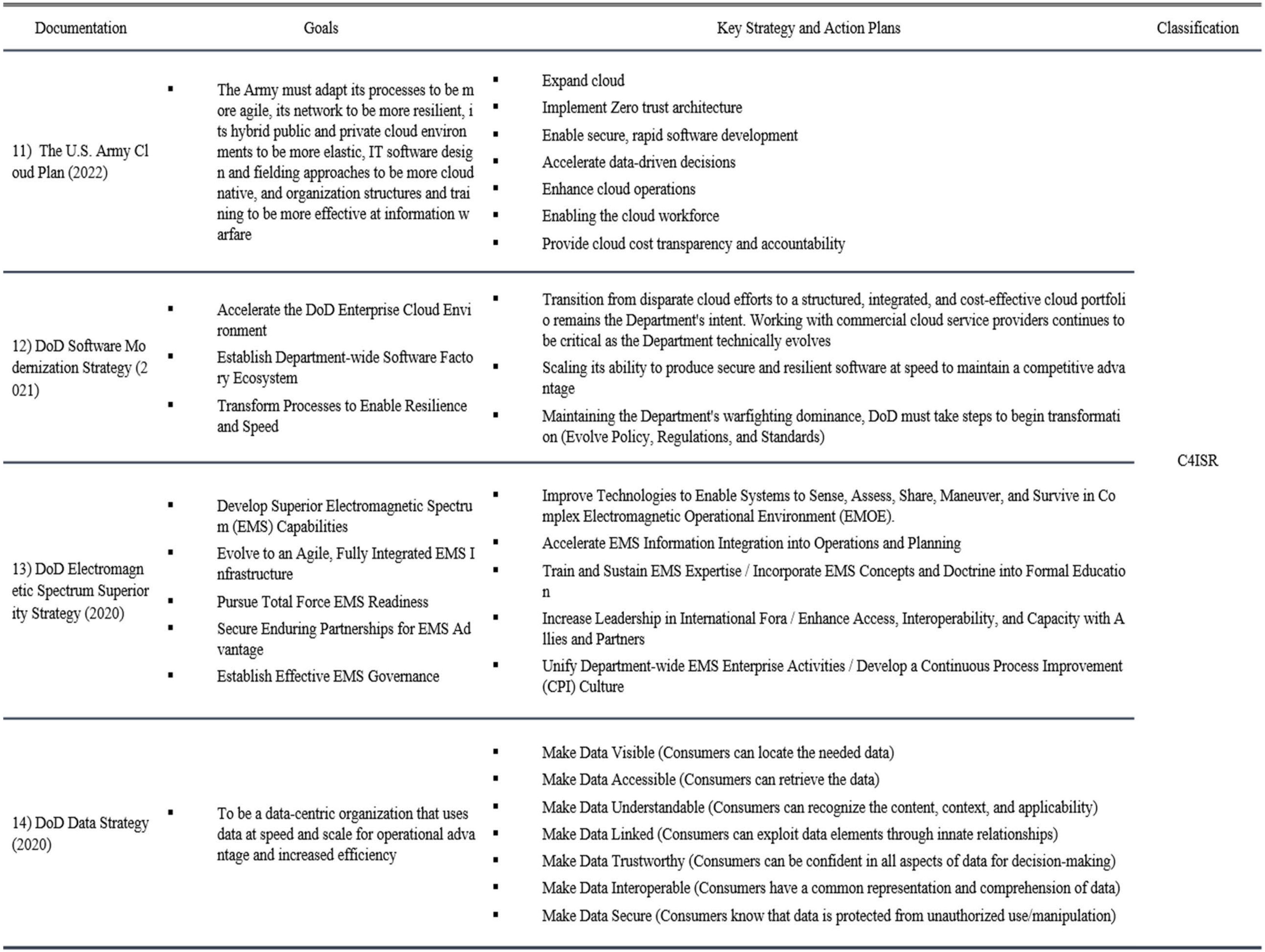
Strategies	Goals	Key Strategy and Action Plans	Classification
1) Summary of the 2018 DoD Artificial Intelligence Strategy	▪ Utilizing AI, to support and protect U.S. service members and civilians, ▪ to create efficient and streamlined organization, and ▪ to become a pioneer in scaling AI across a global enterprise	▪ The Joint Artificial Intelligence Center is a focal point of the DoD AI Strategy ▪ Scaling AI's impact across DoD through a common foundation that enables decentralized development and experimentation ▪ Cultivating a leading AI workforce ▪ Engaging with commercial, academic, and international allies and partners ▪ Leading in military ethics and AI safety	AI Capability
2) U.S. DoD Responsible Artificial intelligent Strategy and Implementation Pathway (2022)	▪ Harnessing new technology in lawful, ethical, responsible, and accountable ways ▪ DoD AI ethical principles (Responsible, Equitable, Traceable, Reliable, Governable)	▪ Modernize governance processes that allow for continuous oversight of DoD use of AI ▪ Exercise appropriate care in the AI product and acquisition lifecycle to ensure potential AI risks are considered from the outset of an AI project ▪ Use the requirements validation process to ensure that capabilities that leverage AI are aligned with operational needs while addressing relevant AI risks ▪ Promote a shared understanding of RAI (Responsible AI) design, development, deployment, and use through domestic and international engagements	
3) Summary of 2023 Cyber Strategy of DoD	▪ Defend the nation ▪ Prepare to fight and win the nation's wars ▪ Protect the cyber domain with allies and partners ▪ Build enduring advantages in cyberspace	▪ Generate insights about cyber threats. Disrupt and degrade malicious cyber actors. Enable defense of US. Critical infrastructure. Protect the defense industrial base ▪ Build cyber capacity and develop capability in allies and partners. Expand avenues of cyber cooperation. Continue hunt forward operations and bilateral technical collaboration. Reinforce norms of responsible behavior in cyberspace. ▪ Invest in the cyber workforce. Prioritize intelligence support for cyber operations. Develop and implement new cyber capabilities. Foster cyber awareness.	Cyber Capability
4) DoD Cyber Workforce Strategy 2023-2027 (2023)	▪ Developing tools, resources and programs for the governance, recruitment, retention and professional development of the DoD cyber workforce	▪ Execute consistent capability assessment and analysis ▪ Establish an enterprise-wide talent management program to better align force capabilities with current and future requirements ▪ Facilitate a cultural shift to optimize Department-wide personnel management activities ▪ Foster collaboration and partnerships to enhance capability development, operational effectiveness and career broadening experiences	
5) DoD Zero Trust Strategy (2022)	▪ Zero Trust Cultural Adoption ▪ DoD Information Systems Secured and Defended ▪ Technology Acceleration ▪ Zero Trust Enablement	▪ A Zero Trust security framework and mindset that guides the design, development, integration, and deployment of information technology across the DoD Zero Trust Ecosystem ▪ DoD cybersecurity practices incorporate and operationalize Zero Trust to achieve enterprise resilience in DoD information systems. ▪ Zero Trust-based technologies deploy at a pace equal to or exceeding industry advancements to remain ahead of the changing threat environment. ▪ Use the requirements validation process to ensure that capabilities that leverage AI are aligned with operational needs while addressing relevant AI risks	

TABLE 6. ***(Continued.)*** **Summary of U.S. military strategies related to ICT.**



Strategies	Goals	Key Strategy and Action Plans	Classification
6) DoD Identity, Credential, and Access Management (ICAM) Strategy (2020)	▪ A secure trusted environment where people and non-person entities can securely access all authorized resources based on mission need, and where we know who and what is on our networks at any time	▪ Implement a data centric approach to collect, verify, maintain, and share identity and other attributes ▪ Improve and enable authentication to DoD networks and resources through common standards, shared services, and federation ▪ Enable consistent monitoring and logging to support identity analytics for detecting insider threats and external attacks ▪ Enhance the governance structure promoting the development and adoption of enterprise ICAM solutions	Cyber Capability
7) Defense Space Strategy Summary (June 2020)	▪ Maintain Space Superiority ▪ Provide Space Support to National, Joint, and Combined Operations ▪ Ensure Space Stability	▪ Build a comprehensive military advantage in space ▪ Integrate military space-power into national, joint, and combined operations ▪ Shape the strategic environment ▪ Cooperate with allies, partners, industry, and other U.S. Government departments and agencies	Space Capability
8) DoD Digital Modernization Strategy (2019)	▪ Agile, resilient, transparent, seamless and secure IT infrastructure and services that transform data into actionable information and ensure dependable mission execution in spite of the persistent cybersecurity threat are vital	▪ Establish the Joint Artificial Intelligence Center (JAIC) to Accelerate Adoption AI-Enabled Capabilities; Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation; Modernize Warfighter Command, Control, Communications, and Computer (C4) Infrastructure and Systems ▪ Shifting to an enterprise-wide operations and defense model; right-sizing DoD data centers; optimizing office productivity and collaboration capabilities, and optimizing voice and video capabilities; strengthening partnerships with industry ▪ Maintain system confidentiality, integrity, and availability by defending against avenues of attack used by sophisticated adversaries ▪ Cultivate Talent for a Ready Digital Workforce	C4ISR
9) DoD C3 Modernization Strategy (2020)	▪ Modernized C3 capabilities will enable a more lethal force through increased battlespace awareness, improved cross-domain maneuver and fires coordination, and more reliable and resilient communications among dispersed forces in complex environments	▪ Develop and Implement Agile Electromagnetic Spectrum Operations (EMSO) ▪ Enhance the Delivery, Diversity, and Resilience of PNT Information ▪ Provide Integrated and Interoperable Beyond-Line-of-Sight Communications ▪ Accelerate and Synchronize the Fielding of Modernized Tactical Communications ▪ Create an Environment to Rapidly Develop 5G Infrastructure and Leverage non-U.S. 5G Networks ▪ Provide resilient and responsive C2 Systems	
10) DoD Cloud Strategy (2018)	▪ Take Advantage of Resiliency in the Cloud ▪ Scale for the Episodic Nature of the DoD Mission ▪ Proactively Address Cyber Challenges ▪ Enable AI and Data Transparency ▪ Extend Tactical Support for the Warfighter at the Edge	▪ DoD requires an extensible and secure cloud environment that spans the homeland to the global tactical edge, as well as the ability to rapidly access computing and storage capacity to address warfighting challenges at the speed of relevance ▪ DoD must create a standard cloud-based cyber architecture that addresses the needs of commercial and internal-based clouds and encompasses infrastructure, applications, and data ▪ DoD must enable decision makers to use modern data analytics, such as Al and machine learning (ML), at the speed of relevance to make time-critical decisions rapidly in the field to support lethality and enhanced operational efficiency	

TABLE 6. *(Continued.)* Summary of U.S. military strategies related to ICT.



Documentation	Goals	Key Strategy and Action Plans	Classification
11) The U.S. Army Cloud Plan (2022)	▪ The Army must adapt its processes to be more agile, its network to be more resilient, its hybrid public and private cloud environments to be more elastic, IT software design and fielding approaches to be more cloud native, and organization structures and training to be more effective at information warfare	▪ Expand cloud ▪ Implement Zero trust architecture ▪ Enable secure, rapid software development ▪ Accelerate data-driven decisions ▪ Enhance cloud operations ▪ Enabling the cloud workforce ▪ Provide cloud cost transparency and accountability	C4ISR
12) DoD Software Modernization Strategy (2021)	▪ Accelerate the DoD Enterprise Cloud Environment ▪ Establish Department-wide Software Factory Ecosystem ▪ Transform Processes to Enable Resilience and Speed	▪ Transition from disparate cloud efforts to a structured, integrated, and cost-effective cloud portfolio remains the Department's intent. Working with commercial cloud service providers continues to be critical as the Department technically evolves ▪ Scaling its ability to produce secure and resilient software at speed to maintain a competitive advantage ▪ Maintaining the Department's warfighting dominance, DoD must take steps to begin transformation (Evolve Policy, Regulations, and Standards)	
13) DoD Electromagnetic Spectrum Superiority Strategy (2020)	▪ Develop Superior Electromagnetic Spectrum (EMS) Capabilities ▪ Evolve to an Agile, Fully Integrated EMS Infrastructure ▪ Pursue Total Force EMS Readiness ▪ Secure Enduring Partnerships for EMS Advantage ▪ Establish Effective EMS Governance	▪ Improve Technologies to Enable Systems to Sense, Assess, Share, Maneuver, and Survive in Complex Electromagnetic Operational Environment (EMOE). ▪ Accelerate EMS Information Integration into Operations and Planning ▪ Train and Sustain EMS Expertise / Incorporate EMS Concepts and Doctrine into Formal Education ▪ Increase Leadership in International Fora / Enhance Access, Interoperability, and Capacity with Allies and Partners ▪ Unify Department-wide EMS Enterprise Activities / Develop a Continuous Process Improvement (CPI) Culture	
14) DoD Data Strategy (2020)	▪ To be a data-centric organization that uses data at speed and scale for operational advantage and increased efficiency	▪ Make Data Visible (Consumers can locate the needed data) ▪ Make Data Accessible (Consumers can retrieve the data) ▪ Make Data Understandable (Consumers can recognize the content, context, and applicability) ▪ Make Data Linked (Consumers can exploit data elements through innate relationships) ▪ Make Data Trustworthy (Consumers can be confident in all aspects of data for decision-making) ▪ Make Data Interoperable (Consumers have a common representation and comprehension of data) ▪ Make Data Secure (Consumers know that data is protected from unauthorized use/manipulation)	

TABLE 7. Keywords used in the search by segments.

Segment	Key words
Military (5)	"military strateg*", "military power", "military warfare", "military tactic*", "military capabilit*"
ICT (21)	"information technolog*", AI, "artificial intelligence", "machine learning", cloud, data IoT, cyber, communication*, "radio frequency", space, satellite*, electromagnetic, "command and control", network*, internet, 5G, sensor*, software, "quantum computing", optic

TABLE 8. The results of the classification of academic papers by ICT-enabled military capabilities.

Domains	2009 ~ 2011	2012 ~ 2014	2015 ~ 2017	2018 ~ 2020	2021 ~ 2023	Total
AI	0	1	3	13	18	35
Cyber	2	3	12	10	5	32
Space	5	3	1	7	7	23
C4ISR	34	29	35	28	17	143
Total	41	36	51	58	47	233

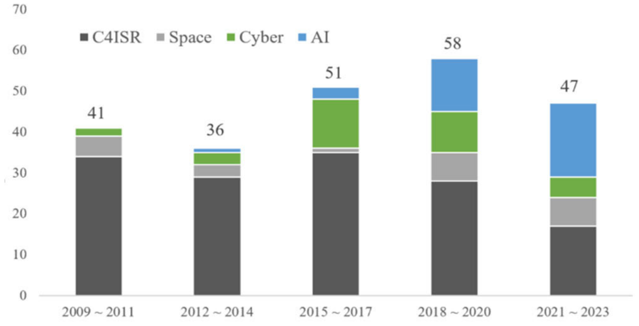


FIGURE 2. The changing proportion of academic research on ICT-based military capabilities over time.

us to a unified structure encompassing these cognitive capabilities.

We are convinced that military meta power will significantly influence future military landscapes. Achieving 'cognitive superiority' will enable militaries to rapidly and effectively counter and adapt to threats, transforming operational performance and efficiency. These findings illuminate not only the transformative characteristics of ICT in military strength but also underscore the increasing influence of cognitive capabilities in modern defense strategies.

The growing reliance on technology in military decision-making raises concerns about oversight and ensuring alignment with human intentions. This challenge becomes particularly pressing when technological evolution outpaces our understanding, potentially leading to unforeseen outcomes. Therefore, establishing guidelines for the development and application of the cognitive military power is desirable and essential, emphasizing ethical considerations.

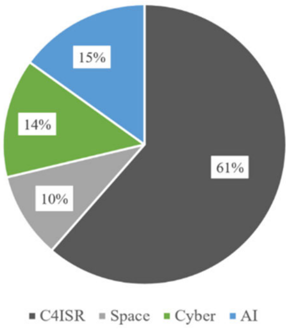


FIGURE 3. The proportion of academic research on ICT-based military capabilities from 2009 to 2023.

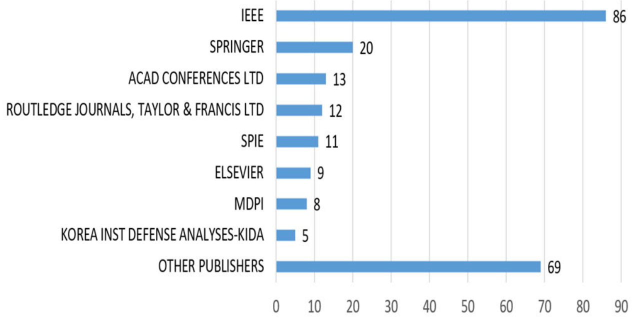


FIGURE 4. The proportion of academic research on ICT-based military capabilities by publisher.

A balanced approach, leveraging technological advancements within the bounds of human oversight and ethical principles, is imperative to ensure military capabilities remain aligned with human value. This commitment ensures secure and responsible warfare in the age of advanced technology.

APPENDIX A

See Table 6.

APPENDIX B

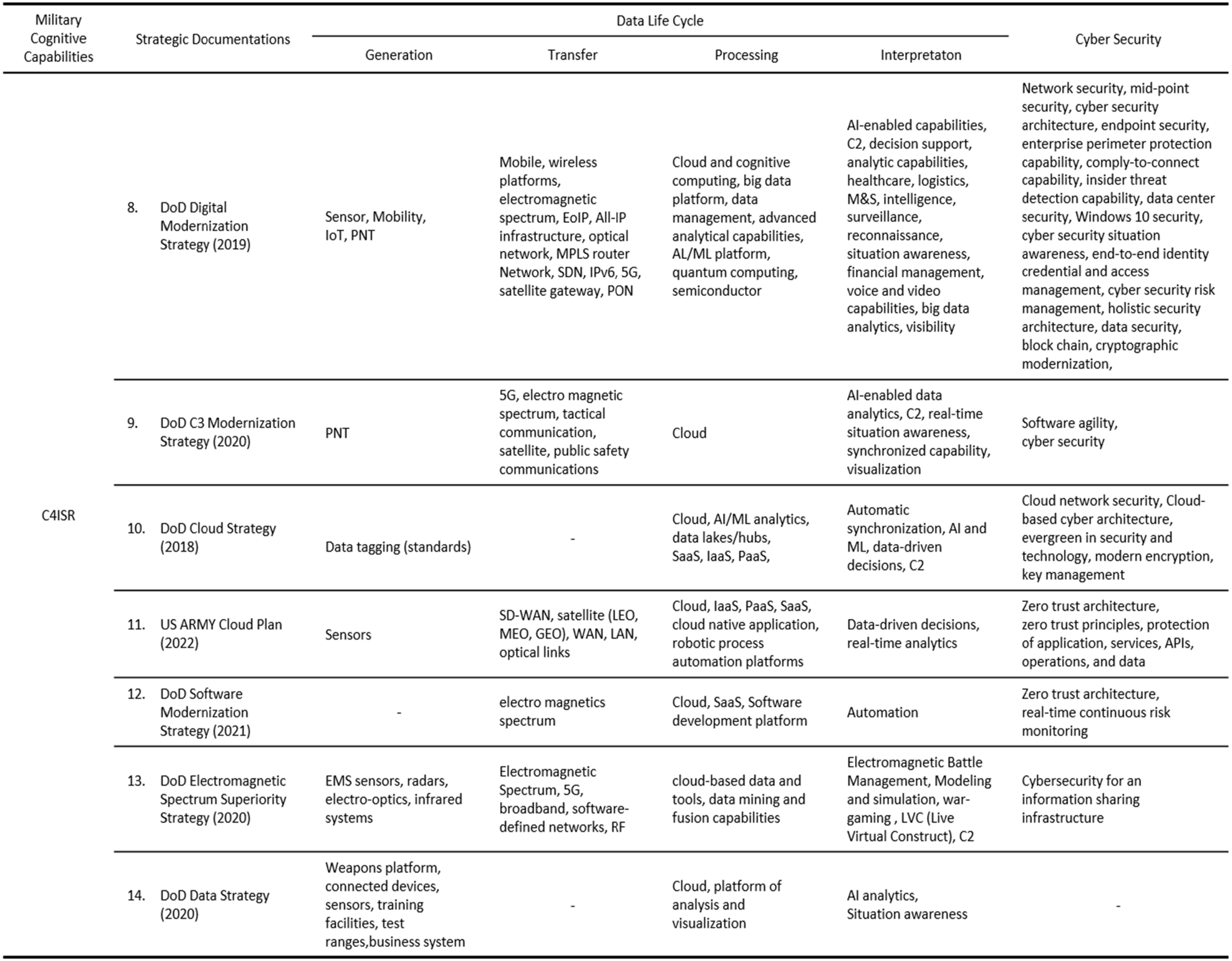
This study conducted a systematic review of academic papers to categorize ICT-enabled military capabilities. Initially, we categorized them into four domains: AI capability, cyber capability, space capability, and C4ISR, drawing from the 14 strategies published by the US military. Through a systematic review, we aimed to assess whether this classification is applicable to the broader academic literature.

The academic papers reviewed were articles published in journals and conferences from 2009 to 2023. The search was conducted using the database of "Web of Science". The search focused on documents that pertained to both of the military segment and the ICT segment. The military segment searched for papers with at least one of five keywords (listed in Table 7) in their abstracts, while the ICT segment searched for papers with at least one of 21 representative keywords from various information and communication areas, also within their abstracts. Ultimately, 597 papers common to both segments were reviewed.

TABLE 9. Relationship between military cognitive capabilities and data life cycle.

Military Cognitive Capabilities	Strategic Documentations	Data Life Cycle				Cyber Security
		Generation	Transmission	Processing	Interpretaton	
AI Capability	1. Summary of the 2018 DoD Artificial Intelligence Strategy (2018)	-	-	Cloud and edge services	Pattern recognition, learning from experience, drawing conclusions, making predictions, risk management, equipment maintenance, situation awareness, decision-making, streamlining business processes, problem solving, safety management	-
	2. US DoD Responsible Arthritical Intelligence Strategy and Implementation Pathway (2022)	-	-	-	AI-ready and data-centric organization	-
Cyber Capability	3. Summary of 2023 Cyber Strategy of DoD (2018)	-	-	-	Automated data analytics	Tracking malicious cyber actors, defending critical infrastructure, cooperating with Allies and partners, implementing Zero Trust architectures, fostering a culture of cyber awareness, modernizing cryptographic algorithms, enhancing cyber forensics
	4. DoD Cyber Workforce Strategy 2023 – 2027	-	-	Cloud, quantum computing	data analytics	Advanced cryptography and zero-trust
	5. DoD Zero Trust Strategy (2022)	Devices (real time inspection), Data tagging	Network environment	Applications, hypervisors, virtual machines, cloud-based technologies, orchestration	Visibility, analytics, AI/ML, real time access decision, intelligent decisions	Zero trust culture adoption, Information systems secured, Technology acceleration, Zero trust enablement (policy and funding etc.), devices security, data encryption, applications and network security, improving detection and reaction
	6. DoD Identity, Credential, and Access Management (ICAM) Strategy (2020)	Data tagging	-	-	Big Data analytics	Access management control, Public Key Infrastructure (PKI) Program
Space Capability	7. Defense Space Strategy Summary (2020)	-	-	-	Intelligence and C2	-

TABLE 9. ***(Continued.)*** **Relationship between military cognitive capabilities and data life cycle.**



Military Cognitive Capabilities	Strategic Documentations	Data Life Cycle				Cyber Security
		Generation	Transfer	Processing	Interpretaton	
C4ISR	8. DoD Digital Modernization Strategy (2019)	Sensor, Mobility, IoT, PNT	Mobile, wireless platforms, electromagnetic spectrum, EoIP, All-IP infrastructure, optical network, MPLS router Network, SDN, IPv6, 5G, satellite gateway, PON	Cloud and cognitive computing, big data platform, data management, advanced analytical capabilities, AL/ML platform, quantum computing, semiconductor	AI-enabled capabilities, C2, decision support, analytic capabilities, healthcare, logistics, M&S, intelligence, surveillance, reconnaissance, situation awareness, financial management, voice and video capabilities, big data analytics, visibility	Network security, mid-point security, cyber security architecture, endpoint security, enterprise perimeter protection capability, comply-to-connect capability, insider threat detection capability, data center security, Windows 10 security, cyber security situation awareness, end-to-end identity credential and access management, cyber security risk management, holistic security architecture, data security, block chain, cryptographic modernization,
	9. DoD C3 Modernization Strategy (2020)	PNT	5G, electro magnetic spectrum, tactical communication, satellite, public safety communications	Cloud	AI-enabled data analytics, C2, real-time situation awareness, synchronized capability, visualization	Software agility, cyber security
	10. DoD Cloud Strategy (2018)	Data tagging (standards)	-	Cloud, AI/ML analytics, data lakes/hubs, SaaS, IaaS, PaaS,	Automatic synchronization, AI and ML, data-driven decisions, C2	Cloud network security, Cloud-based cyber architecture, evergreen in security and technology, modern encryption, key management
	11. US ARMY Cloud Plan (2022)	Sensors	SD-WAN, satellite (LEO, MEO, GEO), WAN, LAN, optical links	Cloud, IaaS, PaaS, SaaS, cloud native application, robotic process automation platforms	Data-driven decisions, real-time analytics	Zero trust architecture, zero trust principles, protection of application, services, APIs, operations, and data
	12. DoD Software Modernization Strategy (2021)	-	electro magnetics spectrum	Cloud, SaaS, Software development platform	Automation	Zero trust architecture, real-time continuous risk monitoring
	13. DoD Electromagnetic Spectrum Superiority Strategy (2020)	EMS sensors, radars, electro-optics, infrared systems	Electromagnetic Spectrum, 5G, broadband, software-defined networks, RF	cloud-based data and tools, data mining and fusion capabilities	Electromagnetic Battle Management, Modeling and simulation, war-gaming , LVC (Live Virtual Construct), C2	Cybersecurity for an information sharing infrastructure
	14. DoD Data Strategy (2020)	Weapons platform, connected devices, sensors, training facilities, test ranges,business system	-	Cloud, platform of analysis and visualization	AI analytics, Situation awareness	-

After reviewing the abstracts of the extracted papers, including one duplicate paper, 364 papers were excluded from the detailed review as they were not relevant to the research topic. The remaining 233 papers underwent a domain assignment process, drawing upon both abstracts and full texts when necessary. The results of the classification into the four ICT-based military domains are summarized by three-year periods in Table 8.

Through the above process, we confirmed that all the reviewed articles were appropriately classified into the four ICT-based military domains of AI capability, cyber capability, space capability, and C4ISR. We ascertained that using the US military strategy as a basis for classifying ICT-based military capabilities is an appropriate approach and is well-aligned with the trends in academic research.

The results of this review show that the number of papers related to AI capability is increasing, while the C4ISR domain is showing a slight decline. On the other hand, C4ISR (61%) accounted for the largest proportion of all reviewed papers, followed by AI capability (15%), cyber capability (14%), and space capability (10%). We classified the reviewed papers by publisher as a reference to identify the research trends in this topic.

APPENDIX C

See Table 9.

REFERENCES

[1] Y. Chen and C.-F. Wang, "Introduction," in *Characteristic Modes: Theory and Applications in Antenna Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2015, pp. 1–35.

[2] J. R. Lindsay, "The technolgoy theory of victory," in *Information Technology and Military Powe*, vol. 1. Ithaca, NY, USA: Cornell University Press, 2020, pp. 28–54.

[3] E. B. Kania, "Artificial intelligence in China's revolution in military affairs," *J. Strategic Stud.*, vol. 44, no. 4, pp. 1–28, May 2021, doi: 10.1080/01402390.2021.1894136.

[4] U.S. Exective Office President Nat. Sci. Technol. Council. (2016). *Preparing for the Future of Aritificial Intelligence*. [Online]. Available: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

[5] U.S. Army. (2017). *The U.S. Army Robotic and Autonomous Sysems Strategy*.

[6] K. Ayoub and K. Payne, "Strategy in the age of artificial intelligence," *J. Strategic Stud.*, vol. 39, nos. 5–6, pp. 793–819, 2016.

[7] J. Johnson, "Artificial intelligence & future warfare: Implications for international security," *Defense Secur. Anal.*, vol. 35, no. 2, pp. 147–169, Apr. 2019, doi: 10.1080/14751798.2019.1600800.

[8] K. Payne, "Artificial intelligence: A revolution in strategic affairs?" *Survival*, vol. 60, no. 5, pp. 7–32, Sep. 2018, doi: 10.1080/00396338.2018.1518374.

[9] A. J. Tellis, "China's military space strategy," *Survival*, vol. 49, no. 3, pp. 41–72, Oct. 2007.

[10] A. Bousquet, "Chaoplexic warfare or the future of military organization," *Int. Affairs*, vol. 84, no. 5, pp. 915–929, Sep. 2008.

[11] J. Johnson, "Artificial intelligence: A threat to strategic stability," *Strategic Stud. Quart.*, vol. 14, no. 1, pp. 16–39, 2020.

[12] P. T. Mitchell, "The future is upon us: Failed predictions, boiling frogs, and gun printers," in *Emerging Critical Technologies and Security in the Asia–Pacific*. Cham, Switzerland: Springer, 2016, pp. 143–153.

[13] *Ministry of National Defense of Repulic of Korea, Defense Vision 2050 Summary*, 2021.

[14] C. Lawson, "Technology and the extension of human capabilities," *J. Theory Social Behaviour*, vol. 40, no. 2, pp. 207–223, Jun. 2010.

[15] E. Kapp, "Organ projecion," in *Elements of a Philosophy of Technology: On the Evolutionary History of Culture*. Minneapolis, MN, USA: U of Minnesota Press, vol. 2, 2018, pp. 68–74.

[16] D. Rothenberg, "Extension's order," in *Hand's End: Technology and the Limits of Nature*, vol. 2. Berkeley, CA, USA: Univ. of California Press, 1993, pp. 28–46.

[17] M. McLuhan, "Media as translators," in *Understanding Media: The Extensions of Man*, vol. 6. Corte Madera, CA, USA: GINGKO Press Inc, 2013, pp. 63–67.

[18] S. Steinert, "Taking stock of extension theory of technology," *Philosophy Technol.*, vol. 29, no. 1, pp. 61–78, Mar. 2016, doi: 10.1007/s13347-014-0186-3.

[19] M. C. Horowitz, "Artificial intelligence, international competition, and the balance of power," *Texas Nat. Secur. Rev.*, vol. 1, no. 3, pp. 36–57, May 2018.

[20] J. Haner and D. Garcia, "The artificial intelligence arms race: Trends and world leaders in autonomous weapons development," *Global Policy*, vol. 10, no. 3, pp. 331–337, Sep. 2019.

[21] J. Johnson, "The end of military-techno pax Americana? Washington's strategic responses to Chinese AI-enabled military technology," *Pacific Rev.*, vol. 34, no. 3, pp. 351–378, May 2021, doi: 10.1080/09512748.2019.1676299.

[22] E. B. Kania, "Chinese military innovation in the AI revolution," *RUSI J.*, vol. 164, nos. 5–6, pp. 26–34, Sep. 2019, doi: 10.1080/03071847.2019.1693803.

[23] M. C. Horowitz, L. Kahn, and C. Mahoney, "The future of military applications of artificial intelligence: A role for confidence-building measures?" *Orbis*, vol. 64, no. 4, pp. 528–543, 2020, doi: 10.1016/j.orbis.2020.08.003.

[24] B. M. Jensen, C. Whyte, and S. Cuomo, "Algorithms at war: The promise, peril, and limits of artificial intelligence," *Int. Stud. Rev.*, vol. 22, no. 3, pp. 526–550, Sep. 2020, doi: 10.1093/isr/viz025.

[25] J. Johnson, "Artificial intelligence in nuclear warfare: A perfect storm of instability?" *Washington Quart.*, vol. 43, no. 2, pp. 197–211, Apr. 2020, doi: 10.1080/0163660x.2020.1770968.

[26] J. Johnson, "Delegating strategic decision-making to machines: Dr. Strangelove redux?" *J. Strategic Stud.*, vol. 45, no. 3, pp. 439–477, Apr. 2022.

[27] M. Raska, "The sixth RMA wave: Disruption in military affairs?" *J. Strategic Stud.*, vol. 44, no. 4, pp. 456–479, Jun. 2021, doi: 10.1080/01402390.2020.1848818.

[28] A. Goldfarb and J. R. Lindsay, "Prediction and judgment: Why artificial intelligence increases the importance of humans in war," *Int. Secur.*, vol. 46, no. 3, pp. 7–50, Feb. 2022.

[29] H. Zhang, S. Li, D. Li, Z. Wang, Q. Zhou, and Q. You, "Sonar image quality evaluation using deep neural network," *IET Image Process.*, vol. 16, no. 4, pp. 992–999, Mar. 2022, doi: 10.1049/ipr2.12199.

[30] R. Ottis and P. Lorents, "Cyberspace: Definition and implications," in *Proc. Int. Conf. Cyber Warfare Secur.*, 2010, pp. 267–270.

[31] T. Rid, "Cyber war will not take place," *J. Strategic Stud.*, vol. 35, no. 1, pp. 5–32, Feb. 2012, doi: 10.1080/01402390.2011.608939.

[32] R. J. Harknett and M. Smeets, "Cyber campaigns and strategic outcomes," *J. Strategic Stud.*, vol. 45, no. 4, pp. 534–567, Jun. 2022, doi: 10.1080/01402390.2020.1732354.

[33] T. Rid and P. McBurney, "Cyber-weapons," *RUSI J.*, vol. 157, no. 1, pp. 6–13, Feb. 2012, doi: 10.1080/03071847.2012.664354.

[34] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," *Comput. Secur.*, vol. 49, pp. 70–94, Mar. 2015, doi: 10.1016/j.cose.2014.11.007.

[35] S. Kreps and J. Schneider, "Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics," *J. Cybersecurity*, vol. 5, no. 1, pp. 1–11, Jan. 2019, doi: 10.1093/cybsec/tyz007.

[36] A. Brantly and M. Smeets, "Military operations in cyberspace," in *Handbook of Military Sciences*, 2020, ch. 19, pp. 1–16.

[37] Q. AL-Durrah and S. B. Sadkhan, "Cyberwarfare techniques: Status, challenges and future trends," in *Proc. 7th Int. Conf. Contemp. Inf. Technol. Math. (ICCITM)*, Aug. 2021, p. 124.

[38] M. Kim, "R&D trend and development direction of cyber warfare weapon system technology," *J. Korea Academia-Ind. Cooperation Soc.*, vol. 23, no. 5, pp. 272–278, May 2022, doi: 10.5762/kais.2022.23.5.272.

[39] L. Maschmeyer, "A new and better quiet option? Strategies of subversion and cyber conflict," *J. Strategic Stud.*, vol. 46, no. 3, pp. 570–594, Apr. 2023, doi: 10.1080/01402390.2022.2104253.

[40] S. Zilincik and I. Duyvesteyn, "Strategic studies and cyber warfare," *J. Strategic Stud.*, vol. 46, no. 4, pp. 836–857, Jun. 2023, doi: 10.1080/01402390.2023.2174106.

[41] J. Moltz, "The changing dynamics of twenty-first-century space power," *J. Strategic Secur.*, vol. 12, no. 1, pp. 15–43, Apr. 2019, doi: 10.5038/1944-0472.12.1.1729.

[42] H. Sohn and J. Lee, "Military space strategy of the R.O.K. forces: Toward dispersal warfare beyond space area recognition," *J. Strategic Stud.*, vol. 29, no. 3, pp. 7–41, Nov. 2022, doi: 10.46226/jss.2022.11.29.3.7.

[43] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T. X. Vu, and G. Goussetis, "Satellite communications in the new space era: A survey and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 70–109, 1st Quart., 2021, doi: 10.1109/COMST.2020.3028247.

[44] J. Ferris, "A new American way of war? C4ISR, intelligence and information operations in operation 'Iraqi Freedom': A provisional assessment," *Intell. Nat. Secur.*, vol. 18, no. 4, pp. 155–174, Dec. 2003, doi: 10.1080/02684520310001688916.

[45] J. Ferris, "Netcentric warfare, C4ISR and information operations: Towards a revolution in military intelligence?" *Intell. Nat. Secur.*, vol. 19, no. 2, pp. 199–225, Jun. 2004, doi: 10.1080/0268452042000302967.

[46] T. Moon, "Net-centric or networked military operations?" *Defense Secur. Anal.*, vol. 23, no. 1, pp. 55–67, Mar. 2007, doi: 10.1080/14751790701254474.

[47] G. C. A. Mathur, M. S. K. Srivastava, and M. I. Prabu, "Leveraging technological advances in C4ISR to enhance situational awareness and decision making," *SYNERGY*, pp. 59–77, 2022.

[48] M. Raska, "The AI wave in military affairs: Enablers and constraints," in *Technological Innovation and Security: The Impact on the Strategic Environment in East Asia*, vol. 6. Tokyo, Japan: Nat. Inst. for Defense Stud., 2022, pp. 89–99.

[49] U.S. Dept. Defense. (2018). *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI To Advance Our Security and Prosperity*. [Online]. Available: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

[50] U.S. Dept. Defense. (2022). *Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathwry*. [Online]. Available: https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF

[51] U.S. Dept. Defense. (2023). *Summary of 2023 Cyber Strategy of The Department of Defense*. [Online]. Available: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

[52] U.S. Dept. Defense. (2023). *DoD Cyber Workforce Strategy 2023-2027*. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf

[53] U.S. Dept. Defense. (2022). *DoD Zero Trust Strategy*. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[54] U.S. Dept. Defense. (2020). *Department of Defense Identity, Credential, and Access Management (ICAM) Strategy*. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Cyber/ICAM_Strategy.pdf

[55] U.S. Dept. Defense. (2020). *Defense Space Strategy Summary*. [Online]. Available: https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF

[56] U.S. Dept. Defense. (2019). *DoD Digital Modernization Strategy*. [Online]. Available: https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF

[57] U.S. Dept. Defense. (2020). *C3 Modernization Strategy*. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf

[58] U.S. Dept. Defense. (2018). *DoD Cloud Strategy*. [Online]. Available: https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF

[59] U.S. Army. (2022). *The U.S. Army Cloud Plan*. [Online]. Available: https://api.army.mil/e2/c/downloads/2022/10/14/106b220e/army-cloud-plan-2022.pdf

[60] U.S. Dept. Defense. (2022). *Department of Defense Software Modernization Strategy*. [Online]. Available: https://media.defense.gov/2022/Feb/03/2002932833/-1/-1/1/DEPARTMENT-OF-DEFENSE-SOFTWARE-MODERNIZATION-STRATEGY.PDF

[61] U.S. Dept. Defense. (2020). *Department of Defense Electromagnetic Spectrum Superiority Strategy*. [Online]. Available: https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF

[62] U.S. Dept. Defense. (2020). *DoD Data Strategy*. [Online]. Available: https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF

[63] A. Kenny, *The Eudemian Ethics*. London, U.K.: Oxford Univ. Press, 2011, p. 129.

[64] R. W. Emerson, "Works and days," in *The Collected Works of Ralph Waldo Emerson, DigiCat*, 2022, p. 14958.

[65] A. C. Michalos, *Encyclopedia of Quality of Life and Well-Being Research*. Springer, 2014, pp. 974–978.

[66] W. Pitts and W. S. McCulloch, "How we know universals the perception of auditory and visual forms," *Bull. Math. Biophys.*, vol. 9, no. 3, pp. 127–147, Sep. 1947.

[67] M. Haenlein and A. Kaplan, "A brief history of artificial intelligence: On the past, present, and future of artificial intelligence," *California Manage. Rev.*, vol. 61, no. 4, pp. 5–14, Aug. 2019.

[68] Z. Davis, "Artificial intelligence on the battlefield," *Prism*, vol. 8, no. 2, pp. 114–131, 2019.

[69] D. Axe. (2023). *U.S. Air Force Sends Robotic F-16s Into Mock Combat*. Accessed: Feb. 1, 2023.

[70] ACTUV. (2023). *Prototype Transitions To Office of Naval Research for Further Development*. [Online]. Available: https://www.darpa.mil/news-events/2018-01-30a

[71] A. Ilachinski. (2023). *AI, Robots, and Swarms*. Accessed: Jan. 15, 2023. [Online]. Available: https://www.cna.org/archive/CNA_Files/pdf/drm-2017-u-014796-final.pdf

[72] A. Octavian, W. Jatmiko, A. Y. Husodo, and G. Jati, "Optimazation of defender drones swarm battle maneuver for gaining air superiority by combining artificial and human intelligence through hand gesture control system," *Int. J. Innov. Comput. Inf. Control, Article*, vol. 19, no. 2, pp. 623–636, Apr. 2023.

[73] P. Scharre, "How swarming will change warfare," *Bull. At. Scientists*, vol. 74, no. 6, pp. 385–389, Nov. 2018.

[74] C.-E. Lee, J. Baek, J. Son, and Y.-G. Ha, "Deep AI military staff: Cooperative battlefield situation awareness for commander's decision making," *J. Supercomput.*, vol. 79, no. 6, pp. 6040–6069, Apr. 2023, doi: 10.1007/s11227-022-04882-w.

[75] K. M. Sayler, "Artificial intelligence and national security," *Congressional Res. Service*, vol. 45178, 2019.

[76] J. Hao, H. Ji, H. Liu, Z. Li, and H. Yang, "Research on colorized physical terrain modeling for intelligent vehicle navigation," *Adv. Mech. Eng.*, vol. 10, no. 7, Jul. 2018, Art. no. 168781401878741, doi: 10.1177/1687814018787410.

[77] M. W. Boyce, R. H. Thomson, J. K. Cartwright, D. T. Feltner, C. R. Stainrod, J. Flynn, C. Ackermann, J. Emezie, C. R. Amburn, and E. Rovira, "Enhancing military training using extended reality: A study of military tactics comprehension," *Frontiers Virtual Reality*, vol. 3, pp. 1–9, Jul. 2022.

[78] A. K. Bojer, F. F. Woldesilassie, T. G. Debelee, S. R. Kebede, and S. Z. Esubalew, "AHP and machine learning-based military strategic site selection: A case study of adea district east shewa zone, Ethiopia," *J. Sensors*, vol. 2023, pp. 1–18, Jul. 2023, doi: 10.1155/2023/6651486.

[79] J. B. A. Bailey, "The first world war and the birth of modern warfare," in *The Dynamics of Military Revolution, 1300–2050*. Cambridge, U.K.: Cambridge Univ. Press, 2001, ch. 8, pp. 132–153.

[80] M. Canan and A. Sousa-Poza, "Integrating cyberspace power into military power in joint operations context," in *Proc. 13th Int. Conf. Cyber Warfare Secur. (ICCWS)*, 2018, pp. 92–100.

[81] W. Gibson, *Neuromancer*. Baltimore, MD, USA: Penguin, 1984, p. 51.

[82] USSTRATCOM. (2009). *He Cyber Warfare Lexicon Version 1.7.6*. [Online]. Available: https://nsarchive.gwu.edu/document/21360-document-1

[83] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," *IEEE Secur. Privacy*, vol. 1, no. 4, pp. 33–39, Jul. 2003.

[84] J. H. Schafer, "International information power and foreign malign influence in cyberspace," in *Proc. 15th Int. Conf. Cyber Warfare Secur. (ICCWS)*, 2020, pp. 423–430.

[85] J. Schneider, "The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war," *J. Strategic Stud.*, vol. 42, no. 6, pp. 841–863, Sep. 2019.

[86] W. D. Reed and R. W. Norris, "Military use of the space shuttle," *Akron Law Rev.*, vol. 13, no. 4, pp. 1–24, 1980.

[87] P. L. Hays, J. Robinson, C. Giannopapa, K.-U. Schrogl, and D. Moura, *Handbook of Space Security: Policies, Applications and Programs*. Springer, 2015, pp. 701–704.

[88] G. M. Moore, V. Budura, and J. Johnson-Freese, "Space and joint space doctrine," *Joint Force Quart.*, vol. 14, pp. 60–63, Jan. 1996.

[89] Defense One. (2024). *C4ISR: The Military's Nervous System*. [Online]. Available: https://www.defenseone.com/insights/cards/c4isr-military-nervous-system/

[90] M. Fewell and M. G. Hazen, *Network-centric Warfare: Its Nature and Modelling*. Chennai, India: DSTO Systems Sciences Laboratory, 2003, pp. 4–40.

[91] A. K. Cebrowski and J. J. Garstka, "Network-centric warfare: Its origin and future," *U.S. Nav. Inst. Proc.*, no. 1, pp. 28–35, 1998.

[92] D. S. Alberts, J. Garstka, and F. P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, DC, USA: National Defense University Press, 1999, pp. 175–180.

[93] A. Skoryk, B. Nizienko, A. Dudush, V. Shulezhko, and I. Romanchenko, "Evolution from the network-centric warfare concept to the data-centric operation theory," *Adv. Mil. Technol.*, vol. 16, no. 2, pp. 219–234, Jun. 2021, doi: 10.3849/aimt.01430.

[94] K. A. Dunkelberger, "Technologies for network-centric C41SR," in *Proc. SPIE*, Jul. 2003, pp. 111–120.

[95] W. J. Perry, "Desert storm and deterrence," *Foreign Affairs*, vol. 70, no. 4, p. 66, 1991.

[96] T. G. Mahnken and B. D. Watts, "What the Gulf war can (and cannot) tell us about the future of warfare," *Int. Secur.*, vol. 22, no. 2, p. 151, 1997.

[97] P. Sharma, K. K. Sarma, and N. E. Mastorakis, "Artificial intelligence aided electronic warfare systems-recent trends and evolving applications," *IEEE Access*, vol. 8, pp. 224761–224780, 2020, doi: 10.1109/ACCESS.2020.3044453.

[98] E. Clark and E. Zelnio, "Synthetic aperture radar physics-based image randomization for identification training: SPIRIT," in *Proc. Algorithms Synth. Aperture Radar Imag.*, Jun. 2023, p. 12520.

[99] G. R. Sullivan, J. M. Dubik, and E. H. Tilford, *War in the Information Age*. Carlisle Barracks, PA, USA: Strategic Studies Institute, 1994.

[100] W. A. Owens, *The Emerging U.S. System-of-systems, National Defense University*. Washington, DC, USA: Inst. for Nat. Strategic Stud., 1996, pp. 1–6.

[101] N. Davendralingam and D. A. DeLaurentis, "A robust portfolio optimization approach to system of system architectures," *Syst. Eng.*, vol. 18, no. 3, pp. 269–283, May 2015, doi: 10.1002/sys.21302.

[102] U.S. Army. (2021). *The U.S. Army in Multi-Domain Operations*.

[103] S. J. Townsend, "Accelerating multi-domain operations," *Mil. Rev.*, pp. 4–7, Aug. 2018.

[104] C. Richards, *Boyd's OODA Loop*, 2020, pp. 142–165.

[105] M. Raska, "Strategic competition for emerging military technologies," *Prism*, vol. 8, no. 3, pp. 64–81, 2019.

[106] T. M. Cheung, T. G. Mahnken, and A. L. Ross, "Assessing the state of understanding of defense innovation," *SITC Res. Briefs*, no. 1, pp. 1–5, 2018.

[107] M. C. Horowitz and S. Pindyck, "What is a military innovation and why it matters," *J. Strategic Stud.*, vol. 46, no. 1, pp. 85–114, Jan. 2023, doi: 10.1080/01402390.2022.2038572.

[108] E. De Angelis, A. Hossaini, R. Noble, D. Noble, A. M. Soto, C. Sonnenschein, and K. Payne, "Forum: Artificial intelligence, artificial agency and artificial life," *RUSI J.*, vol. 164, nos. 5–6, pp. 120–144, Sep. 2019, doi: 10.1080/03071847.2019.1694264.

[109] S. Bubeck, V. Chandrasekaran, R. Eldan, J. Gehrke, E. Horvitz, E. Kamar, P. Lee, Y. Tat Lee, Y. Li, S. Lundberg, H. Nori, H. Palangi, M. Tulio Ribeiro, and Y. Zhang, "Sparks of artificial general intelligence: Early experiments with GPT-4," 2023, *arXiv:2303.12712*.

[110] G. Pistilli, "What lies behind AGI: Ethical concerns related to LLMs," *Revue Ethique Et Numérique*, Mar. 2022.

[111] N. Bostrom, "Ethical issues in advanced artificial intelligence," in *Science Fiction and Philosophy: From Time Travel To Superintelligence*, Sep. 2020, pp. 69–75.

SANG JIN OH (Member, IEEE) was born in Andong-si, South Korea, in 1970. He received the bachelor's degree in electronics engineering from Hanyang University, Seoul, in 1993, and the M.B.A. degree from the University of Oregon, USA, in 2005, funded by a Korean Government Scholarship. He is currently pursuing the Ph.D. degree with Korea Advanced Institute of Science and Technology (KAIST), focusing on future military innovation.

From 1993 to 2022, he was a Civil Servant in the South Korean government. He mainly focused on promoting national digital transformation in the Ministry of Science and ICT. His role involved the development and utilization of ICT in many areas in the country. He also served as an Officer in the Republic of Korea Air Force for three years. In his final government role as a Deputy Minister, in charge of the Office of Defense Reform at the Ministry of National Defense. He planned the integration of ICT into the defense sector. He is also an industry-academia Cooperation Professor with the Department of Artificial Intelligence, Korea University, Seoul.

Mr. Oh is also a member of the Korea Information Processing Society.

SANG KEUN CHO is currently a Research Professor with the Future Institute for National Strategic Technology and Korea Advanced Institute of Science and Technology (KAIST). His current research is concerned with future warfare and revolution in military affairs. He has been in the ROK Army as a Future Planner for ten years. In particular, he is a working-level person who actually develops military strategies, operational concepts, and tactics for the future in Korea.

YONGSEOK SEO is currently an Associate Professor with the Graduate School of Future Strategy, Korea Advanced Institute of Science and Technology (KAIST). His research interest includes strategic foresight drawing on the theories of social changes. In particular, he has been working on social change and governance design that technological innovation will bring for the past two decades. His work has been published in scholarly journals, including *Futures*, *European Journal of Futures Research*, and *Technological Forecasting and Social Change*.