

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SUMY NATIONAL AGRARIAN UNIVERSITY
ECONOMICS AND MANAGEMENT FACULTY

Department of Finance, Banking and Insurance

QUALIFICATION WORK

Education degree - Master

on: **«Research on the Role and Application of Information
Systems and Technology in Conflicts»**

Completed

Liu Nian

student of

073 «Management» (EP «Administrative Management»)

Supervisor

Heyenko Mykhaylo

PhD, professor of the Department of Finance,
Banking and Insurance

Reviewer

Yatlov Serhiy

Head of «SVIDA» LLC

Sumy – 2024

ABSTRACT

Liu Nian. Research on the Role and Application of Information Systems and Technology in Conflicts.

Qualification work on specialty 073 “Management” EP “Administrative management” SNAU, Sumy 2024, Manuscript.

In this qualification work the theoretical and methodological foundations of the role and application of information systems and technology in conflicts were studied.

In the first chapter “Theoretical and Methodical Aspects of Research on the Role and Application of Information Systems and Technology in Conflicts” the evolution, concept, and essence of role and application of information systems and technology in conflicts are investigated.

Chapter two, “Research on the Role and Application of Information Systems and Technology in Conflicts”, which contains three sub-chapters, studies the typical application of information systems and technology in conflicts and civil intelligence crowdsourcing application.

Chapter three, “Develop Information Systems and Technology in Conflicts according to the research of the Institute of Intelligent Computing Information Management”, which contains two sub-chapters, proposes recommendations to development considerations for combat management.

Combat management is the foundation for winning modern wars and is at the core of modern combat systems. It involves planning, organizing, coordinating, and controlling personnel, equipment, information, resources, and time-space elements during the combat process. To delve deeper into the role and application of combat management systems in modern warfare, this paper elaborates on the concept and characteristics of combat management systems, analyzes the mechanisms of combat management systems, and proposes a classification method for combat management systems based on their scope of application. By comparing the commercial internet order service model and using the Russo-Ukrainian conflict as a case study, three typical modes of combat management system applications are analyzed, along with an examination of the use of combat management systems and kill chain construction during the conflict. As the engine for constructing military kill chains, five key technologies for developing combat management systems are proposed, including communication integration, intelligence integration, force integration, security integration, and system integration.

Keywords: Information Systems and Technology, Conflicts, Combat Management Systems, Military Internet of Things, Order Strikes, Information Security, Content Aggregation, System Integration.

АНОТАЦІЯ

Люй Ніан. Дослідження ролі та застосування інформаційних систем і технологій у конфліктах.

Кваліфікаційна робота за спеціальністю 073 «Менеджмент» ОП «Адміністративний менеджмент» СНАУ, Суми-2024 - Рукопис.

У даній кваліфікаційній роботі були вивчені теоретико-методологічні основи ролі та застосування інформаційних систем і технологій у конфліктах.

У першому розділі «Теоретико-методичні аспекти дослідження ролі та застосування інформаційних систем і технологій у конфліктах» досліджено еволюцію, концепцію та сутність ролі та застосування інформаційних систем і технологій у конфліктах.

Розділ другий «Дослідження ролі та застосування інформаційних систем і технологій у конфліктах», який містить три підрозділи, вивчає типові застосування інформаційних систем і технологій у конфліктах і застосування інформаційних систем цивільної розвідки.

У третьому розділі «Розвиток інформаційних систем і технологій у конфліктах згідно з дослідженнями Інституту управління інтелектуальною обчислювальною інформацією», який містить два підрозділи, пропонуються рекомендації щодо розвитку міркувань щодо управління бойовими діями.

Управління бойовими діями є основою для перемоги у сучасних війнах і лежить в основі сучасних бойових систем. Воно передбачає планування, організацію, координацію та контроль особового складу, обладнання, інформації, ресурсів і часово-просторових елементів під час бойового процесу. Щоб глибше заглибитися в роль і застосування систем бойового управління в сучасній війні, у цій статті докладно розглядаються концепція та характеристики систем бойового управління, аналізуються механізми систем бойового управління та пропонується метод класифікації систем бойового управління на основі їх сфери застосування. застосування. Шляхом порівняння моделі комерційної служби замовлення в Інтернеті та використання російсько-українського конфлікту як тематичного дослідження аналізуються три типові режими застосування систем управління бойовими діями, а також дослідження використання систем управління бойовими діями та побудови ланцюга вбивства під час конфлікту. В якості двигуна для побудови військових ланцюжків вбивства запропоновано п'ять ключових технологій для розробки систем управління бойовими діями, включаючи інтеграцію зв'язку, інтеграцію розвідки, інтеграцію сил, інтеграцію безпеки та інтеграцію систем.

Ключові слова: інформаційні системи та технології, конфлікти, системи бойового управління, військовий Інтернет речей, наказові удари, інформаційна безпека, агрегація контенту, системна інтеграція.

CONTENT

INTRODUCTION	7
CHAPTER 1. THEORETICAL AND METHODOLOGICAL ASPECTS OF RESEARCH ON THE ROLE AND APPLICATION OF INFORMATION SYSTEMS AND TECHNOLOGY IN CONFLICTS	11
CHAPTER 2. RESEARCH ON THE ROLE AND APPLICATION OF INFORMATION SYSTEMS AND TECHNOLOGY IN CONFLICTS	23
2.1. Typical Application of Information Systems and Technology in Conflicts	23
2.2. Civil Intelligence Crowdsourcing Application	26
2.3. Analysis GIS Art for Artillery from the Institute of Intelligent Computing Information Management	36
CHAPTER 3. DEVELOP INFORMATION SYSTEMS AND TECHNOLOGY IN CONFLICTS ACCORDING TO THE RESEARCH OF THE INSTITUTE OF INTELLIGENT COMPUTING INFORMATION MANAGEMENT	45
3.1. Key Technologies of Combat Management System	45
3.2. Development Considerations for Combat Management	56
CONCLUSIONS	60
REFERENCES	64
APPENDIXES	69

INTRODUCTION

Relevance of the topic. At the beginning of the 20th century, the concept of scientific management began to gain traction, and the military quickly applied it to combat operations. The term "combat management" first appeared in the U.S. Air Force, where combat managers within the force provided remote target indication and voice guidance to fighter jets based on radar detection. The core combat organization was referred to as the BM/C3 system (Battle Management and Command, Control, Communication). In 1946, the first electronic computer, ENIAC, was developed, and the military began using computers to store and process various data related to combat. In 1958, the U.S. military built the world's first semi-automated combat management system, the "SAGE" air defense command and control system, which, for the first time, used computers to automate parts of the information collection, processing, transmission, and command decision-making processes. In the same year, the Soviet military built the "Sky-1" semi-automated air defense command and control system. Combat management systems began to emerge on the battlefield, and human-machine collaborative decision-making gradually became the primary method of combat decision-making for commanders. During the Vietnam War's "Operation Rolling Thunder," the U.S. military commanded over 5,000 aircraft, making 1.29 million sorties and dropping 7.75 million tons of bombs, an endeavor impossible through manual command alone.

Combat management is the foundation for winning modern wars and is the core of modern combat systems. It involves the planning, organizing, coordinating, and controlling of personnel, equipment, information, resources, and space-time elements during the combat process. A combat management system refers to the command information system that supports combat management activities, including intelligence collection, information transmission, target identification, threat assessment, weapon allocation, and mission planning. It has gradually evolved with warfare and technological progress. The advent of the U.S. Air Force's Advanced Battle Management System (ABMS) has sparked widespread attention and debate in the academic

community regarding the understanding of combat management systems and their relationship with Joint All-Domain Command and Control (JADC2). Additionally, during the Russo-Ukrainian conflict, the concept of "order strike" has repeatedly captured the world's attention and become a hot topic of discussion. In essence, the realization of this combat style relies on the support of combat management systems, which act as "couplers," "dispatchers," and "accelerators." This paper provides an in-depth analysis of the concept, classification, and mechanisms of combat management systems, and, in conjunction with their usage in the Russo-Ukrainian conflict, explores their application and development in modern warfare.

The purpose of the master's work is to develop recommendations for improving the efficiency of the role and application of information systems and technology in conflicts.

According to the purpose, **the main objectives of the study** were identified:

- to investigate the theoretical and methodological aspects of the role and application of information systems and technologies in conflicts;
- to investigate the role and application of information systems and technologies in conflicts;
- to analyze the typical use of information systems and technologies in conflicts;
- to consider an application for crowdsourcing civilian intelligence;
- to analyze GIS Art for Artillery from the Institute of Intelligent Computing Information Management;
- to consider the possibilities of developing information systems and technologies in conflicts according to the research of the Institute of Intelligent Information Management;
- to study the key technologies of the combat control system;
- to develop considerations for managing combat operations.

The object of the study is Institute of Intelligent Computing Information Management.

The subject of the study is the management of the role and application of information systems and technology in conflicts.

Methods of research. The theoretical basis, scientific and methodological basis of the master's work is based on the provisions of the economic theory of enterprise management. To form the organizational and economic foundations of the management of the role and application of information systems and technology in conflicts, several modern scientific methods were used, in particular: the dialectical method of knowledge; abstract-logical (with a theoretical generalization of the essence and content of management processes); economic analysis and comparison; tabular and graphical method (to display information); formal and dialectical logic (to identify opportunities for adapting foreign experience).

The theoretical and methodological basis of the study is scientific and educational literature on the topic of research, as well as scientific periodicals, materials from scientific conferences, data from Internet sources, and statistical and analytical materials.

The scientific novelty of this research lies in its focus on the role and application of information systems and technology in conflicts.

received further development:

the research further develops the role and application of information systems and technology in conflicts. Combat management is one of the critical links in aggregating individual elements to form a complex combat system and achieve systemic combat capabilities.

improved:

combat management as the foundation for winning modern wars and is at the core of modern combat systems. It involves planning, organizing, coordinating, and controlling personnel, equipment, information, resources, and time-space elements during the combat process. To delve deeper into the role and application of combat management systems in modern warfare, this paper elaborates on the concept and characteristics of combat management systems, analyzes the mechanisms of combat management systems, and proposes a classification method for combat management systems based on their scope of application.

The practical significance of the results is: by comparing the commercial internet order service model and using the Russo-Ukrainian conflict as a case study,

three typical modes of combat management system applications are analyzed, along with an examination of the use of combat management systems and kill chain construction during the conflict. As the engine for constructing military kill chains, five key technologies for developing combat management systems are proposed, including communication integration, intelligence integration, force integration, security integration, and system integration.

The structure and scope of work. Master's thesis consists of an introduction, three chapters, conclusions, and proposals list of references with **49** titles. The main text posted on the **69** pages of computer text, the work contains **16** figures.

CHAPTER 1

THEORETICAL AND METHODOLOGICAL ASPECTS OF RESEARCH ON THE ROLE AND APPLICATION OF INFORMATION SYSTEMS AND TECHNOLOGY IN CONFLICTS

At the beginning of the 20th century, the concept of scientific management began to gain traction, and the military quickly applied it to combat operations. The term "combat management" first appeared in the U.S. Air Force, where combat managers within the force provided remote target indication and voice guidance to fighter jets based on radar detection. The core combat organization was referred to as the BM/C3 system (Battle Management and Command, Control, Communication). In 1946, the first electronic computer, ENIAC, was developed, and the military began using computers to store and process various data related to combat. In 1958, the U.S. military built the world's first semi-automated combat management system, the "SAGE" air defense command and control system, which, for the first time, used computers to automate parts of the information collection, processing, transmission, and command decision-making processes. In the same year, the Soviet military built the "Sky-1" semi-automated air defense command and control system. Combat management systems began to emerge on the battlefield, and human-machine collaborative decision-making gradually became the primary method of combat decision-making for commanders. During the Vietnam War's "Operation Rolling Thunder," the U.S. military commanded over 5,000 aircraft, making 1.29 million sorties and dropping 7.75 million tons of bombs, an endeavor impossible through manual command alone.

Combat management is the foundation for winning modern wars and is the core of modern combat systems. It involves the planning, organizing, coordinating, and controlling of personnel, equipment, information, resources, and space-time elements during the combat process. A combat management system refers to the command information system that supports combat management activities, including intelligence collection, information transmission, target identification, threat assessment, weapon

allocation, and mission planning. It has gradually evolved with warfare and technological progress. The advent of the U.S. Air Force's Advanced Battle Management System (ABMS) has sparked widespread attention and debate in the academic community regarding the understanding of combat management systems and their relationship with Joint All-Domain Command and Control (JADC2). Additionally, during the Russo-Ukrainian conflict, the concept of "order strike" has repeatedly captured the world's attention and become a hot topic of discussion. In essence, the realization of this combat style relies on the support of combat management systems, which act as "couplers," "dispatchers," and "accelerators." This paper provides an in-depth analysis of the concept, classification, and mechanisms of combat management systems, and, in conjunction with their usage in the Russo-Ukrainian conflict, explores their application and development in modern warfare.

The concept of Battle Management (BM) originated from the U.S. military, but to this day, no standardized definition exists. Instead, the term is explained in various field manuals across different domains. In the U.S. military's "Air and Missile Defense Operations Manual", battle management is defined as [1] "the management of combat activities in the operational environment based on appropriate authorization, commands, directives, and guidance." The U.S. military's "Electronic Warfare Operations Manual" defines Electromagnetic Battle Management (EMBM) as [2] "the dynamic monitoring, assessment, planning, and management of joint electromagnetic spectrum operations to support the commander's maneuver plan." The "Military Management Science published by the Military Science Press [3] states that "battle management is the process of planning, organizing, commanding, coordinating, and controlling combat forces, combat actions, and the battlefield to ensure the smooth execution of operations and effectively allocate and utilize various combat resources."

This definition clarifies the objectives, content, and elements of combat management. In this paper, we propose that the core of combat management revolves around building a reliable and efficient kill chain or kill web. By means of planning, organizing, coordinating, commanding, and controlling, combat management integrates sensor platforms, command platforms, weapon platforms, and support resources into a

cohesive system that can optimally perform combat operations to achieve mission objectives [4].

Combat management is the product of an organic combination of command and control science with information technology. Its evolutionary stages are closely related to the combat doctrines and information technologies of their respective eras. With the continuous development of communication, computing, and other information technologies, as well as the evolution of combat doctrines and warfare styles, combat management has gone through several stages of development: from weapon-centric to platform-centric, and finally to network-centric [2].

Combat management first appeared in the 1960s, introduced and implemented by the U.S. Air Force. It was used to support ground commanders by providing remote target indication, voice guidance, and other instructions to combat aircraft based on networked early warning radar information, assisting pilots in detecting and striking targets before the enemy. The functionality of the systems during this phase was relatively simple, focusing on providing external guidance data to combat weapons. The information-firepower coupling was low, reflecting the characteristic of being weapon-centric.

To meet the need for comprehensive defense capabilities that could simultaneously counter large-scale attacks from combat aircraft, anti-ship missiles, and other multi-directional threats, the U.S. Navy developed the "Aegis" combat management system in the late 1960s. This system achieved integrated, comprehensive coordination of shipborne phased array radar, missiles, launch systems, and electronic warfare equipment, enabling the detection, tracking, identification, and engagement of hundreds of targets in a very short time, thereby effectively conducting sea-based air defense and missile defense operations. During this phase, the system focused on independent platforms, such as ships, integrating and controlling all combat elements and equipment resources within the platform. The information-firepower coupling within the platform was highly integrated, reflecting the characteristic of being platform-centric.

Since the 1990s, combat management has been widely applied in U.S. missile

defense systems. The U.S. developed the Ground-Based Midcourse Defense (GBMC3) system and the Command and Control, Battle Management, and Communications (C2BMC) system, which effectively integrated ground-based, sea-based, and space-based combat units dispersed globally. These systems coordinated combat planning and interception strategies, allocating optimal sensor, weapon, and command-control resources in the shortest possible time, significantly enhancing the effectiveness of the ballistic missile defense system and achieving combat capabilities beyond those of individual systems. In this phase, the system efficiently integrated widely distributed sensors and weapon systems through a network to form an organic whole. The information-firepower coupling was highly integrated, reflecting the characteristic of being network-centric.

From the development process outlined above, it is clear that the most prominent and widespread application of combat management is in aerospace defense operations. This is mainly due to the high time-sensitivity of aerospace defense, which involves rapid responses to enemy combat actions after they are initiated. The defensive nature of the tasks, the compressed time and space of engagements, and the need for real-time situational awareness, impromptu planning, and closed-loop precision links impose higher demands than offensive tasks, which emphasize the art of command. The scientific application of combat equipment and the development of highly automated, information-firepower-integrated combat management systems are particularly well-suited to this context. Combat management systems enable the organic integration and unified coordination of battlefield resources such as sensors and intercept weapons, ensuring the maximization of the overall combat effectiveness of limited defense resources.

Timely and precise command and control of combat operations, along with decisive and swift decision-making, have always been the goals and aspirations of commanders throughout different periods of warfare. Before the advent of scientific management, the concept of combat management did not exist in warfare, and naturally, there were no combat management systems. However, rudimentary forms of combat management activities and systems have always coexisted with warfare, evolving and

developing together. With the invention of the telegraph, telephone, and radio, the long-distance, rapid transmission of combat orders and battlefield information became a reality, expanding the scope of combat management from a two-dimensional plane to a three-dimensional space. The once mythic notion of “strategizing from afar and achieving victory thousands of miles away” became feasible. Of course, traditional battlefield management methods did not entirely lose their relevance.

Combat management essentially employs the logic of combat mission planning. In essence, it targets the combat mission, constrained by the dynamic battlefield environment, relying on the military Internet of Things (IoT). Based on overall military values, it uses methods such as inferential analysis, rule matching, or real-time calculations to optimize the allocation of various battlefield resources, thereby forming the optimal immediate kill chain.

Taking aerospace defense as a typical application example, from the forward design perspective of “combat research – system design – model application – system integration,” the functional characteristics of combat management can be distinguished from traditional command information systems. Aerospace defense operations, particularly long-range strategic ballistic missile defense, represent a typical problem of defending against long-range, rapid strike weapons. The most significant challenge is the vast engagement space, spanning thousands or even tens of thousands of kilometers, while engagement time is extremely short. This imposes extremely high demands on the construction of the aerospace defense system. Specifically, based on the profile of aerospace defense missions, combat management has the following characteristics:

Aerospace defense operations face multiple threats, including aerodynamic targets, ballistic missiles, and near-space weapons, with unpredictable attack directions and a variety of types and ranges. At the same time, defensive operations demand high precision and real-time information, and countermeasures like electromagnetic interference and decoys can consume substantial equipment resources. It is necessary to integrate and coordinate multiple types of equipment to manage information, firepower, command communication, and other operational resources to meet the highly real-time and strong-counteraction demands of aerospace defense.

Current and future aerospace threats extensively use measures such as ultra-low stealth, electromagnetic interference, escorting decoys, and concentrated fire attacks, creating complex, high-speed, dense, and intermittent threat scenarios. To effectively support interception operations, complex aerial situations must be processed and updated in a sub-second timeframe under strong interference conditions. By using a combination of decision-level and feature-level identification methods, the system can eliminate decoys and confirm real threats, forming an engagement-level situation that meets the requirements for identification probability and interception accuracy.

The compressed time and space of aerospace defense engagements demand extreme time sensitivity, often requiring response times in seconds, making human command ineffective. To fully leverage the advantages of automated information systems, scientific models, rule-based plans, and experiential knowledge must be integrated into the combat management system. This enables the real-time formation and updating of engagement sequences and combat rules, assisting commanders in completing engagement tasks in sequence, supporting automatic analysis, real-time decision-making, and intelligent resource allocation.

Practice shows that networked combat is an advanced tactical method to effectively respond to complex battlefield environments and expand system capabilities. This is an advanced application of combat management systems. To maximize the effectiveness of networked combat, the combat management system is integrated with controlled equipment to support the dynamic combination of sensors, control nodes, and firepower elements, as well as the dynamic closure of precision chains. This ensures that command relationships can be adjusted as needed, and system functions can be dynamically reorganized, ensuring seamless coordination and combat management.

Aerospace defense operations require extremely high interception probabilities. Since a single type of weapon system has limited interception attempts and probabilities, it is necessary to develop reasonable interception strategies and implement segmented, multi-layered interceptions during different phases of the target's flight, increasing interception opportunities and ensuring higher interception rates. Based on unified combat effects, aerospace defense targets are tracked and intercepted in stages, with

close coordination throughout the combat process. To achieve this, it is essential to deeply integrate cross-domain combat equipment and implement flat control, ensuring the efficient operation of the aerospace defense equipment system.

Thus, it can be argued that the core of battle management is operational mission planning. Traditional operational planning focuses on firepower and actions, while battle management centers on planning the kill chain. In peacetime, the focus is on accumulating data, refining rules, and perfecting algorithms; during wartime, the focus shifts to constructing the kill chain based on battlefield assessments. Across different operational domains, there are significant disparities in troop deployment speeds and attack velocities.

A simple example can illustrate how a kill web functions. For instance, an Air Force F-35 fighter jet flying at high altitude detects an enemy tank convoy advancing toward an Army position on the ground below. The Army has short-range weapons capable of engaging the tanks, but if it follows a single-domain kill chain, the Army could only attack when the tanks are in very close proximity. A Navy destroyer equipped with cruise missiles is stationed a few miles offshore. In a kill web, the F-35 pilot would send targeting data from his radar screen to the destroyer's combat system, uploading the tank's coordinates into the missile. The pilot then controls the missile launcher, remotely launching the cruise missiles from the ship to strike the enemy tanks threatening the Army. In other words, the F-35 pilot can use Navy weapons to attack targets threatening the Army.

However, integrating kill chains into a kill web is no simple task due to the unique characteristics, needs, platforms, and weapons of each operational domain. In the military, this vertical structure is referred to as a "silo," meaning each problem is solved within a specific domain using domain-specific solutions. To achieve a kill web, the inherent barriers between services must be overcome.

1) Technical Barriers: There is insufficient interoperability between operational domains. When different military branches designed their systems, they didn't foresee integration into a unified kill web. Challenges arise from intelligence systems, command systems, and weapons systems being incompatible with one another.

2) Conceptual Barriers: It's unclear how kill chains should be integrated. Completely dismantling service-specific boundaries is unrealistic, and trying to coordinate and overlap kill chains with different natures and paces could lead to conflicts rather than enhancements.

3) Practical Barriers: The "service-centric" mindset still prevails in the military. Each service is reluctant to give up control over its domain and doesn't want funds intended for its own branch to be used for joint initiatives.

As a result, the development from kill chains to a fully operational kill web is still in progress.

The relationship between battle management (BM) and command and control (C2) has long been debated. Two primary viewpoints exist:

1. BM encompasses C2: Some argue that the Joint All-Domain Command and Control (JADC2) system is an important part of the Advanced Battle Management System (ABMS). This perspective highlights that battle management's five key elements include command decisions (planning) and command control, while also emphasizing activities like organization and coordination. Various foreign military battle management systems integrate command control and decision-making systems, suggesting that BM inherently includes C2.

2. ABMS as a technical enabler of C2: Others believe that the ABMS is merely a technical means for achieving all-domain C2. In this view, the BM system serves as the information infrastructure for C2 systems, providing data flow and computational support for C2 functions.

BM systems have evolved through weapon-centric, platform-centric, network-centric, and system-centric phases. Modern BM systems can process inputs from multi-domain sensors, generate real-time operational pictures, and automatically command and control forces and equipment. For instance:

Israel's "Dominant" BM System: This system connects individual soldier's digital devices with tactical units for real-time situational awareness and C2 data.

U.S. Navy's Aegis Combat System: It integrates air defense and missile defense capabilities, combining phased-array radar, command decisions, and weapons control.

NATO's ACCS-LOC1 System: Deployed in a distributed network, it integrates various radar types and interfaces to handle mission planning and combat supervision for air operations.

Since the Gulf War, the U.S. has reduced the time from sensor information collection to weapons engagement from 24 hours to 2.5 minutes, demonstrating the increasing efficiency of BM systems.

Rather than focusing on the semantic relationship between BM and C2, it is more useful to see BM as a concept and model that represents the future of C2. In fact, BM could be viewed as the evolution of traditional C2. The focus should therefore be on the differences between traditional C2 and BM in terms of concepts and models, and how C2 systems can evolve into BM systems.

BM systems are rapidly evolving into distributed operating systems, designed to collect and process sensor data, integrate various information channels, and generate operational assessments and decisions. These systems aim to optimize the OODA loop (Observe, Orient, Decide, Act) by accelerating the cycle from battlefield awareness to weapons engagement.

The main difference between traditional C2 and modern BM systems lies in their technological infrastructure:

- C2 is based on a command information internet.
- BM operates on a military resource Internet of Things (IoT).

Additional differences between traditional C2 and BM include:

1. Real-time, dynamic battlefield awareness: BM systems emphasize real-time awareness and decision-making, whereas C2 often operates with delayed information.
2. Automated decision-making: BM systems incorporate artificial intelligence and predictive algorithms to automate portions of decision-making and operational planning.
3. Resource integration: BM systems can integrate resources across multiple domains, unlike traditional C2, which is often domain-specific and soloed.

BM can be seen as a comprehensive evolution of C2, with its focus on integrating multi-domain resources, automating decision processes, and optimizing real-time

combat effectiveness.

This paper argues that the primary purpose of any military information system is to support combat operations. Therefore, there is no need to overly focus on the relationship between Battle Management (BM) and Command and Control (C2). BM should be understood more as a concept and model, and it can even be seen as the direction of development for C2. Based on this understanding, the focus should be on examining the differences in concepts and models between traditional C2 and BM, and on researching how to evolve C2 systems into BM systems.

Battle management systems widely use technologies such as situational assessment and prediction, operational spatiotemporal analysis, real-time online planning, combat resource management, and battle management engines. They employ an information technology-based architecture that integrates "cloud + network + edge" components.

In fact, the primary difference between traditional Command and Control (C2) and Battle Management (BM) models is that the former is based on command information networks, while the latter relies on military resource networks. Besides this, the differences between BM and traditional C2 models mainly include:

1. Comprehensive Management: Managing not only internal assets but also the environment and adversaries, encompassing information, electromagnetic, and energy management.
2. Deep Management: Employing an integrated approach with coordinated methods, aiming for closed-loop systems, including platforms, weapons, and controls.
3. Flexible Management: Featuring adaptability and variability, along with automation and intelligence.
4. Rapid Management: Focusing on time-sensitive targets, using information-driven and time-priority models and criteria.
5. Routine Management: Integrating combat, testing, and training into a unified system for comprehensive management of tests, training, and engagements.

The U.S. military pioneered the use of information technology to develop the C4ISR system, integrating Command, Control, Computers, Communications,

Intelligence, Surveillance, and Reconnaissance, which laid the foundation for battle management systems. During the Afghanistan War, the C4ISR system achieved near-real-time transmission of operational information to combat platforms for the first time. With the continuous advancement of sensors, networks, and artificial intelligence, technologies such as intelligent situational understanding and prediction, intelligent information push, intelligent task planning, intelligent collaborative control, intelligent rapid reconfiguration, and intelligent parallel command are increasingly impacting battle management systems. These systems typically support functions such as situational awareness, task planning, engagement management, communication, modeling, simulation, and analysis, and training.

For example, a missile defense battle management system mainly includes functions for command and control, engagement management, and communication. The command and control function enables pre-combat planning and situational awareness; the engagement management function supports combat decision-making, allocation of missile defense weapons, and task completion; the communication function facilitates the transmission and sharing of intelligence and data among various missile defense units.

Battle management systems are complex, open systems. The structure of the system determines its functionality, with different structures leading to different functional expansions. For instance:

- A ship's self-defense battle management system provides robust self-defense capabilities through automated weapon control orders, collaborative engagement management systems, and tactical data links.
- An electromagnetic battle management system enhances electromagnetic spectrum planning, sharing, and maneuvering capabilities by integrating and displaying battlefield electromagnetic spectrum data.
- A soldier's battle system integrates individual protection, combat weapons, and communication equipment, enhancing mobility, support, lethality, and survivability.

As battle management systems continue to evolve, their scope and connotation also change. Currently, typical battle management systems can be classified into the

following three categories based on their application scope:

1. Specialized Systems (Small Concept): These are systems tailored for specific platforms or domains. Examples include:

Aegis Combat System (ACS): Manages the Aegis-equipped ship's air defense, missile defense, anti-submarine warfare, anti-ship operations, and electronic warfare actions, including information fusion, identification, threat assessment, interception prioritization, and weapon control.

Battle Management, Command, Control, and Communications (BMC3): Used to instantiate real-time engagement procedures or “kill chains” in missile defense.

2. General-purpose Systems (Medium Concept): These systems are cross-platform and cross-service. Examples include:

Theater Battle Management Core System: Integrates and coordinates the use of air combat forces across the Army, Navy, and Air Force from the perspectives of intelligence, planning, command, communication, and support.

Suter System: Integrates intelligence, surveillance, reconnaissance, cyber warfare, electronic warfare, and firepower into a cohesive system through information, electromagnetic, and energy management.

3. Universal Systems (Large Concept): These are wide-area, foundational information infrastructures based on military IoT. Examples include:

Advanced Battle Management System (ABMS): Develops a distributed open architecture with components like cloudONE, dataONE, crossDomainONE, OmiaONE, radioONE, and apertureONE to achieve communication, data, situational, security, and application integration. The goal is to achieve a unified air force, joint forces, and alliance, providing the network information “foundation” for Joint All-Domain Command and Control (JADC2).

CHAPTER 2

RESEARCH ON THE ROLE AND APPLICATION OF INFORMATION SYSTEMS AND TECHNOLOGY IN CONFLICTS

2.1 Typical Application of Information Systems and Technology in Conflicts

Typical commercial internet order-based service models can be categorized into the following three types:

1) Self-Service Model.

Example: Bike-sharing services.

Description: Customers find and use bikes by scanning a QR code themselves.

Advantages: Immediate access and use, with no intermediaries, leading to fast service.

Disadvantages: Limited options in terms of bike types, availability, and quality. In remote areas or during peak times, finding an available bike may be difficult.

2) Order-Based Model

Example: Food delivery services like Meituan.

Description: Customers select dishes, place orders online, and receive deliveries from couriers. They can provide feedback on the service.

Advantages: Choice of preferred restaurants and dishes.

Disadvantages: Multiple steps involved, longer wait times as promised by the merchant, and the need to place orders well in advance to ensure timely delivery.

3) Adaptive Model

Example: Ride-hailing services like Didi.

Description: Users provide their departure and destination locations along with vehicle preferences. The management system automatically dispatches a nearby driver to meet the customer's needs.

Advantages: Convenient and fast service.

Disadvantages: During special periods such as the Spring Festival or in congested

areas, wait times may be extended, and sometimes no vehicles may be available.

Military strike chain management differs from commercial order management in the following ways:

1) High Counteractivity: Military resources are often heavily depleted during combat, making high resistance a norm.

2) High Dynamics: Mission tasks, strike targets, and operational environments frequently change.

3) High Complexity: Task allocation often involves multidimensional, constrained, and nonlinear planning problems. Traditional solving methods may not yield optimal solutions.

4) Global Constraints: Task allocation must align with overarching military values to avoid local optimizations that lead to winning battles but losing the campaign.

Comparing to commercial internet order service models, military internet order services can also be classified into three types:

1) Designated Model

Description: Based on a fixed strike chain, with pre-planned strategies and manual command modes used for attacking predetermined targets.

2) Order-Based Model

Description: Based on a temporary strike chain, with on-the-fly planning and semi-automated command modes used for attacking opportunistic targets.

3) Summon Model

Description: Based on a random strike chain, with online planning and automated command modes primarily used for attacking time-sensitive targets.

The Russia-Ukraine conflict has demonstrated a novel style of order-based strikes, supported by new command and information systems developed by Western nations and Ukraine. This section selects several of these systems and provides a summary analysis based on open-source information.

Key Systems and Their Utilization.

1. Western Command and Control Systems

Description: Western nations have developed advanced command and control

systems that integrate various data sources and operational tools to enhance battlefield effectiveness. These systems often feature real-time data processing, automated decision-making processes, and seamless communication capabilities.

Examples:

NATO's Integrated Air and Missile Defence (IAMD): Utilized for comprehensive air and missile defense, providing real-time situational awareness and coordination across multiple domains.

US Army's Tactical Command System (TCS): Supports command and control functions in real-time, facilitating the management of forces and resources in complex operational environments.

2. Ukrainian Command and Control Innovations

Description: Ukraine has leveraged Western technologies and developed its own systems to enhance its operational capabilities. These innovations focus on integrating real-time intelligence, improving communication networks, and enhancing strike coordination.

Examples:

Ukrainian ISR Systems: Employ drones and satellite imagery to provide detailed reconnaissance and intelligence, feeding information into a centralized command system for timely decision-making.

Artillery Coordination Systems: These systems enable precise targeting and coordination of artillery strikes, incorporating real-time data from various sources to maximize effectiveness.

Analysis of Kill Chain Construction:

1. Integration of Sensors and Data Sources

Mechanism: Modern systems integrate multiple sensors (drones, satellites, reconnaissance aircraft) to provide a comprehensive picture of the battlefield. This integration allows for the rapid identification and tracking of targets.

Impact: Enhances situational awareness and enables more accurate and timely targeting decisions.

2. Automated Decision-Making

Mechanism: Utilizes algorithms and machine learning to process data and generate actionable insights. Automated systems can suggest optimal strike options based on real-time data.

Impact: Reduces decision-making time and increases the accuracy of strike planning.

3. Real-Time Communication and Coordination

Mechanism: Ensures that all relevant units and command centers are updated with the latest information and can coordinate their actions effectively. Advanced communication systems facilitate the seamless exchange of data.

Impact: Improves the efficiency of operations and enhances the ability to respond quickly to changing battlefield conditions.

4. Dynamic Adaptation and Flexibility

Mechanism: Systems are designed to adapt to evolving threats and operational requirements. Flexibility is achieved through modular design and the ability to reconfigure resources dynamically.

Impact: Enables rapid adjustments to strategies and tactics in response to new intelligence or changes in the operational environment.

The use of advanced command and control systems in the Russia-Ukraine conflict illustrates a significant evolution in modern warfare. By integrating real-time data, automating decision-making processes, and enhancing communication and coordination, these systems have reshaped how military operations are conducted, leading to more precise and effective strike capabilities.

2.2 Civil Intelligence Crowdsourcing Application

After the outbreak of the Russia-Ukraine conflict, Mikhail Fedorov, Ukraine's Deputy Prime Minister and a millennial, quickly led the Ministry of Digital Transformation in developing a crowdsourcing intelligence application based on the Telegram chatbot called "e-Enemy" (also known as eVororog or eBopor). He encouraged the Ukrainian public to download the app extensively, allowing them to upload real-time

information and location data of Russian troops captured by their smartphones. This information was then used by the Ukrainian military to identify and target Russian forces.

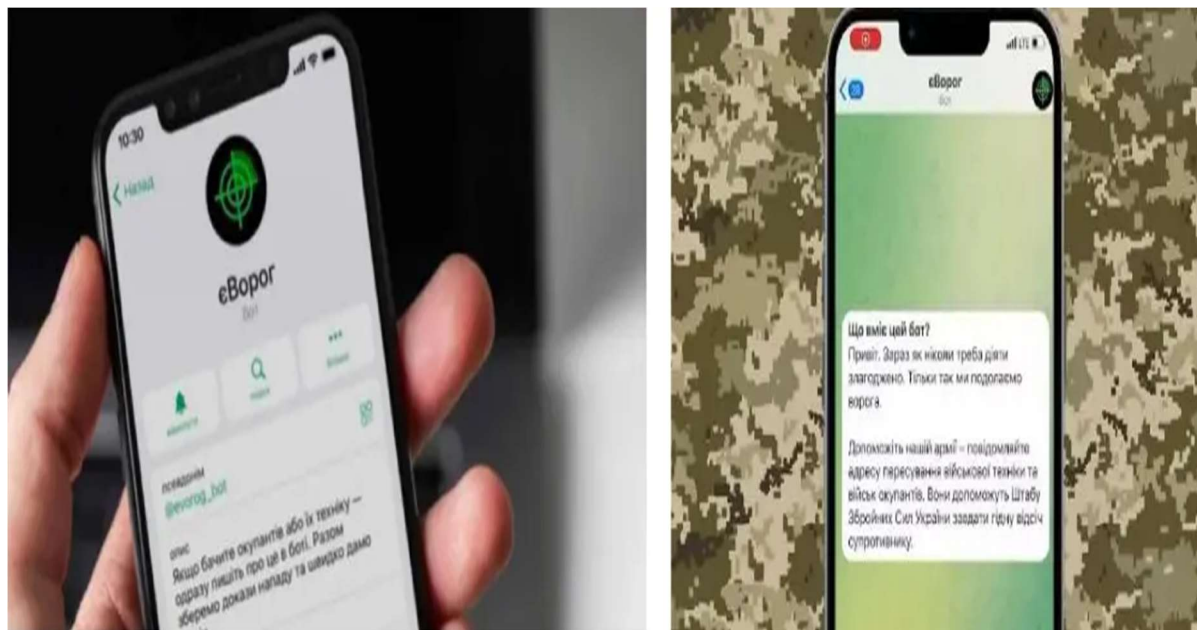


Figure 2.1 – Ukrainian intelligence crowdfunding app

Source: formed by the author

The app allows users to report events (such as Russian armored convoys on the move), location coordinates, precise timestamps, event categories (such as personnel, equipment), urgency levels marked by color, and to provide links to images or videos.

With a total population of only 41.9 million, Ukraine's app has been downloaded up to 40 million times. As of April 28, 267,000 Ukrainians had submitted data through the platform, with an average of 2,000 reports of Russian troop positions received daily. This real-time intelligence has helped the Ukrainian military to kill over 16,000 Russian troops and destroy more than 4,000 military vehicles, plunging Russian forces into what is termed a "people's war." This mode of operation is likened to a "Didi Chuxing" model - order (providing intelligence), service (conducting strikes), and settlement (reporting damage) - or a "Meituan delivery" model, where the Ukrainian military acts like delivery personnel, receiving orders (target intelligence), delivering (launching portable missiles), and confirming receipt (documenting damage).

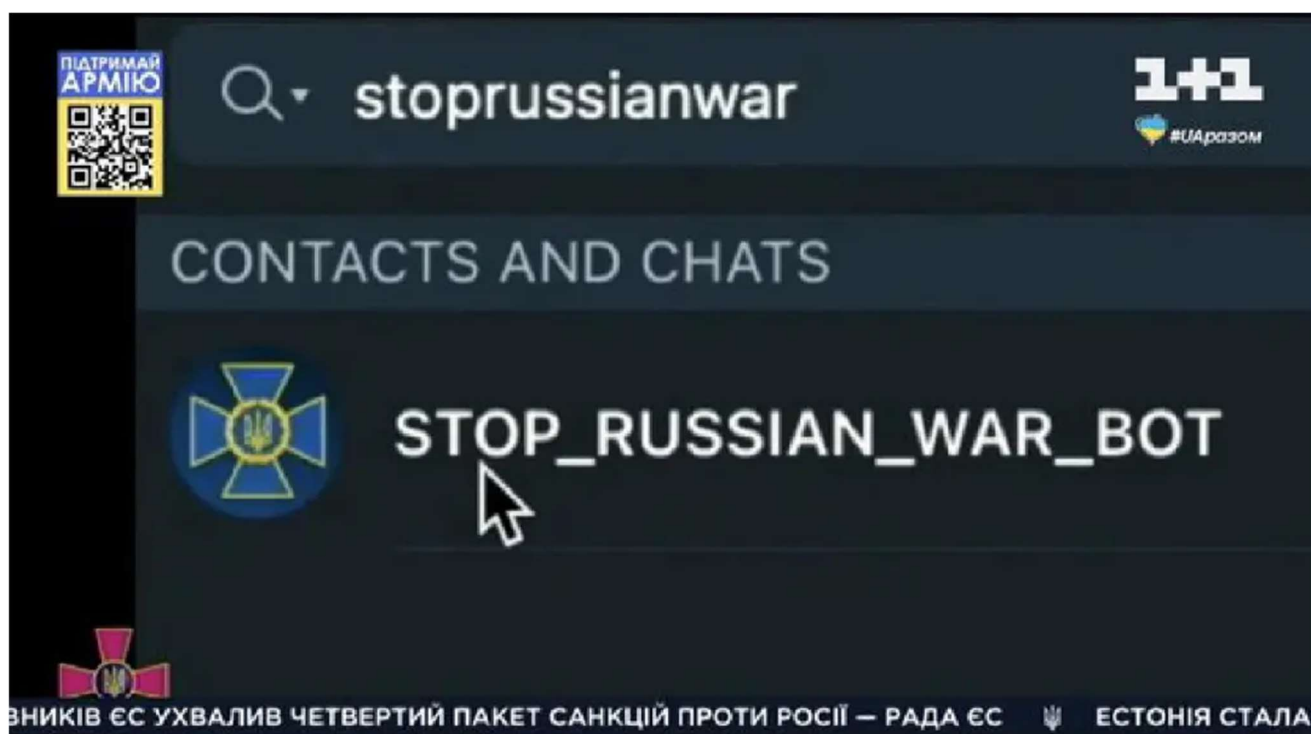
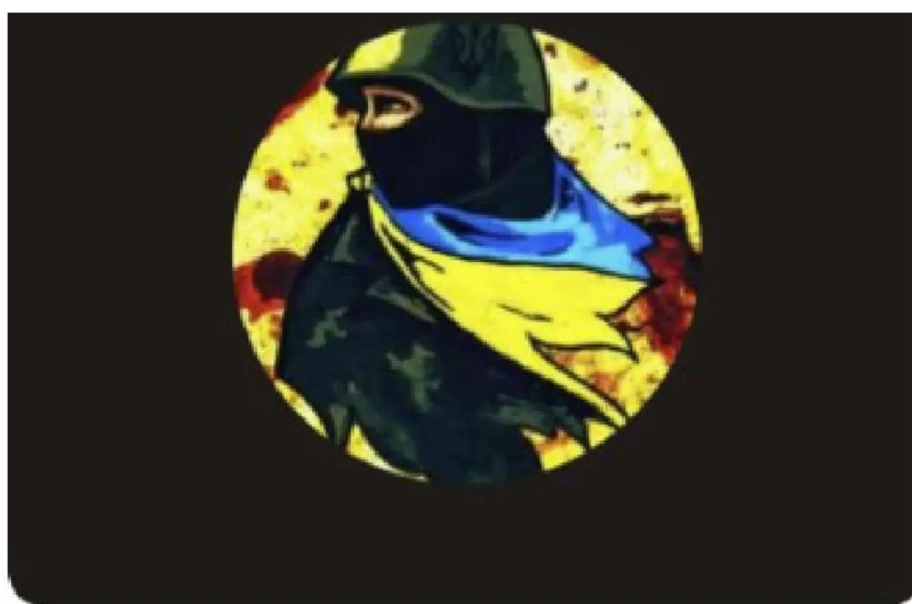


Figure 2.2 – “stop_russian_war”app

Source: formed by the author



Народний месник
@ukraine_avanger_bot

Figure 2.3 – “ukraine_avanger”app

Source: formed by the author

Additionally, Ukraine has developed chatbots such as “Stop Russian War” (@stop_russian_war_bot), “Ukraine Avenger” (@ukraine_avanger_bot), and “Air Alert” (Повітряна тривога), which similarly provide platforms for Ukrainian citizens to report Russian troop movements via their smartphones.

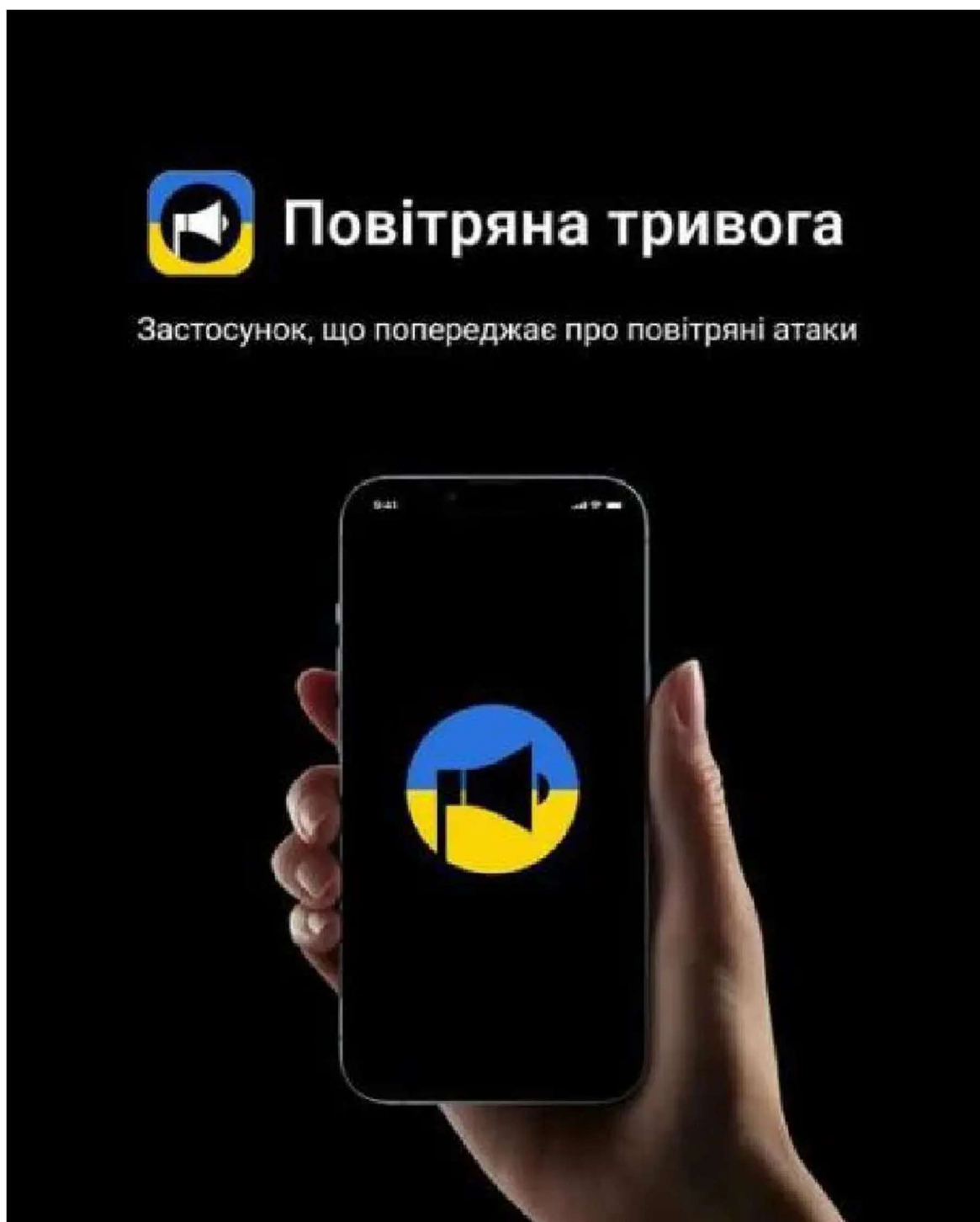


Figure 2.4 – “Air Alert” app

Source: formed by the author

On May 16, 2022, Colonel Paul Weizer, the Digital Applications Executive for U.S. Special Operations Forces, revealed at a U.S. Special Operations Command (USSOCOM) industry conference that the U.S. Department of Defense had provided the Android Tactical Assault Kit (ATAK) to the Ukrainian military. This tool was used by Ukrainian reconnaissance teams to quickly establish reconnaissance networks and provide commanders with real-time battlefield situational awareness.



Figure 2.5 – 5Android tactical assault kit

Source: formed by the author

ATAK was initially developed by the U.S. Air Force Research Laboratory (AFRL) in 2010. The software, which has evolved through various versions, is widely used by the U.S. Armed Forces, including Special Operations Forces and other military units across the Army, Navy, and Air Force. It has also been applied in civilian scenarios such as disaster response and rescue operations. As of now, ATAK has approximately 40,000 Department of Defense (DoD) users and 32,000 non-federal users. The software is considered a "game-changer" and has advanced to version 2.6.

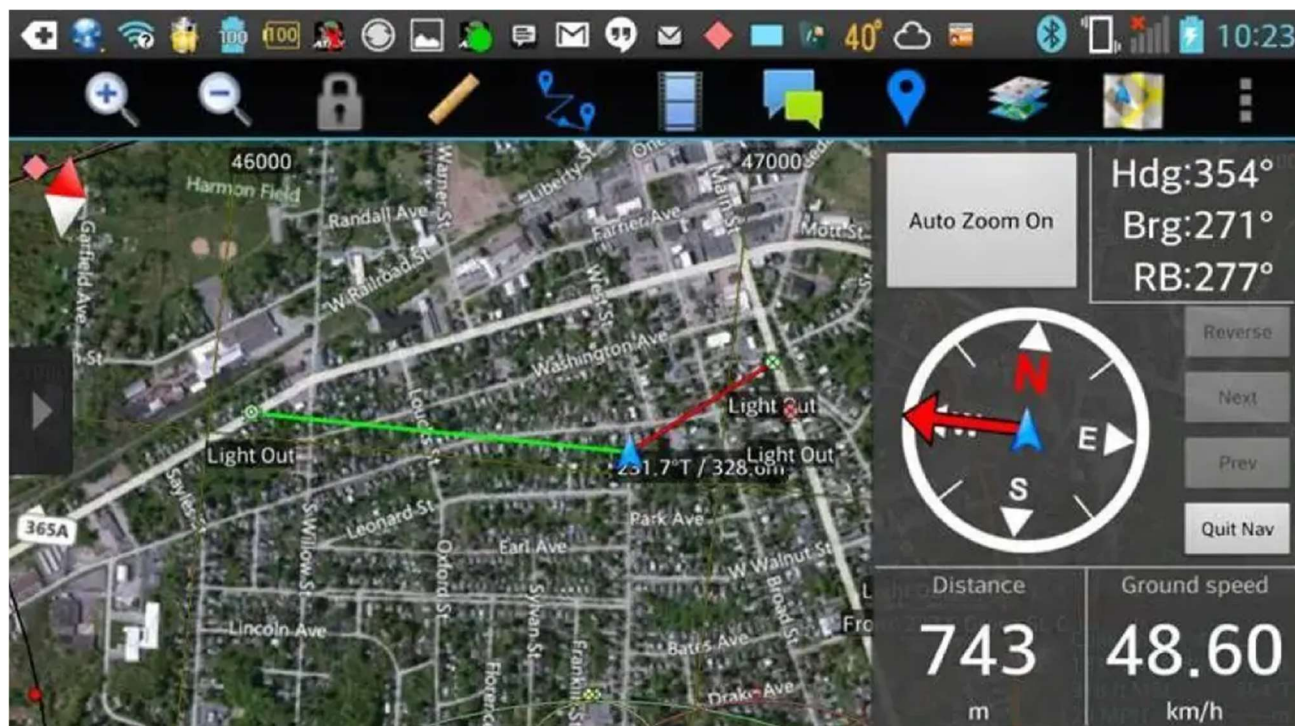


Figure 2.6 – Interface of Android tactical assault kit

Source: formed by the author

Components of the Tactical Assault Kit (TAK).

The Tactical Assault Kit (TAK) is a multi-platform, map-based situational awareness software suite. It includes:

- ATAK: Designed for Android operating systems.
- WinTAK: For Windows operating systems.
- iTAK: For iOS operating systems.
- TAK Server: Runs on Linux operating systems.
- AR TAK: Augmented Reality Head-Up Display.
- vTAK: Professional-grade Virtual Reality (Vive Pro).
- WebTAK: Web browser-based interface.

These applications provide tactical support for military, federal government, and emergency response operations, enabling rapid response and situational awareness in critical situations.

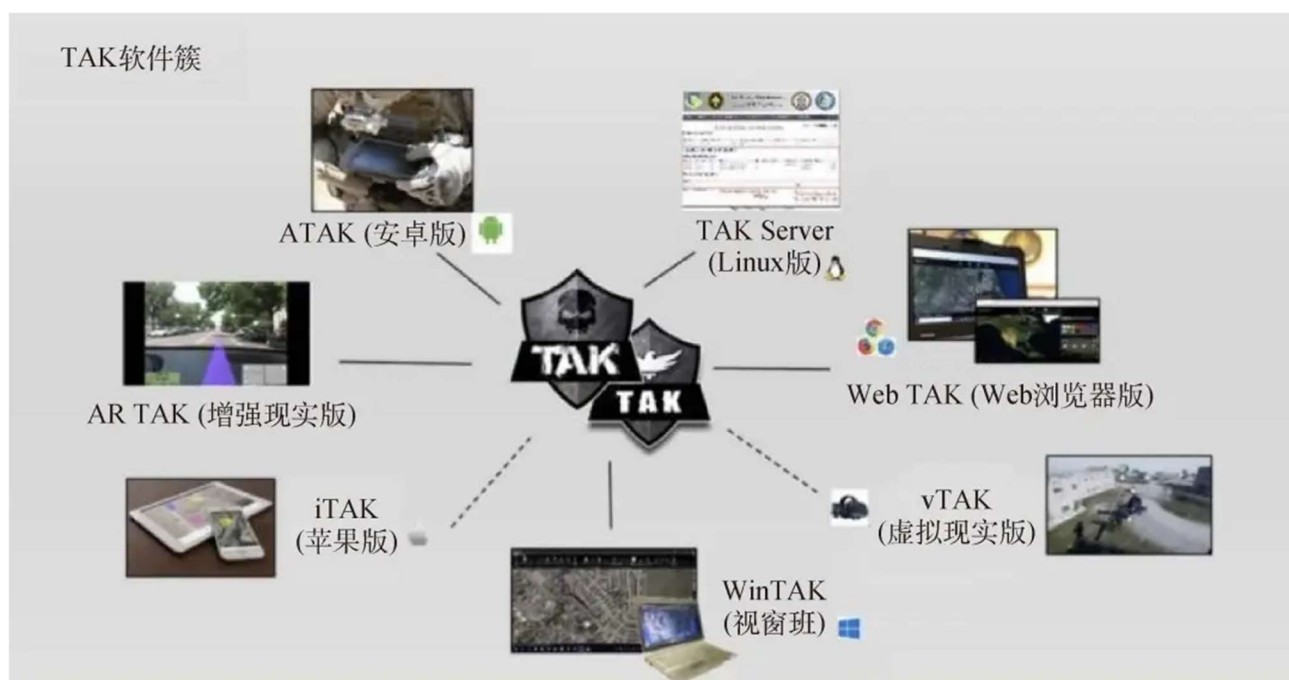


Figure 2.7 – Composition of tactical attack kit

Source: formed by the author

The ATAK software uses a plugin architecture which allows developers to add new applications to the system. The hardware for ATAK consists of rugged end-user devices (EUD) provided by Panasonic. These devices feature a 2.2 GHz octa-core processor, which provides the capability for integrated edge processing of data from drones, robots, and other devices.

The TAK is a toolkit designed for conducting tactical missions in spectrum-denied environments. As an intelligence-gathering tool, its primary uses include:

- **Situational Awareness:** Providing a comprehensive view of the operational environment.
- **Mission Planning:** Assisting in the development and preparation of tactical plans.
- **Remote Command:** Enabling command and control from a distance.
- **Mission Execution:** Supporting the execution of missions by providing necessary information and tools.
- **Call for Fire:** Facilitating the request and coordination of fire support.



Figure 2.8 – ATAK End User Device

Source: formed by the author

The TAK is a toolkit designed for conducting tactical missions in spectrum-denied environments. As an intelligence-gathering tool, its primary uses include:

1. Situational Awareness: Providing a comprehensive view of the operational environment.
2. Mission Planning: Assisting in the development and preparation of tactical plans.
3. Remote Command: Enabling command and control from a distance.
4. Mission Execution: Supporting the execution of missions by providing necessary information and tools.
5. Call for Fire: Facilitating the request and coordination of fire support.

Specific functionalities include:

1. Situational Awareness Capabilities: Includes "Blue Force Tracking" for coordinating fire actions among team members, and "Red Force Tracking" for viewing

enemy positions as well as terrain, weather, and other geographical elements.

2. **Communication Integration Capabilities:** Supports multiple communication methods, including smartphones, for encrypted data communication across different agencies. This includes data, text, images, and video, with the capability to set communications between user-to-user, user-to-team, user-to-command post, or user-to-entire unit.

3. **Mapping Capabilities:** Provides rapid rendering of various standard-format images both online and offline, location marking, collaborative mapping, area fencing, fixed/moving target tracking, measurement on maps, terrain analysis, altitude profile plotting, navigation (walking, vehicle, aircraft), and historical records. Uses U.S. military standard MIL-STD-2525B for symbol annotation.

4. **Instant Messaging Capabilities**:** Supports chat, file sharing, photo sharing, video sharing, and streaming.

5. **Unique Military Capabilities**:** Includes site survey tools, targeting, precise geo-location measurement, runway survey tools, military radio control (supporting situational awareness data link SADL, Link-16 data link, TrellisWare/Harris SA tactical radios, etc.), messaging and interfaces, and conflict airspace clearance and drone control.

The Tactical Assault Kit (TAK) is a geospatial application that enables coordination among thousands of users through functions such as location data, chat, mission planning, and shared overlays. Since its introduction, over 10,000 active-duty personnel have tested it. In September 2015, DARPA reported that ATAK was successfully demonstrated for persistent close air support. By January 2016, ATAK was deployed with Air Force Special Operations. By 2019, approximately 160,000 Army users had joined the ATAK program. The U.S. Army and Special Operations Forces have utilized the Android Tactical Assault Kit (ATAK) in Iraq, Afghanistan, and Syria, allowing troops to access more information, communicate more easily with other units, and quickly locate potential enemy positions, as shown in Figure 2.10.

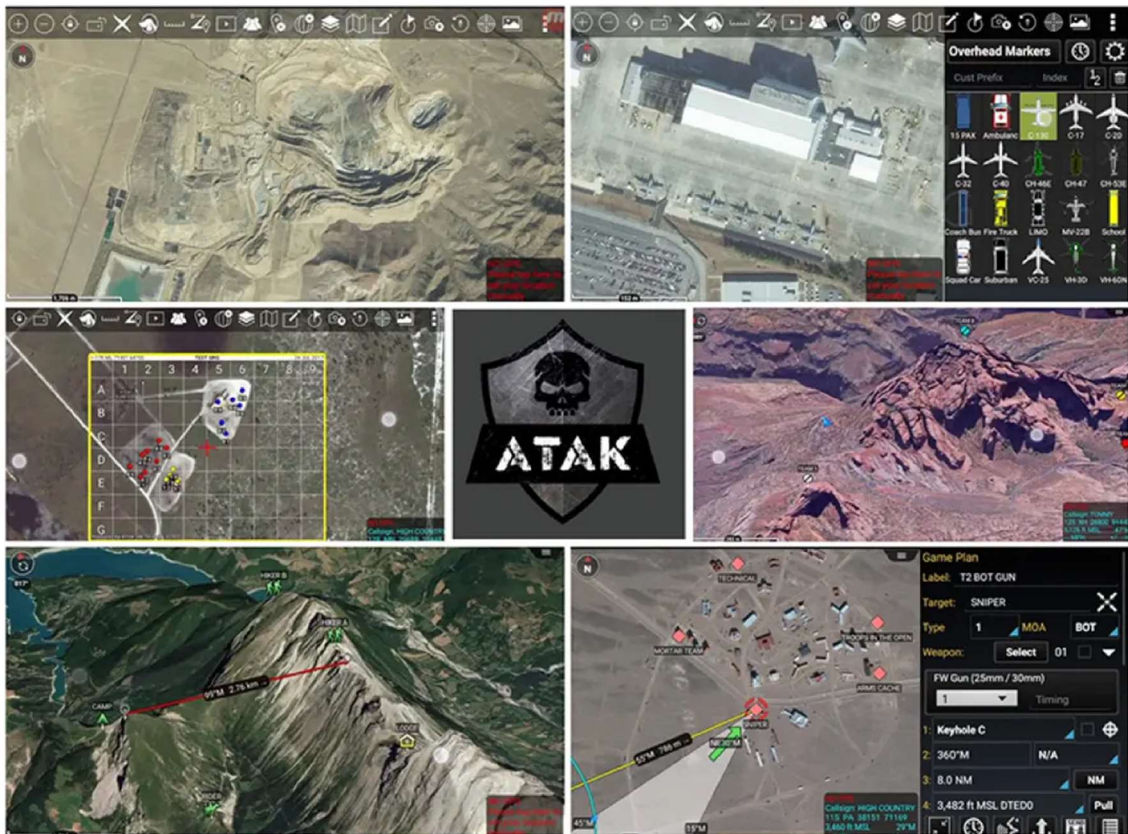


Figure 2.9 – ATAK application scenario

Source: formed by the author



Figure 2.10 – Use of ATAK on the battlefield

Source: formed by the author

Colonel Joel Babbitt, head of the Special Forces Warrior Office, stated: “This app can reduce the Joint Terminal Attack Controllers' (JTAC) kill chain (which has 16 steps) from minutes to seconds, enabling close air support to be coordinated in seconds” [19].

2.3 Analysis GIS Art for Artillery from the Institute of Intelligent Computing Information Management

Starting from May 11, 2022, the Ukrainian Ministry of Defense [20], Ukrainian demining engineer Maxim [21], and Ukrainian software engineer Volodymyr [22] confirmed via Twitter and The Times that the Ukrainian military used the "GIS Arta" software, similar to an "Uber" ride-hailing app, in an order-based strike mode. This software directed various types of artillery, including self-propelled howitzers, self-propelled guns, and multiple rocket launchers, to simultaneously strike from different directions. This approach successfully ambushed a Russian battalion tactical group (BTG) preparing to cross the Seversky Donets River, destroying 73 vehicles.

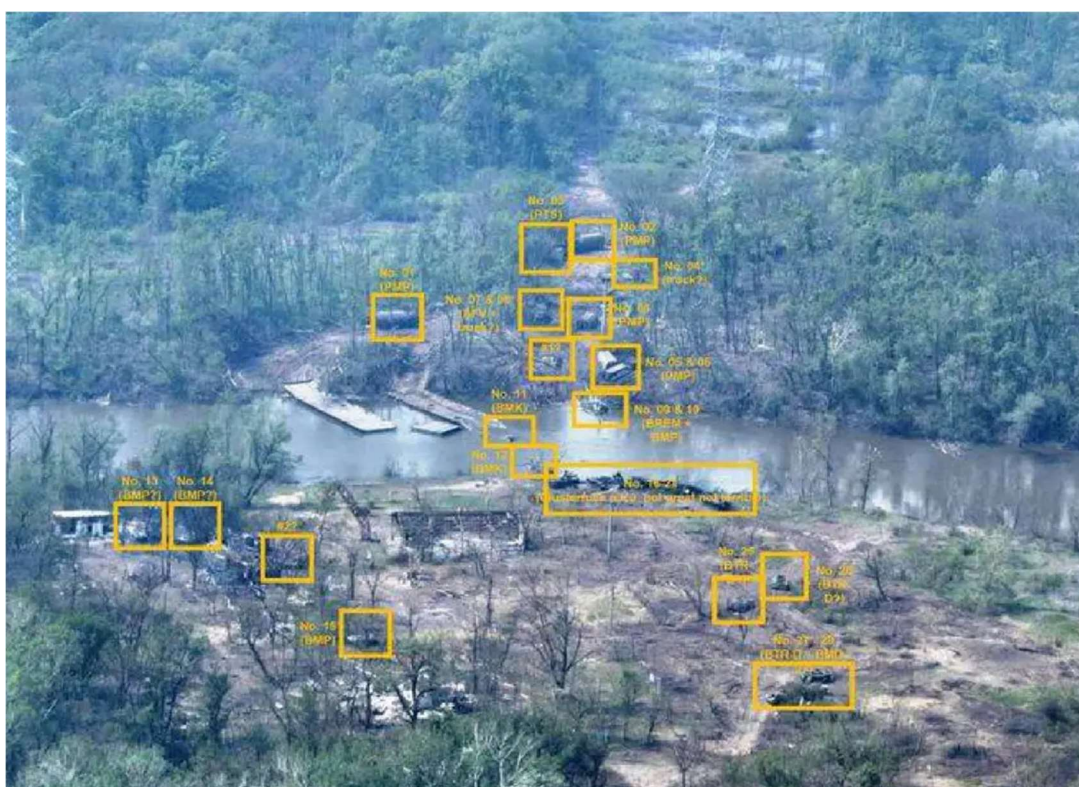


Figure 2.11 – Russian troops ambushed on the banks of the North Donetsk River
Source: formed by the author

Maxim conducted close reconnaissance of the targets using drones and range finders, and uploaded the results to the command post. He used the "GIS Arta" software to mark the relevant combat situation, as shown in Figure 12. Additionally, Volodymyr, a member of the "GIS Arta" software development team, specifically mentioned that Elon Musk's Starlink satellite system ensured the secure transmission of information for the "GIS Arta" system.

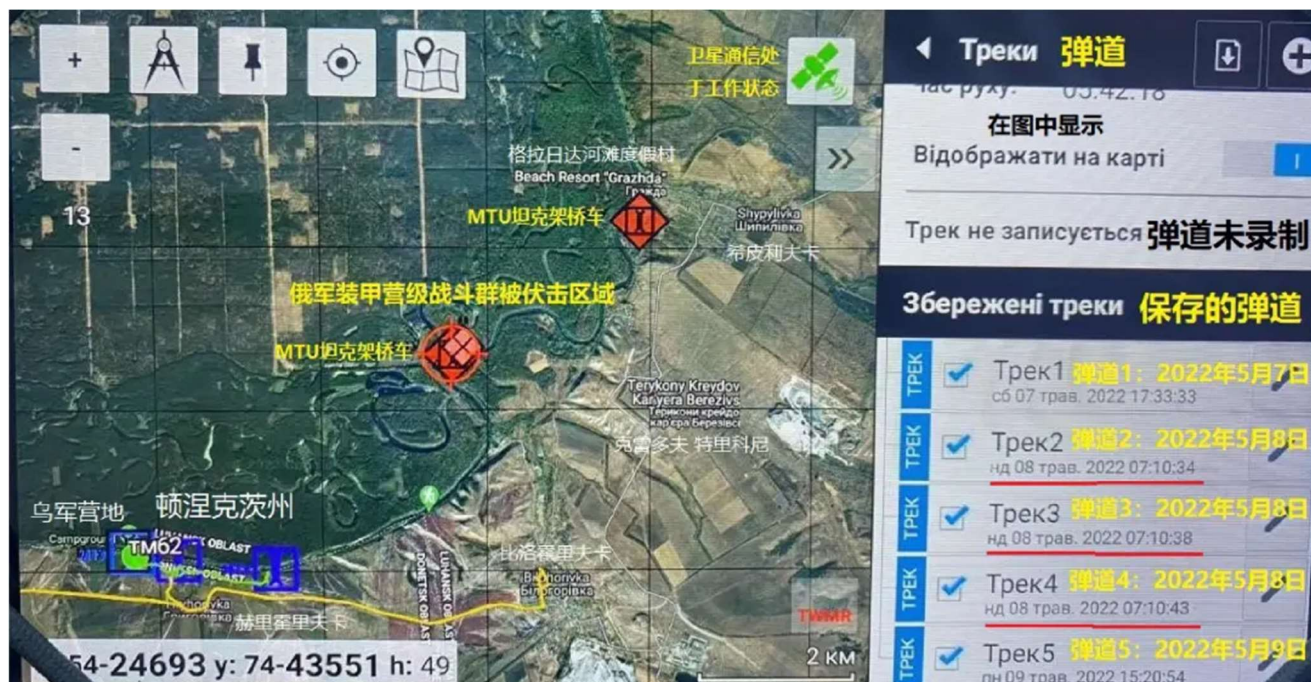


Figure 2.12 – Application of GIS Arta software in ambush combat

Source: formed by the author

The highlighted portion of the interface shows that on May 8, 2022, three Ukrainian combat units conducted simultaneous saturation attacks on the target at 7:10:34, 7:10:38, and 7:10:43, with intervals of 4 and 5 seconds, respectively. This matches the Ukrainian official announcement. The Ukrainian forces participating in this battle were from the 17th Tank Brigade's artillery units, which included one 2S1 "Gvozdika" self-propelled howitzer battalion, one 2S3 "Akatsiya" self-propelled gun battalion, and one BM-21 "Grad" multiple rocket launcher battalion. Additionally, two other strikes occurred on May 7 and May 9.

The system was developed by 34-year-old Ukrainian programmer Yaroslav Sherstyuk. After Crimea's annexation by Russia, Sherstyuk's team developed an early version known as the "Target Allocation Network" in May 2014, which was subsequently improved to form the current version. The system is described by its creators as the "Uber for artillery" and is also known as the "Artillery Combat Management System." It has been integrated into the Ukrainian military. While specific deployment details in Ukraine are not widely reported, it is claimed that the system is extensively used and capable of targeting all Russian forces on the battlefield, including within Russia itself.

The software is touted as a revolutionary application for solving complex targeting problems, providing accurate tracking and location of targets, and significantly reducing the time required to call in strikes. Its equipment and software interface are shown in Figure 13. Each target is assigned high-precision coordinates, its terrain is identified, and its ingress and egress routes are determined.

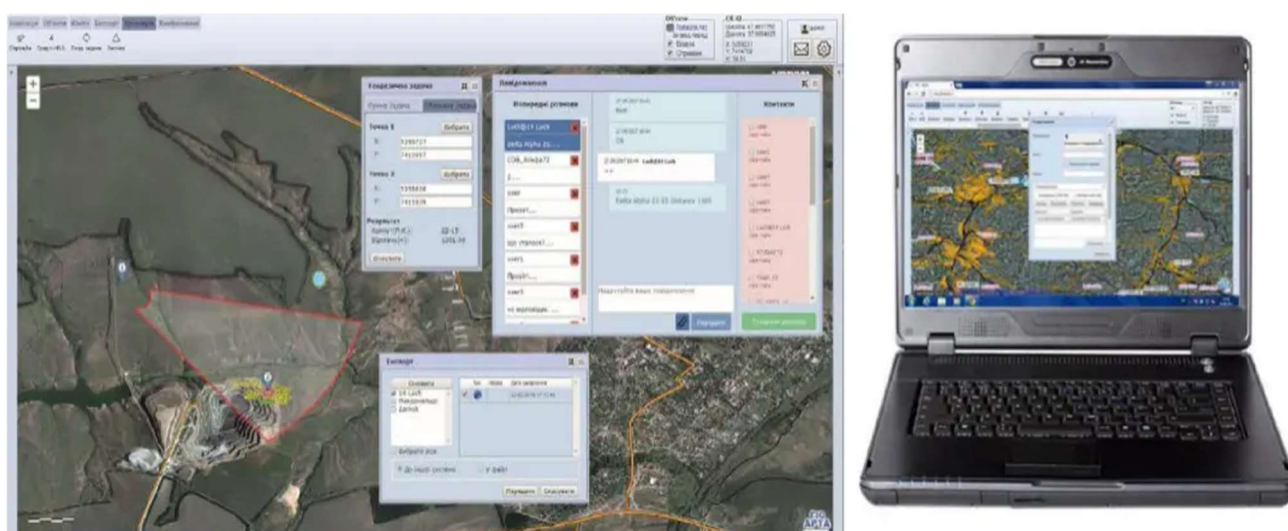


Figure 2.13 – "GIS Arta" software interface and equipment form

Source: formed by the author

Basic principles, main functions and development directions.

GIS Arta operates similarly to Uber's ride-hailing technology. Just as Uber locates passengers and dispatches the nearest available vehicle, GIS Arta identifies, tracks, and locates Russian military targets and swiftly selects suitable artillery, mortars, missiles,

or drone units within range to engage the target.

The main functions of the GIS Arta system are as follows:

1. **Target Intelligence Integration:** The software is a complex tracking and localization system capable of receiving data from drones, reconnaissance aircraft, smartphones, rangefinders, satellite imagery, and video feeds. It can even integrate intelligence from certified crowdsourced phones. Using advanced technology, it quickly processes this data to generate precise target coordinates. Similar to Google Maps, it continuously updates coordinates based on target movement to guide firepower attacks.

2. **Strike Task Allocation:** Based on the intended strike, tasks can be assigned to the most suitable artillery, mortars, drones, rocket launchers, or special forces units within the Ukrainian military.

3. **Parameter Calculation:** By calculating the Time Over Target (TOT), the system can coordinate multiple distributed fire units to conduct simultaneous strikes from different directions on the same target area.

4. **Network Communication Connectivity:** The system facilitates communication between command posts and distributed operational units via military communication systems and methods like Starlink, allowing for command instructions and parameter distribution.

Performance Metrics

Compared to traditional systems, the GIS Arta software has reduced the time from target identification to target destruction from 20 minutes to 30 seconds, with a shooting accuracy of 6 to 25 meters. However, information on the software's multi-target strike support capability remains classified and is not publicly disclosed. Additionally, the software supports calculations for distributed operational units to simultaneously attack the same target from different directions. This capability helps to disrupt enemy radar observation and makes it more challenging for them to execute retaliatory strikes.

GIS Arta outperforms the U.S. Army's Advanced Field Artillery Tactical Data System (AFATDS). The former is a truly distributed software system, while the latter uses a mainframe-minicomputer-terminal architecture. Moreover, AFATDS has a deliberately set reaction time of 1 hour to allow for the commander's judgment, aiming

to prevent friendly fire. Without this factor, the fastest reaction time for AFATDS is 15 minutes.

5. When a reconnaissance system detects a target in a designated area, it reports the target's location and image data to the GIS Arta system. Once the commander decides to engage the target, the system selects the most suitable missiles, artillery, or drones. It then automatically calculates the attack sequence and firing parameters to ensure synchronized arrival at the target. The strike instructions are transmitted to the distributed task forces via communication links such as "Starlink." The target is destroyed within 30 seconds.



Figure 2.14 – GIS Arta combat procedures

Source: formed by the author

Development direction of the kill chain from the perspective of global operations.

5F Model:

In integrating the kill chain across different domains, the focus is on compatibility to ensure each domain can execute every step of the kill chain, enabling coordination and interchangeability among steps. A simplified 5F model, which includes Find, Fix, Fire, Finish, and Feedback, is used for streamlining the process. This model omits tracking and aiming phases, simplifying the procedure and facilitating domain compatibility. Under this model:

1. Find: Intelligence, surveillance, and reconnaissance (ISR) networks detect any object entering the network.
2. Fix: The ISR systems locate the target and share target data with all weapon systems in the network.
3. Fire: The joint command system determines which weapons are suitable for the target and controls these weapons to carry out the attack.
4. Finish: Unmanned aerial vehicles (UAVs) can provide damage assessment images. If targets are still intact, UAVs can use Hellfire missiles to finish the job.
5. Feedback: Various reconnaissance devices assess final damage, completing the feedback phase.

Multi-domain Integration: In the era of all-domain operations, the kill chain's advantage lies in providing multiple options for cross-domain operations based on specific situations. According to Metcalfe's Law, the value of a network increases with the number of nodes. Similarly, the more devices and connections in a kill chain network, the more options are available for attacking the enemy, creating numerous opportunities and making it difficult for the enemy to escape once they enter the kill chain network. Currently, the U.S. military is integrating 17 types of intelligence systems – signal intelligence, electronic intelligence, measurement and signature intelligence, human intelligence, open-source intelligence, imagery intelligence, geospatial intelligence, cyber intelligence, etc. connecting them with various command and control systems and weapon systems to form a comprehensive battlefield network with more devices and nodes, thus building a more complex and dense kill network.

Dynamic Integration: Transforming the traditional static, sequential kill chain into a dynamic network with multiple simultaneous processes requires robust data integration and command control capabilities. Solving data integration issues is crucial for seamless connection from sensors to shooters and effective coordination among different intelligence systems. The U.S. military has proposed numerous development plans aimed at enhancing overall command capability, including:

Advanced Battle Management System (ABMS): Air Force

- Target Recognition and Adaptation in Contested Environments (TRACE): DARPA
- Collaborative Operations in Denied Environments (CODE): DARPA
- Joint All-Domain Command and Control (JADC2): Joint project
- Integrated Battle Management System (IBMS): Army
- Cooperative Engagement Capability (CEC): Navy

These programs aim to improve coordination and control across all domains, supporting the creation of a more effective and integrated kill chain network.

Composition of the Ukrainian Army's Tactical Kill Chain for Attacking Time-Sensitive Targets

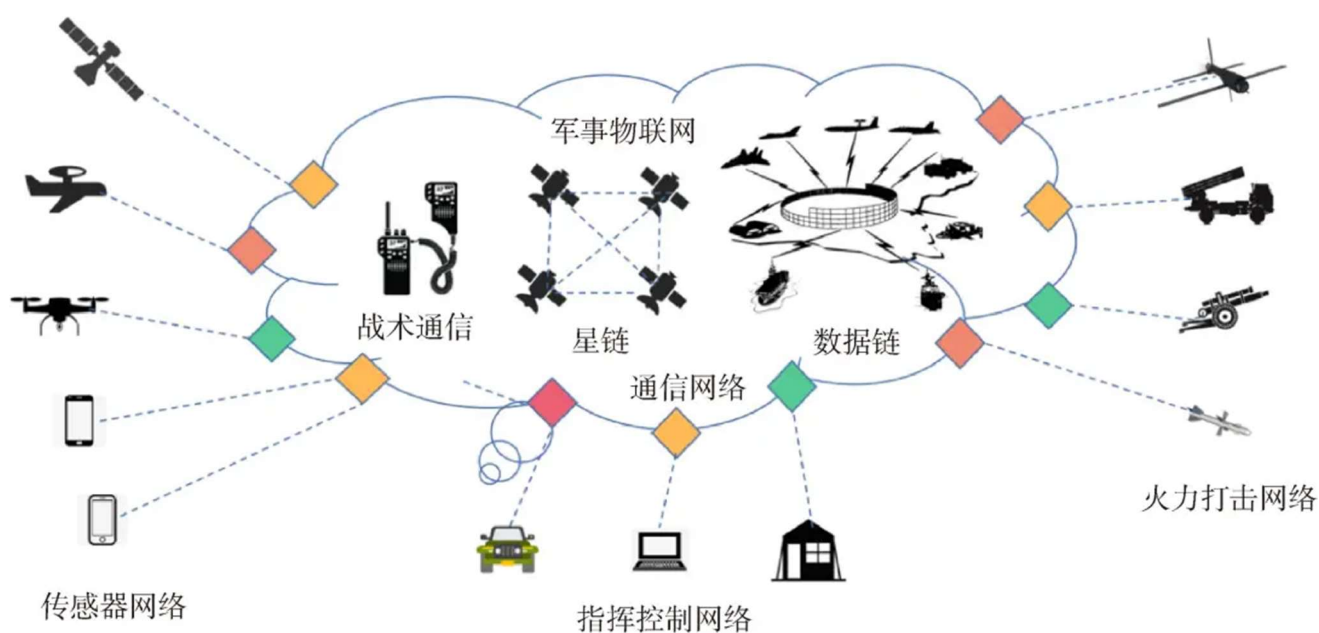


Figure 2.15 – Ukrainian army kill chain

Source: formed by the author

Detection, Location, and Target Indication

1. External Reconnaissance Means:

U.S. and NATO Reconnaissance Satellites: Provide high-resolution imagery and real-time data to assist in locating and monitoring targets.

Reconnaissance Aircraft: Such as the U.S. U-2 or Global Hawk unmanned reconnaissance aircraft, used for aerial reconnaissance and intelligence gathering.

2. Internal Reconnaissance Means:

ATAK Collaborative Awareness Tool: Provides situational awareness, target location, and real-time data sharing capabilities.

Drones and Rangefinders: Conduct close-range reconnaissance and location of ground targets.

3. Intelligence Crowdsourcing Software:

“e-Enemy”: Collects and aggregates real-time intelligence from Ukrainian civilians.

“Stop Russian War”: Provides a platform for civilians to report Russian military movements.

“Ukraine Avenger”: Another crowdsourced intelligence reporting platform for real-time updates and target data analysis.

Communication and Transmission

1. Military Communication Equipment:

Military Tactical Communication Devices: Includes satellite terminals, tactical radios, and data link terminals for secure data transmission and command communication.

2. “Starlink” Terminals:

SpaceX’s “Starlink” System: Provides global high-speed internet connectivity to ensure real-time data transmission and system reliability.

Decision-Making and Task Allocation

1. Command and Control Centers:

U.S. and NATO Command and Control Centers: Responsible for strategic decision-making, task allocation, and operational command.

GIS Arta:

Ukrainian Artillery Operations Management System: Used for rapid task allocation, target location, and fire control.

3. ATAK:

Android Tactical Assault Kit: Provides battlefield situational awareness, mission planning, and fire control capabilities.

Strike and Engagement

1. Main Combat Forces:

Artillery: Includes self-propelled howitzers and rocket launchers for providing long-range fire support.

Drones: Used for reconnaissance, target engagement, and battlefield monitoring.

Portable Cruise Missiles: Such as the Javelin anti-tank missile, used for engaging armored targets.

Tactical Missiles: Used to strike high-value and time-sensitive targets.

CHAPTER 3

DEVELOP INFORMATION SYSTEMS AND TECHNOLOGY IN CONFLICTS ACCORDING TO THE RESEARCH OF THE INSTITUTE OF INTELLIGENT COMPUTING INFORMATION MANAGEMENT

3.1 Key technologies of combat management system

The operational management system is the engine behind the construction of the kill chain. In a distributed contested environment, the key technologies of the operational management system include:

1. Communication Integration: The core is the construction of a military Internet of Things (IoT), enabling cross-domain distributed connectivity and control.
2. Intelligence Integration: The core is the rapid and accurate fusion of multi-source heterogeneous information.
3. Force Integration: The core is the task allocation method based on a global military value perspective.
4. Security Integration: The core is ensuring trustworthiness and reliability at every link in a contested environment.
5. System Integration: The core is the construction of an agile and resilient system architecture.

The architecture determines the operational mode and capabilities of the system. Both Uber and Didi use a technology architecture based on real-time data stream buses and dispatch engines, but they differ in their dispatch models. Uber primarily employs a forced dispatch model, where once a passenger requests a ride, the system assigns the request to the driver and vehicle it deems most suitable. Didi, on the other hand, uses a grab-based dispatch model, where the request is sent to multiple eligible drivers, allowing them to compete to accept the ride.

Regarding operational management systems, DARPA announced the "Adapting Cross-Domain Kill-Webs (ACK)" project on August 3, 2018. The goal is to develop an

auxiliary decision-making tool for constructing kill chains in complex contested environments. The project aims to address the following issues:

1. Capability Boundary Issue: During operations, commanders often have limited or no understanding of the capabilities available across different domains and the quality of services that other domains might offer.

2. Value Trade-Off Issue: Each domain has its own set of authorizations and tasks, making it challenging to evaluate the "value" or "cost" of supporting a new task from another domain against their current set of tasks.

3. Optimal Decision Issue: Given a range of diverse cross-domain kill chain options, decision-makers need a method to quickly compare and select the "best" option.

To address these challenges, a "Request-Bid-Competition" model architecture has been proposed, drawing from e-commerce principles. This model includes the following components and steps:

Model Components:

1. Virtual Liaison: Acts as an intermediary to facilitate communication between commanders and available resources.

2. Capability Market: A platform where various operational resources are listed as suppliers, and commanders are customers.

3. Suppliers: Various operational resources, such as military assets or systems, are listed as suppliers in the market.

4. Consumers: Commanders or decision-makers are the customers who need to request and select suitable resources.

Process Steps:

1. Request: The commander (consumer) identifies their task requirements and selects one or more "plays" or high-level templates from the ACK system that can meet these needs. This corresponds to the initial stages where requirements are defined and published.

2. Bid: The ACK system sends "bid requests" to the Virtual Liaison. The Virtual Liaison then provides "offers" from available resources that meet the requirements. This involves returning task fulfillment degrees and constraints back to the customer.

3. Competition: The commander (consumer) evaluates the offers based on value functions such as minimizing risk or optimizing overall performance. They then choose the most suitable kill chain option to accomplish the task.

This approach allows for a service-oriented method of constructing specific kill chains in a denied environment, leveraging intelligent decision support algorithms to optimize resource allocation and task execution.

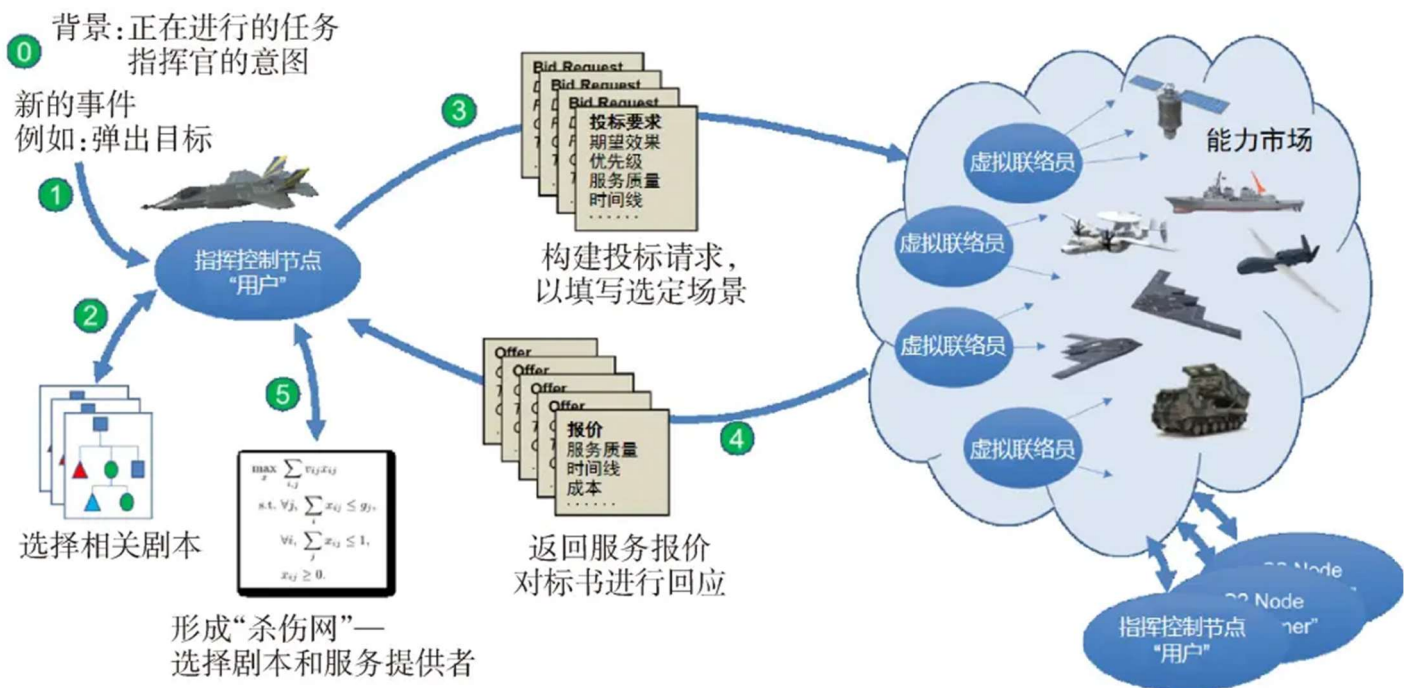


Figure 3.1 – Adapting Cross-Domain Kill-Webs

Source: formed by the author

In September 2020, the U.S. Air Force conducted a technical demonstration and verification of the Adaptive Cross-Domain Kill Web (ACK) [29], with the scenario being air defense operations. The Adaptive Cross-Domain Kill Web analyzes thousands of cross-domain "kill chain" solutions and recommends the best one to the mission commander. Once selected by the commander, the solution will be sent to the Command Control Incident Management Emergency Response Application (C2IMERA) and the land-based Composite Tracker and Classifier (CTC) integrated fire control system, using Link-16 and other means to disrupt enemy fighters and intercept cruise missiles using

automatic messaging and machine-to-machine methods.

The core of this function is the Multi-Domain Adaptive Request Service (MARS) software, which is essentially a mission planning software. Multi-Domain Operations Mission Planning is a complex task involving a large number of distributed variables, such as domains, systems, resources, and manned and unmanned platforms. The software helps commanders make informed decisions by automatically identifying available capabilities across domains and quickly assessing the costs and benefits of using those capabilities when adjusting missions.

The prerequisite for achieving a closed-loop kill chain is to integrate all nodes into an Internet of Things (IoT) network. The IoT architecture consists of the application layer, service and application support layer, network layer, and device layer, as shown in Figure 17. Compared to the Internet of Vehicles (IoV) used in ride-hailing systems like Didi, the Internet of Military Things (IoMT) is characterized by the following four aspects:

1. At the Device Layer: The connected objects are multi-domain, including sensors, command centers, firepower units, and various support elements.
2. At the Network Layer: The communication channels are complex, encompassing military communication systems, commercial satellite communication systems, and public mobile communication systems.
3. At the Service Layer: The types of information processed are cross-domain, involving land, sea, air, space, and electromagnetic fields. There are higher demands for the speed, accuracy, and security of information acquisition, transmission, and processing.
4. At the Application Layer: There is an adversarial nature, with high demands for the system's agility, flexibility, and autonomy under denial and countermeasures conditions.

Device Integration: At the device layer, access to software development kits (SDKs) is provided to vendors of sensing and execution devices. Additionally, methods such as Attention (AT) instruction sets from data terminal equipment (DTE) to terminal adapters (TA) are used to shorten the device integration cycle.

Network Adaptation: At the network layer, multiple communication networks are integrated based on TCP/IP protocols. A message queuing telemetry transport (MQTT) communication module is added to support subscription and publishing mechanisms for message queue transmission protocols.

Service Compatibility: At the service layer, compatibility with various types of services is achieved. For example, storage services must be compatible with traditional relational databases like MySQL, distributed storage databases like HDFS, columnar databases like HBase, distributed caching databases like Redis, and data warehouses like Hive. Seamless integration with foundational services such as navigation, time-space reference, geographic information, and streaming media services is also required.

Agile Application: At the application layer, over-the-air (OTA) technology is employed to enable remote management of mobile terminal devices. This facilitates online training, monitoring, maintenance, and upgrades of operational application software to adapt to changes in operational requirements and battlefield environments.

Content aggregation technology.

GIS Arta utilizes a geographic information platform-based aggregation technology that focuses on target intelligence. Through artificial intelligence, it aggregates heterogeneous data, images, and videos from satellites, aircraft, drones, and smartphones on a map. This creates a dynamic target situation map that continuously updates the target's location and behavior, allowing Ukrainian artillery to quickly identify and track targets and adjust firing parameters in real-time. Before this solution, locating a target could take over 15 minutes; now it takes only 30 seconds, significantly improving reaction times and potentially determining survival on the battlefield.

Content aggregation is a common concept in internet digital products and e-commerce. It involves solving the following key technologies:

1. Unified Description Technology: Technology for unified description of cross-media data resources based on geographic information platforms.
2. Dynamic Data Collection Technology: Technology for dynamic data collection across domains based on a unified space-time reference.
3. Theme Classification Technology: Technology for theme classification based

on multimedia content feature extraction.

4. Rapid and Accurate Fusion Technology: Technology for rapid and accurate fusion of multi-source information based on target themes.

5. Information Association and Conflict Resolution: Technology for information association and conflict resolution based on sensor location and network topology.

6. Hotspot Discovery and Behavior Prediction: Technology for hotspot discovery and target behavior prediction based on complex event processing (CEP).

7. Message-Driven Aggregation Technology: Technology for proactive aggregation of information based on message-driven methods.

8. Heterogeneous Content Management and Intelligent Cataloging: Technology for managing heterogeneous digital content and intelligent cataloging based on parallel computing.

9. Content Service Evaluation Technology: Technology for evaluating content services based on feedback mechanisms.

Matching technology

The Didi Chuxing system, the dispatch algorithm is crucial. When Uber went public, it highlighted the dispatch engine as a core technology in its prospectus. The effectiveness of the dispatch algorithm determines the overall platform's transaction efficiency and user experience. However, dispatch algorithms are not as simple as assigning customer orders to the nearest driver. In scenarios such as many-to-many dispatch, ride-sharing, and peak-hour dispatch, a greedy algorithm that assigns orders based on proximity or first-come-first-served can only achieve a local optimal solution. This approach fails to account for future demand and does not provide a global optimal solution, which is necessary to best meet the needs of all passengers and drivers on the platform.

Moreover, in many-to-many scenarios, the number of permutations and combinations can be enormous. For example, consider assigning 20 passengers to 20 cars with the goal of minimizing the total waiting time. The solution space for this problem is 20 factorial, which equals 2,432,902,008,176,640,000—approaching the scale of 200 quintillion. This magnitude makes finding a quick solution extremely

challenging.

The United States perceives the primary threat as the risk of great power conflict, particularly the impact of Russia's anti-access/area denial (A2/AD) strategy on the effectiveness of U.S. military operations. Additionally, the third offset strategy may diminish U.S. advantages in specific domains. Consequently, building all-domain kill webs has become a crucial development direction for the U.S. military. The main points are as follows:

1) Building Intelligence, Surveillance, and Reconnaissance (ISR) Systems for Joint All-Domain Operations:

ISR systems must be sensitive, adaptive, interoperable, modular, and multifunctional.

The U.S. Army's 2020 "Military Intelligence Professional Report" suggests improvements in five areas: platforms, sensors, processing/utilization and distribution, data transmission and network architecture, and integration of signal intelligence/electronic warfare/cyber operations. These improvements aim to adapt to evolving threats and meet various operational needs.

To address interoperability issues among different military branches, the Department of Defense issued the "DoD Data Strategy," calling for the establishment of data standards and interoperability requirements to eliminate data discrepancies and ensure data linkage across different sources within the DoD. The U.S. Army and Air Force signed an agreement in September 2020 to develop "Common Standards for Data Sharing and Service Interfaces."

2) Developing Distributed Forces to Enhance Precision and Diversity of Firepower: To create an effective kill web, more attack nodes should be deployed to avoid centralized setups, which reduce attack flexibility and survivability.

The U.S. military aims to form lower-level combat units with relevant capabilities, emphasizing mobility and flexibility for diverse operational environments. Research and deployment of robotics and drones are also key focus areas.

3) Establishing Command and Decision Systems Utilizing AI and Big Data:

Developing AI-based decision support systems to help users select operational

equipment across different domains, creating adaptive kill webs.

Ensuring systems can autonomously adjust to changing battlefield conditions to enable faster and better decision-making. Raytheon has begun research for the Defense Advanced Research Projects Agency (DARPA) on decision support software, including the development of "Real-time Reasoning and Analysis for Cross-Domain Kill Web Negotiation and Instantiation" software, which has been applied in the Air Force's Advanced Battle Management System (ABMS). In August 2020, the U.S. military conducted the largest-scale testing of its network, AI systems, and sensors, demonstrating the execution thread of an "AI-enabled kill web."

4) Emphasizing Allied Collaboration:

U.S. military operations often involve multinational coalitions, requiring interoperability with allies' ISR, command, and weapon systems.

In developing all-domain kill webs, the U.S. will consider collaboration with allies. Secretary of Defense Mark Esper announced plans for "Project Convergence" in 2021, which aims to include international partners and allies to integrate more air and ground weapons, including F-35 fighters and precision-guided missiles.

The U.S. military's kill web theory is a new operational concept developed under the impetus of threat assessment and military revolution, aimed at achieving overall superiority in multi-domain operations and enabling rapid, effective responses to various situations. This practice could profoundly alter modern warfare dynamics, having a significant global impact and providing valuable insights and references for future developments.

The construction of U.S. military kill webs will accelerate the pace of warfare and enhance joint advantages. Compared to a single kill chain, a kill web can more effectively utilize multi-domain systems for more efficient information collection and threat response, thereby speeding up the pace of war, altering warfare modes, and potentially triggering a new arms race. Additionally, the U.S. military is continually strengthening its own capabilities and expanding unilateral advantages.

For combat management systems, dynamic task allocation based on targets and environment is a core algorithm. This paper proposes a task allocation technology based

on a dual-gene genetic encoding combined with an annealing algorithm [34], aimed at addressing the following two issues:

1. Solving Dynamic Optimization Problems: Traditional genetic algorithms do not consider losses in cargo handling, while combat task allocation must account for significant losses due to offense and defense confrontations. This introduces variability in the solution space due to task allocation relationships and weapon ammunition consumption. To address this, a “relationship-quantity” dual-gene encoding method is designed to construct a multi-constraint sparse matrix that reflects dynamic changes within the maximum solution space. The allocation relationships are optimized according to a reward function, and the allocation quantities are optimized according to a penalty function to solve the dynamic optimization problem.

2. Solving Global Optimization Problems: Traditional genetic algorithms use single-objective optimization results as the termination condition for searches. However, combat task allocation requires global optimization, aiming to minimize weapon ammunition consumption while achieving the best damage effects. To address this, the minimum consumption is first determined and used as a constraint, followed by searching for the optimal effect solution. During the solving process, the simulated annealing algorithm is introduced, where each sub-task retains several optimal solutions, and a backtracking combination calculation is performed in the case of multiple tasks. The calculation only stops when the global optimum is reached.

In July 2021, during the "Global Information Dominance Experiment 3 (GIDE3)" exercise organized by U.S. Northern Command, Raytheon demonstrated the core software of ACK - “Anytime Reasoning and Analysis for Kill-Web Negotiation and Instantiation across Domains (ARAKNID)” [35]. Military commanders often have to make decisions with limited information. This system establishes a military IoT that connects distributed, cross-domain sensors and strike weapons, enabling the real-time creation, evaluation, and visualization of hundreds to thousands of action plans, far faster than manually creating single action plans by air combat managers. During the exercise, various scenarios were tested where the software assigned fighter jets to engage multiple targets and dynamically adjusted plans in real-time. Results showed that the software

significantly reduced the time for aircraft deployment and increased the likelihood of immediate interception.

Using crowdfunding software to quickly gather open-source intelligence is a very effective approach. One key issue that needs to be addressed is how to verify the randomly sent data. To address this, Ukrainian citizens are required to undergo real-name authentication through the Diia app before sending intelligence information about Russian troops via the chatbot (eVorog) [36].

Diia, launched by Ukraine's Ministry of Digital Transformation in early 2020, is a digital identity verification application that can embed various public service documents. It has been proven that authorizing through the Diia app on eVorog is a very effective method.

Additionally, blockchain-based information security solutions represent a systemic solution for non-trusted adversarial environments [37].

3.2 Development Considerations for Combat Management

Combat management systems generally have the characteristics of integration, automation, optimization, and real-time. The combat mode of modern warfare is complex, the battlefield scale is expanding, and the requirements for force control, resource integration, and task scheduling are increasing. It is necessary to achieve system integration. The French Army's "Scorpion" system fully integrates tanks, armored vehicles, infantry fighting vehicles, unmanned ground vehicles, drones, and attack helicopters into the same combat group, and links all platforms and combat units in the task group.

With the increase in combat elements in modern warfare and the expansion of battlefield perception space, the command automation system that relies heavily on people can no longer fully adapt, and the system must be automated. All operating functions of Pakistan's combat management artillery control system are fully automated, "providing automated solutions for preparing, coordinating, transmitting, executing, and modifying fire support plans and shooting plans."

The pace of modern warfare operations is accelerating, and battlefield data is massive. It is necessary to quickly grasp the situation and make decisions efficiently, and it is necessary to achieve system optimization decisions. Military powers are combining artificial intelligence, cloud computing, the Internet of Things, and big data technologies to facilitate faster decision-making in multi-domain operations. Traditional combat management systems place more emphasis on engagement sequences and combat rules based on pre-established rules. However, future wars will highlight the confrontation between systems. It is impossible to exhaust all kinds of situations in advance, and the battlefield information that needs to be mastered will become more complex and massive. To this end, the armies of various countries have begun to abandon the traditional method of developing combat management systems for each combat domain separately, and are centered on the network and supported by artificial intelligence, trying to help commanders make combat decisions more quickly and realize the real-time connection between sensors in each combat domain and any shooter.

The combat management system will promote the implementation of combat concepts. The "Advanced Combat Management System" developed by the US Air Force plans to connect all services and their weapon platforms in real time in a military Internet of Things. Its core is to seamlessly link various intelligence reconnaissance platforms, command and control platforms, strike platforms and combat management platforms with various cross-domain capabilities, convert intelligence and target indication data into timely and usable information, shorten the "discovery-positioning-tracking-targeting-strike-evaluation" cycle, and execute combat operations at a speed that opponents cannot keep up with. The Russian army proposed the theory of "military unified information space" and organized the development of an "automatic control system" for integrated joint operations of land, sea and air networks. By establishing a network-centric command model, it attempts to integrate the command, communication, reconnaissance, firepower, and support of the entire army, realize cross-domain operations in the true sense, and enhance battlefield situation awareness and combat command efficiency.

The combat management system will rely on artificial intelligence technology.

The application of artificial intelligence will not only cause the capabilities of weapon systems to multiply, but will also fundamentally change the realization of the OODA loop. In the future combat management system, artificial intelligence technology will become the core support and driving engine, and the key factor is the quality of the algorithm. The system will have built-in upgradeable artificial intelligence, and people will be in a supervisory or collaborative state to minimize manual input, spontaneously identify and classify threat targets in the combat environment, autonomously evaluate and weigh, and automatically allocate weapons, thereby providing adaptive combat advantages and decision-making options.

For example, the "Intelligent Autonomous System Strategy" released by the US Navy in July 2021 aims to accelerate the development and deployment of intelligent platforms through a highly distributed command and control architecture, integrate unmanned systems, artificial intelligence, and autonomous driving technologies, and realize future combat decisions facilitated by intelligent autonomous systems. The Russian military is developing more than 150 artificial intelligence projects, one of the focuses of which is to introduce artificial intelligence into the command and control system, adapt intelligent software to different weapon platforms, achieve the unification of the physical domain and the cognitive domain, and double the combat effectiveness in an intelligent empowering way.

The combat management system will achieve a breakthrough in cross-domain capabilities. The combat management capabilities of the military are shifting towards full-domain coordination such as land, sea, air, space, electricity, network, cognitive domain, and social domain. To adapt to the full-domain environment, the combat management system needs to have the following functions: a resilient and redundant communication system, flexible and secure data operation; artificial intelligence and machine learning directly extract and process data from sensors, and conduct decentralized integration and sharing; segmented access according to confidentiality levels to meet perception, understanding and action needs. On this basis, it is also necessary to provide reconnaissance and surveillance, tactical communications, data processing, network command and control, etc. to the troops.

The future combat management system will focus on security processing, connectivity, data management, application, sensor integration, and effect integration capabilities, optimize data sharing, collaborative operations, and command and control in the entire combat domain, and support decision-making advantages from the tactical level to the strategic level. There is only one purpose: to give commanders the ability to surpass their opponents.

The Russian-Ukrainian conflict has become a testing ground for advanced military technologies, especially new technologies and products of information technology and intelligence. The practice of war fully reflects the extreme importance of agile kill chains in modern warfare, and the combat management system is the core and soul of it. Therefore, we must attach great importance to the construction and development of combat management systems at all levels to provide network information system support for winning high-end wars under strong confrontation conditions.

The core task of combat management is the integrated use of information and firepower. From the experience of the U.S. C2BMC system, it is clear that aerospace defense operations often span multiple theaters, with high demands for information accuracy and timeliness. A centralized management mechanism for integrated information and firepower is needed. Integrated information and firepower can fully leverage the predictability of ballistic targets and the characteristics of cross-theater operations. Before combat, sensors, interception weapons, and other resources should be strategically planned based on possible incoming ballistic threats. During combat, real-time prediction of ballistic trajectories allows for dynamic generation of sensor detection plans and weapon interception plans. These comprehensive combat plans help in the unified scheduling of sensor and interception weapon resources, effectively avoiding resource scheduling conflicts under multiple-target conditions. This approach maximizes the combat effectiveness of the equipment system under limited resources. To serve future high-intensity, high-tech warfare, the system's overall design should focus on combat effectiveness, iteratively developing a multi-level, integrated combat management system that achieves unified command and control capabilities under joint operations. By orienting towards practical combat, adopting a spiral development model

of "research, test, and trial," and deepening scientific understanding of combat tasks through management practice, the system's practical combat capability can be progressively enhanced.

Following the Integration and Development Principles of Joint and Domain-Specific Combat Management. Given the complexity of joint combat systems, it is worth considering whether a combat management system that directly controls all-domain resources can be established. From the construction of the U.S. Joint All-Domain Command and Control (JADC2) and systems like ABMS and C2BMC, on one hand, it is essential to advance the top-level design and integration of joint combat management systems while simultaneously developing domain-specific combat management systems. The principle of "develop first, then integrate" reflects the objective evolution of complex, large-scale systems. Although the Chinese military has a late start in combat management system construction, it is challenging to quickly form a full-domain command and control system supporting joint operations. In constructing the joint combat management system for the entire military, it is crucial to address the joint design issues between different domains and establish top-level design frameworks and technical constraints. Domain-specific combat management systems should be developed, tested, and validated before integration into the joint combat management system, which is a feasible approach.

From the operational management construction principles summarized from the U.S. ABMS system, it is evident that the U.S. is advancing the appropriate separation of command and control functions. This separation clarifies the interface relationships between combat management and command, planning, and intelligence, which has guiding significance for the current command and control system construction. The separation principle reflects a refined division of labor between command art and control science, promoting a focus on enemy assessment and macro decision-making by commanders, while the combat management system performs specialized and precise control based on the commander's intent. This organization method enables task-oriented command through information systems, allowing for autonomous coordination and efficient collaboration under unified guidance, thus adapting to complex and changing

battlefield environments.

The U.S. is actively advancing distributed command and control and combat management models, and has initially proposed applications for distributed architecture. As shown in Figure 1, the distributed model does not mean completely dispersing functions but retains independent combat management functions within individual systems. Through the coupling of support and support relationships, the system's information decision-making advantages are further enhanced.

Distributed models are an effective organizational management mode for large-scale resistance, requiring persistent combat capabilities even under communication constraints or interruptions. Completely dispersed functions deepen the system's dependence on ideal communication conditions, resulting in significantly reduced combat effectiveness under limited or interrupted communication, potentially becoming a weak link in the combat system and failing to meet the needs of sustained combat. Therefore, it is necessary to develop a self-coordinating distributed combat management model that maximizes the coherence of independent decision-making solutions at distributed control nodes, ensuring that distributed decision-making solutions are compatible and coordinated without conflicts or omissions.

CONCLUSIONS

Combat management systems generally have the characteristics of integration, automation, optimization, and real-time. The combat mode of modern warfare is complex, the battlefield scale is expanding, and the requirements for force control, resource integration, and task scheduling are increasing. It is necessary to achieve system integration. The French Army's "Scorpion" system fully integrates tanks, armored vehicles, infantry fighting vehicles, unmanned ground vehicles, drones, and attack helicopters into the same combat group, and links all platforms and combat units in the task group.

With the increase in combat elements in modern warfare and the expansion of battlefield perception space, the command automation system that relies heavily on people can no longer fully adapt, and the system must be automated. All operating functions of Pakistan's combat management artillery control system are fully automated, "providing automated solutions for preparing, coordinating, transmitting, executing, and modifying fire support plans and shooting plans."

The pace of modern warfare operations is accelerating, and battlefield data is massive. It is necessary to quickly grasp the situation and make decisions efficiently, and it is necessary to achieve system optimization decisions. Military powers are combining artificial intelligence, cloud computing, the Internet of Things, and big data technologies to facilitate faster decision-making in multi-domain operations. Traditional combat management systems place more emphasis on engagement sequences and combat rules based on pre-established rules. However, future wars will highlight the confrontation between systems. It is impossible to exhaust all kinds of situations in advance, and the battlefield information that needs to be mastered will become more complex and massive. To this end, the armies of various countries have begun to abandon the traditional method of developing combat management systems for each combat domain separately, and are centered on the network and supported by artificial intelligence, trying to help commanders make combat decisions more quickly and realize the real-time connection between sensors in each combat domain and any shooter.

The combat management system will promote the implementation of combat concepts. The "Advanced Combat Management System" developed by the US Air Force plans to connect all services and their weapon platforms in real time in a military Internet of Things. Its core is to seamlessly link various intelligence reconnaissance platforms, command and control platforms, strike platforms and combat management platforms with various cross-domain capabilities, convert intelligence and target indication data into timely and usable information, shorten the "discovery-positioning-tracking-targeting-strike-evaluation" cycle, and execute combat operations at a speed that opponents cannot keep up with. The Russian army proposed the theory of "military unified information space" and organized the development of an "automatic control system" for integrated joint operations of land, sea and air networks. By establishing a network-centric command model, it attempts to integrate the command, communication, reconnaissance, firepower, and support of the entire army, realize cross-domain operations in the true sense, and enhance battlefield situation awareness and combat command efficiency.

The combat management system will rely on artificial intelligence technology. The application of artificial intelligence will not only cause the capabilities of weapon systems to multiply, but will also fundamentally change the realization of the OODA loop. In the future combat management system, artificial intelligence technology will become the core support and driving engine, and the key factor is the quality of the algorithm. The system will have built-in upgradeable artificial intelligence, and people will be in a supervisory or collaborative state to minimize manual input, spontaneously identify and classify threat targets in the combat environment, autonomously evaluate and weigh, and automatically allocate weapons, thereby providing adaptive combat advantages and decision-making options.

For example, the "Intelligent Autonomous System Strategy" released by the US Navy in July 2021 aims to accelerate the development and deployment of intelligent platforms through a highly distributed command and control architecture, integrate unmanned systems, artificial intelligence, and autonomous driving technologies, and realize future combat decisions facilitated by intelligent autonomous systems. The

Russian military is developing more than 150 artificial intelligence projects, one of the focuses of which is to introduce artificial intelligence into the command and control system, adapt intelligent software to different weapon platforms, achieve the unification of the physical domain and the cognitive domain, and double the combat effectiveness in an intelligent empowering way.

The combat management system will achieve a breakthrough in cross-domain capabilities. The combat management capabilities of the military are shifting towards full-domain coordination such as land, sea, air, space, electricity, network, cognitive domain, and social domain. To adapt to the full-domain environment, the combat management system needs to have the following functions: a resilient and redundant communication system, flexible and secure data operation; artificial intelligence and machine learning directly extract and process data from sensors, and conduct decentralized integration and sharing; segmented access according to confidentiality levels to meet perception, understanding and action needs. On this basis, it is also necessary to provide reconnaissance and surveillance, tactical communications, data processing, network command and control, etc. to the troops.

The future combat management system will focus on security processing, connectivity, data management, application, sensor integration, and effect integration capabilities, optimize data sharing, collaborative operations, and command and control in the entire combat domain, and support decision-making advantages from the tactical level to the strategic level. There is only one purpose: to give commanders the ability to surpass their opponents.

The Russian-Ukrainian conflict has become a testing ground for advanced military technologies, especially new technologies and products of information technology and intelligence. The practice of war fully reflects the extreme importance of agile kill chains in modern warfare, and the combat management system is the core and soul of it. Therefore, we must attach great importance to the construction and development of combat management systems at all levels to provide network information system support for winning high-end wars under strong confrontation conditions.

In order to better respond to security threats under the new situation, first of all,

the most fundamental thing is to strengthen the concept innovation in the military field. Reform and innovation are one of the most important driving forces for improving the combat effectiveness of the army. It is necessary to actively propose new concepts, formulate new strategies, and develop new weapons based on the background of changes in war styles and its own needs. Secondly, pay attention to the coordination of various services in combat and give play to the synergy of the system. As the scope of war develops to a wider space, cross-domain operations have become an important manifestation of war. We must make full use of resources and capabilities in specific space fields and use global thinking to command battles. Finally, pay attention to the application of technologies such as artificial intelligence in the military field. It can be seen that technologies such as artificial intelligence have great potential in the military field and have become one of the key technologies of the US military's kill network. This is not only the technical basis for relying on all-domain operations, but also a necessary technical condition for future unmanned warfare.

REFERENCES

1. Joint Chiefs of Staff. Joint publication 3-01. Countering Air and Missile Threats. 2017:3.
2. Joint Chiefs of Staff. Joint publication 3-13.1. *Electronic Warfare*. 2012: GL-6.
3. Liu Jixian. Military Management. Beijing: Military Science Press, 2009:288.
4. Zhao Guohong. Research on combat management system. *Science and Technology Review*, 2019, 37(13): 6-13.
5. Feng Mang, Qian Ning. Overview of the Development of the US Army's Advanced Battle Management System (ABMS). 2020-11-14. URL: www.sohu.com/a/431852764_743125
6. Douglas A. B. Command and control imperatives for the 21st century: The next areas of growth for ABMS and JADC2. 2021-05-27. URL: www.mitchellaerospacepower.org/wp-content/uploads/2021/06/C2ISR_Policy_Paper_27-final.pdf
7. Missile Defense Agency (MDA). Missile defense agency fiscal year 2009 (FY 09) budget estimates overview. 2009-01-12. URL: www.doc88.com/p-584670392917.html
8. Zhu Hong. U.S. Air Force releases ABMS technology categories [EB/OL]. 2020-06-09. URL: www.i-zb.com/21448.html
9. David S. Ukrainians use Telegram Chatbot to track and target Russian troops [EB/OL]. 2022-03-28. URL: www.news.hookupcellular.com/ukrainians-use-telegram-chatbot-to-track-and-target-russian-troops/
10. В Україні запустили бот для повідомлень про пересування диверсантів, війська та техніки Росії [EB/OL]. 2022-02-26 URL: www.ms.detector.media/trendi/post/29048/2022-02-26-v-ukraini-zapustyty-bot-dlya-povidomlen-pro-pere-suvannya-dyversantiv-viysk-ta-tekhniky-rosii
11. Stew M. Pentagon speeds tactical software to Ukraine [EB/OL]. 2022-05-17. URL: www.nationaldefensemagazine.org/articles/2022/5/17/pentagon-speeds-tactical-software-to-ukraine

12. AFRL. Tactical Assault KIT (TAK) [EB/OL]. 2022-05-30. URL: www.afresearchlab.com/technology/information-technology/tactical-assault-kit
13. U.S. Department of Homeland Security. ATAK increases situational awareness, communication and alters understanding of actions across agencies [EB/OL]. 2022-05-30. URL: www.dhs.gov/science-and-technology/news/2017/11/17/snapshot-atak-increases-situational-awareness-communication
14. Soldier systems. USSOCOM PEO-SOF digital applications update [EB/OL]. 2021-05-19. URL: www.soldiersystems.net/2021/05/19/ussocom-peo-sof-digitalapplications-update
15. Panasonic. 5 Reasons the Toughbook N1 Tactical EUD belongs in your KIT [EB/OL]. 2021-03-22. URL: www.na.panasonic.com/us/sites/default/files/2021-03/11482522_pna_atak_infographic_fpjb.pdf#:~:text=Designed%20specifically%20for%20situational%20awareness%20in%20tactical%20settings%2C,elements.%204%20ALWAYS%20EVOLVING%20TO%20MEET%20NEW%20CHALLENGES.
16. Tacadmin. What is ATAK? [EB/OL]. 2022-06-05. URL: www.tacticalblueprint.com/what-is-atak/
17. U.S. Department of Homeland Security. ATAK increases situational awareness, communication and alters understanding of actions across agencies [EB/OL]. 2017-11-17. URL: www.dhs.gov/scienceand-technology/news/2017/11/17/snapshot-atak-increases-situational-awareness-communication
18. Department of Defense. Common warfighting symbology (MIL-STD-2525B) [EB/OL]. 2022-06-05. URL: www.mapsyms.com/ms2525b_ch1_full.pdf.
19. Paul Mcleary. Close air support timeline cut; Wait for tech was too long [EB/OL]. 2019-05-22. URL: www.breakingdefense.com/2019/05/close-air-supportslashed-to-seconds-wait-for-tech-was-too-long/.
20. @kms_d4k EB/OL. 2022-05-11. URL: www.twitter.com/kms_d4k/status/1524506104192974849?ref_src=twsrc%5Etfw
21. Defence of Ukraine. (@Defence U) [EB/OL]. 2022-05-11 URL: www.twitter.com/DefenceU/status/1524438980191731717?ref_src=twsrc%5Etfw
22. Ray P. Uber-style tech helped wipe out almost entire Russian battalion

[EB/OL]. 2022-05-15 URL: www.veteranweb.asn.au/news/uber-style-tech-helpedwipe-out-almost-entire-russian-battalion/

23. Wiki.17th Tank Brigade (Ukraine) [EB/OL]. 2022-06-06. URL: [www.military-history.fandom.com/wiki/17th_Tank_Brigade_\(Ukraine\)](http://www.military-history.fandom.com/wiki/17th_Tank_Brigade_(Ukraine))

24. Gisarta. GIS Art automated command and control system [EB/OL]. 2022-06-06. URL: www.gisarta.org/en/index.html.

25. Jonathan L. The reason Ukraine's use of off-shelf software is destroying Russia's military [EB/OL]. 2022-05-11 URL: www.thelowdownblog.com/2022/05/the-reason-ukraines-use-of-off-shelf.html#:~:text=GIS%20Art%20for%20Artillery%2C%20or%20%22GIS%20Art%22%20for,to%20trigger%20pull%20from...20%20minutes%20to%2030%20seconds.

26. Valeria A. Come funziona l'app ucraina Gis Art che localizza i bersagli russi da colpire .2022-05-13 URL: www.fanpage.it/innovazione/scienze/come-funziona-lapp-ucraina-gis-art-che-localizza-i-bersagli-russi-da-colpire/

27. Alipay Chengdu Team: Analysis and Thoughts on Didi's Intelligent Scheduling [EB/OL]. 2017-01-15. URL: www.jianshu.com/p/fd80741bb6fd

28. Strategic Technology Office. Adapting cross-domain killwebs (broad agency announcement HR001118S0043). 2018-08-03 URL: www.darpa.mil/program/adapting-cross-domain-kill-webs

29. DARPA. Creating cross-domain kill webs in real time [EB/OL]. 2020-09-21 URL: www.techxplore.com/pdf519898086.pdf

30. ITU Telecommunication Standardization Sector.Overview of the Internet of things [EB/OL]. 2022-06-10. URL: www.itu.int/rec/T-REC-Y.2060-201206-I/en

31. Liu Ding. Infrastructure of Didi IoT[EB/OL]. 2018-12-26. URL: www.blog.didiyun.com/index.php/2018/12/26/iot-infrastructure/

32. Ashley C. Gis way of working the Ukrainian army's“Uber of guns”:Geolocating Russian targets in 30 seconds [EB/OL]. 2022-06-07. URL: www.spamchronicles.com/gis-way-of-working-the-ukrainian-armys-uber-of-guns-geolocating-russian-targets-in-30-seconds/ .

33. Wang Ben, Liu Chunyang, Xu Zhe. A brief discussion on Didi's order

- dispatching algorithm [EB/OL]. 2019-09-26. URL: www.cloud.tencent.com/developer/article/1513756
34. Zhao Guohong, Gao Runfang, Jiang Guangde, et al. A multi-to-multi cargo scheduling optimization allocation method based on available resource coding. *Chinese Patent*: CN114493047B, 2022-06-14.
35. Raytheon Intelligence and Space. Deterrence via faster decision-making [EB/OL]. 2022-02-14. URL: www.raytheonintelligenceandspace.com/news/2022/02/14/deterrence-faster-decision-making
36. Aleksei K AFP. Smartphones, crowdsourcing play crucial role in defence of Ukraine [EB/OL]. 2022-03-24 URL: www.central.asia-news.com/en_GB/articles/cnmi_ca/features/2022/03/24/feature-03
37. Zhao Guohong. System-centric warfare: the top-level operational concept of future wars. *Journal of Command and Control*, 2021, 7 (3): 225-240.
38. History Room of People's Education Press. Modern Era of the World: Volume I. 2nd ed. Beijing: *People's Education Press*, 2006.
39. ZHAO Guohong. Research on System Based Combat Management System. URL: www.sohu.com/a/550243009_358040
40. ZHAO Guohong. SoS-Based Battle Management System. *Science & Technology Review*, 2019, 37(13), P.6-13.
41. ZHAO Guohong. Review on Battle Management System from Kill Chain Application in the Russia-Ukraine Conflict. *Tactical Missile Technology*, 2022 (4), 1-16.
42. WANG Hu, DENG Dasong. Research on Functional Composition and Operational Capability of C2BMC System. *Tactical Missile Technology*, 2019 (4): 106-112.
43. LI Junchao, ZHANG Zhanyue, XU Li. The Capability of US C2BMC System. *Journal of Academy of Equipment*, 2013, 24 (5): 78-82.
44. YANG Xuerong, CHENG Zilong, XIAO Longlong. Research on Missile Defense Command, Control and Battle Management System. *Journal of Command and Control*, 2015, 1 (1): 86-91.

45. WANG Gang, WANG Mingyu, YANG Shaochun, et al. Research of Anti-missile Battle Management Technique. *Modern Defense Technology*, 2012, 40 (1): 26-30.
46. ZHOU Hairui, ZHANG Zhen. U. S. Air Force Advanced Battle Management System. *Command Information System and Technology*, 2020, 11 (4) P. 57-63.
47. LIU Yutong, ZHANG Yang. Progress and Enlightenment of the US Air Force Advanced Combat Management System Project. *Aerodynamic Missile Journal*, 2021 (5): P. 13-16.
48. FENG Mang. Overview of the Progress of the US Air Force Advanced Operations Management System in 2022. (2023-02-05) URL: www.mp.weixin.qq.com/s__biz=MzI4OTkyNDgxNA=&mid=2247783028&idx=8&sn=27274ec6fa1721b3a1eef569b4b9a8fa&chksm=ec2961d5db5ee8c3085e683fa5da725d0b84340b657d22cd02515fab7a7918bd04a5863916a1&scene=27
49. WANG Tong, LI Lei, JIANG Qi. Distributed Battle Management Program Promotes the Development of Distributed Command and Control Capability. *Tactical Missile Technology*, 2019 (1), P. 25-32.

APPENDIX