DOI: https://doi.org/10.52651/vr.a.2023.3.59-73
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2023, Number 3, Page 59-73

OPPORTUNITIES AND DIRECTIONS FOR THE EVOLUTION OF COMMAND AND CONTROL SYSTEMS IN THE CONTEXT OF MULTI-DOMAIN OPERATIONS

Andras TOTH, Tibor FARKAS

ARTICLE HISTORY

Submitted: *05. 10. 2023*
Accepted: *06. 12. 2023*
Published: *31. 12. 2023*

ABSTRACT

The military conflicts of recent times have highlighted the need for modern military operations to focus on multi-domain operations, which requires a transformation of the command and control system, by creating mobile and flexible headquarters that can provide relevant information at any time, even during redeployments and redeployments. Cloud computing can be used to integrate data collection tools, ensuring fast and accurate analysis of large amounts of incoming data. A private 5G network can provide a secure, high-speed and reliable communication environment for cloud-based command and control systems. This network will enable real-time information transfer, facilitate rapid decision-making processes and enable the deployment of autonomous vehicles and drones. The authors have also explored capabilities that support the deployment of autonomous vehicles and drones, enabling commanders to conduct intelligence and surveillance more effectively. By leveraging technology and advanced communications systems, commanders can lead their teams in a dynamic environment while providing a high level of situational awareness. This integration of information and mobility allows commanders to react quickly and decisively, ultimately increasing their effectiveness on the battlefield.

KEYWORDS

command and control, multi-domain operations, command posts, 5G, cloud computing.

INTRODUCTION

The Russian-Ukrainian conflict seems to be overturning many military principles that were once considered fundamental and that the armies of the present day are typically designed to uphold. There has been no preparation for symmetrical warfare in recent decades, with the emphasis shifting to peacekeeping operations, where asymmetric traits are typical. Accordingly, the conceptual and practical implementation of command and control (C2) has moved in a direction that does not meet the requirements of conventional multidimensional operations. The abbreviation "C2" stands for both the conceptual side of command and

control, the command, control, cooperation, and coordination scheme. However, it can also be applied to the physical components that provide the interconnection. NATO's Allied Joint Doctrine (AJP-01) emphasizes that command and control are related concepts, generally used together but not synonymously. The military leader, the commander at all levels, is an expert in decision-making, motivating, and directing to accomplish a given task. His or her main task is personal leadership and decision-making while sharing accountability and command and control with his or her tribe (NATO, 2022).

This divergence of emphasis has led to a lack of preparedness for symmetrical warfare, with potentially devastating consequences. To address this problem, it is important to re-evaluate current C2 strategies and make them more relevant to the needs of traditional multi-domain operations. This could include the incorporation of new technologies and tactics, as well as improved communication and coordination between different military disciplines. In addition, a new emphasis on training and preparation for symmetric warfare, including scenarios involving both conventional and asymmetric threats, is needed. By taking these steps we can better ensure that our soldiers are prepared for any type of conflict that may arise in the future.

This was recognized by three senior US Army leaders (Lt. Gen. Milford "Beags" Beagle, Brig. Gen. Jason C. Slider, Lt. Col. Matthew R. Arrol) who examined the lethality and transparency of the modern battlefield through the example of the Battle of Chornobayevka during the Russian-Ukrainian conflict, using the coordinated application of multi-domain effects on the warfare function. The article highlights the need for a rethinking of command and control in this new era of warfare. Faced with the immediate threat, armies must transform their command and control systems to incorporate the principles of multi-domain operations (MDO). To fight and win in large-scale combat operations in the modern theatre, the Army's command posts must become more resilient, agile and responsive without sacrificing effectiveness. Otherwise, command posts become places where commanders go to die (Beagle et. al., 2023).

1 MULTI-DOMAIN OPERATIONS

Under the concept of multi-domain operations (MDO), in the future, multiple operations will be conducted simultaneously on the battlefield, including space, information, and cyber operations, in addition to traditional air, land, and naval military operations. In the event of a major power conflict, this will be the most likely form of warfare in the coming decades.

The future of military operations will be complex and multifaceted. With the emergence of space, information, and cyber operations, navigating the battlefield will become an even more challenging environment alongside traditional air, land, and naval military operations. Combat in this new form of warfare will require a high degree of

coordination and cooperation between the different branches of the military, as well as other government agencies and private sector partners.

Collecting and analyzing large amounts of data in real time will be critical to success in the field. In addition, advanced technologies such as artificial intelligence, autonomous systems, and robotics will play an increasingly important role in future military operations. Looking ahead to the coming decades, it is clear that those who adapt quickly to this changing environment will be best placed to engage in any great power conflict successfully. To this end, military organizations must prioritize developing and implementing cutting-edge technologies that enable real-time data collection and analysis. Significant investment in research and development and a willingness to embrace emerging technologies such as artificial intelligence, autonomous systems, and robotics, as mentioned above, will be required. In addition to technological developments, military leaders will also need to prioritize the training and education of personnel to ensure they have the skills to operate new systems effectively.

Ultimately, success on the battlefield depends on the ability of the military to adapt quickly to changing circumstances and leverage technology to gain a strategic advantage over adversaries. Those who can do so will be well placed to engage successfully in future conflicts with the great powers. In addition, military leaders need to establish clear communication channels and protocols to ensure effective coordination between different units and branches. Doing so will enable them to respond quickly and decisively to any threats or challenges during combat operations.

By investing in technology and personnel development, military organizations can increase their preparedness and effectiveness against evolving security threats. In addition, training programs focusing on leadership development and cross-functional collaboration can help to develop a culture of innovation and adaptability in the military. At the same time, it is particularly important in today's rapidly changing global security environment, where new threats and challenges are emerging at an unprecedented pace. By adopting these strategies, military leaders can ensure that their organizations remain resilient and resilient in the face of adversity. Ultimately, this will help them fulfil their mission of protecting their countries and promoting peace and stability worldwide (Perkins, 2017).

MDO integration combines autonomous platforms with intelligent command and control systems to achieve tasks and goals. However, current C2 systems struggle to manage the operational tempo between autonomy, people, and battlefield dynamics. Internet of Battlefield Things (IoBTs) such as unmanned aerial, ground, maritime, and space vehicles (UxVs) create benefits and problems for C2 systems. The ubiquity, dispersion, complexity, stochasticity, and heterogeneity of IoBTs will require a change in the way C3I (Command, Control, Communications, and Intelligence) decision-making and support systems acquire situational awareness, structure operational problems, assess courses of action, and provide feedback on execution. The collective intelligence nature of IoBTs can create battlefield

dynamics that only IoBT itself can address. MDO and cross-domain capabilities will increase the complexity of situational awareness and challenge the nature of warfare. How, for example, does a commander decide between autonomous combat and long-range artillery or cyber-attacks? How do they integrate data from integrated forces to create a unified picture of what is happening?

The nature of the effects - whether initiated by the IoBT or by the commander's decision - creates new dynamics that require new battlefield concepts that combine human command with machine control. Disrupting enemy decision-making has always been a goal in combat, but automated C2 tools and IoBT technologies can rapidly assemble, adapt and reassemble the force structure and implications to achieve military objectives. The MDO battlefield also requires new concepts of operations that take full advantage of the potential of artificially intelligent and autonomous systems (Russell et. al., 2019).

The advent of MDO and the integration of advanced technologies will undoubtedly transform the nature of warfare. Combining human command and control with machine control can improve military decision-making, enabling more effective targeting and mission execution. Furthermore, artificially intelligent and autonomous systems will enable new operations concepts that can exploit these technologies' potential. However, it is important to consider the ethical implications of such warfare developments and ensure that they are used responsibly. As we move towards a more technologically advanced battlefield, we must maintain a balance between human decision-making and machine control to ensure optimal outcomes for both military objectives and humanitarian concerns.

2 REQUIREMENTS FOR THE OPTIMIZATION OF COMMAND AND CONTROL SYSTEMS

Optimizing command posts requires reducing the reliance on the physical dimension (assets), increasing the use of the information dimension (data), and maximizing the ability to interact with the human dimension (commanders). This approach involves leveraging technology and data analytics to streamline operations and improve decision-making processes. Resources can be allocated more efficiently by reducing the need for physical assets such as vehicles and equipment. In addition, using data can provide valuable insights into trends and patterns that can inform strategic planning.

Finally, by enhancing communication and collaboration between commanders, the overall effectiveness of command posts can be significantly improved. This perspective requires a shift towards adopting new technologies and operational methods, but ultimately can greatly improve military operations. In today's rapidly evolving military environment, commanders must look for new ways to optimize their operations. One key strategy is to leverage data analytics to gain valuable insights into the causes of changes in their environment (trends, patterns). As a result, they can make more informed decisions about resource allocation and streamline their processes for maximum effectiveness. Another

important factor is communication and collaboration between command posts. By promoting a culture of openness and teamwork, headquarters can work together more effectively and achieve greater success on the battlefield. While these changes may require a shift in mindset, the potential benefits are significant. With the right approach, new technologies and operational methods can help military organizations achieve their goals more effectively than ever before.

Developing an effective and survivable command post in large-scale operations requires focusing on four key principles. The first principle is to ensure the command post is mobile and can be rapidly deployed to different locations as required. This allows commanders to respond quickly to changing conditions on the battlefield. In a conflict, mobility is essential, whether tactical or strategic. Its importance comes from how it relates to the creation of opportunities and how it gives the actor multiple strategies for thinking, fighting, moving, and planning. Moreover, immobility makes the actor a convenient target. Both physical and mental immobility are possible. Because cognitive immobility limits the actor's alternatives, his future behavior becomes predictable, making him more vulnerable to intentional harm.

The second principle focuses on integrating advanced technologies to improve data collection, analysis, and dissemination. This will enable commanders to make informed decisions based on real-time information and gain a tactical advantage over the enemy. Armies can integrate these technologies into systems comprising subsystems that communicate with each other to maintain balance. Sustainment, the physical manifestation of the system's equilibrium, is essential for its proper functioning, and the actor must aggressively target and defend it. Mapping the adversary's system helps to identify barriers and bottlenecks that lead to exhaustion and depletion. In large-scale combat operations, actors must operate to fend off sophisticated attacks against their sustainment network.

The third principle is to establish a clear line of communication between all members of the command, including those in the field. This guarantees that everyone can access critical information and work together seamlessly towards a common goal. Information is a crucial element of military operations, and the effectiveness of operations often depends crucially on the flow of information. Another serious problem can be information manipulation, including delays, misinformation, and delayed or distorted data, which can cause instability and misrepresentation. Protecting the integrity of information is key in warfare, and actors must contribute to properly functioning the system while remaining vigilant about their information (Fox, 2021).

Finally, it is essential to focus on human factors such as leadership, training, and morale. By investing in these areas, commanders can maximize their ability to interact with their teams and make informed decisions under pressure. In addition to the abovementioned principles, other factors must be considered for success in combat. One such factor is the importance of intelligence and analysis. By gathering and analyzing

intelligence information, commanders can better understand the enemy's capabilities and intentions and thus plan and execute operations more effectively. It is also important to consider the impact of terrain on operations. Understanding the impact of terrain on movement and communications can help commanders plan and execute operations more effectively. Finally, it is important to maintain flexibility in planning and execution. On the battlefield, the ability to adapt to changing conditions can mean the difference between success and failure. Suppose commanders consider these factors in addition to the command principles outlined above. In that case, they can increase their chances of victory over the enemy.

Recognizing the challenges of the current environment, the cross-cutting operation stresses that command posts must follow the principles of agility, alignment, resiliency, and depth as an element of the command system. Examining these four principles will help define what it means to develop an acceptable, reliable, and comprehensive command post that is effective and survivable in a large-scale military operation against a strong adversary.

2.1 Agility

The command posts are currently facing an endless cycle of installation, decommissioning, relocation, and redeployment to maintain operational efficiency and effectiveness. Reducing the number of tents and mounting systems on vehicles can improve mobility. However, it does not eliminate the need for constant set-up and configuration. To address this problem, militaries are exploring new approaches to designing and deploying command posts, such as modular, prefabricated structures that can be quickly assembled and disassembled.

These structures can be customized to meet specific mission requirements and are easily transported by air or ground. By using these innovative solutions, forces can improve the ability to rapidly deploy command posts in any environment, increasing operational readiness and effectiveness on the battlefield. Using modular and prefabricated structures also brings many other benefits to headquarters. For example, these structures are often more cost-effective than conventional command posts because they can be produced in large quantities and require less time and human resources to assemble. In addition, modular structures can be easily adapted to changing mission requirements or operational environments, providing greater flexibility and agility for military forces.

Furthermore, these structures can be equipped with advanced technologies such as satellite communication systems, secure data networks, and real-time situational awareness tools to increase the efficiency of command and control operations. Overall, using modular and prefabricated structures for command posts represents a promising new approach to military operations that can greatly enhance operational readiness and effectiveness on the battlefield.

2.2 Alignment

Current systems and on-site servers cannot adequately support effective C2 processes nor maintain a steady flow of relevant data to make the best decisions. This requires moving to the cloud and improving data servers and data federation concepts. A data grid is a decentralized data architecture that combines creating, managing, and sharing data within and between domains. The data fabric automates data integration, reducing dependencies on individual platforms or data stores.

The move to the information dimension requires new methodologies and competencies to achieve efficient operations. Integrating sensors, weapon systems, and decision-makers through machine learning and artificial intelligence can improve efficiency and enable faster decision-making and more effective response to dynamic situations. Cloud computing and distributed systems can further enhance the scalability and flexibility of information infrastructure, ensuring that teams stay at the leading edge and achieve optimal efficiency.

Military organizations can also benefit from deploying emerging communications technologies, such as 5G networks, providing high-speed connectivity and low latency for real-time data transmission. In addition, using unmanned aerial vehicles (UAVs) and autonomous ground vehicles (AGVs) can reduce the risk to human personnel in hazardous situations while providing enhanced situational awareness and intelligence capabilities. Furthermore, integrating Augmented Reality (AR) and Virtual Reality (VR) technologies can provide an immersive training experience for military personnel, allowing them to simulate different scenarios and develop their decision-making skills.

Altogether, using advanced technologies can greatly improve the operational capabilities of military organizations, enabling them to achieve their objectives with greater efficiency and effectiveness. Adaptation to new technologies is key for military organizations to maintain their competitive advantage in modern warfare. By investing in cutting-edge technologies such as artificial intelligence (AI) and Internet of Things (IoT), military personnel can gain real-time insights into the battlefield, enabling them to make informed decisions quickly and efficiently. Moreover, integrating these technologies can also lead to the developing of autonomous systems that can perform tasks with minimal human intervention.

This reduces the risk of casualties and allows military personnel to focus on more strategic tasks. In addition, drones and other unmanned vehicles can provide valuable intelligence and reconnaissance capabilities, allowing military organizations to gather critical information without risking their personnel. Advanced communications systems can also greatly improve coordination and cooperation between different units, allowing them to work seamlessly towards a common goal. Overall, embracing emerging technologies is essential for military organizations to achieve alignment and ensure that the established command posts contribute to maintaining the dominance gained on the battlefield.

2.3 Resiliency

Resilience in the military is another key benefit of using emerging technologies. Adapting and responding quickly to changing situations enables military organizations to withstand unexpected challenges and threats better. This resiliency can lead to more successful missions and effectiveness in achieving strategic objectives. In addition, new technologies can enhance the safety of military personnel by providing advanced surveillance and communication systems.

Moreover, it can reduce the risk of casualties and improve situational awareness, allowing for more informed decision-making on the battlefield. In addition, these technologies can also improve the efficiency and speed of operations, enabling faster reaction times and better coordination between units. However, it is important to balance the use of technology with appropriate training and preparation to ensure that military personnel have the necessary skills to use these tools effectively in combat situations. Another important aspect of military technology is cyber security. As military operations become increasingly reliant on digital networks and communications systems, they become more vulnerable to cyber-attacks by hostile actors.

Therefore, this highlights the need for robust cybersecurity measures to protect sensitive information and prevent unauthorized access to critical systems. Cyber resilience is also key, allowing military units to recover quickly from cyber-attacks and continue operations without major disruptions. Therefore, investing in cyber security and resilience is as important as investing in advanced military technology. As technology continues to evolve, so does the risk of cyber-attacks. Military units are particularly vulnerable to these attacks, which can compromise sensitive information and critical systems. To combat this threat, robust cybersecurity measures are needed to prevent unauthorized access and protect against hostile actors. By prioritizing these measures, military units can ensure they are well prepared to face the evolving threat of cyber-attacks and protect their critical assets from damage.

Command posts and communications networks are particularly vulnerable to cyber-attacks compromising sensitive information confidentiality, integrity, and availability. Therefore, military units must implement robust cybersecurity protocols and conduct regular training and exercises to enhance their cyber defense capabilities. As modern warfare increasingly relies on technology, the complexity and frequency of cyber threats are expected to increase, making cybersecurity a key priority for military leaders worldwide.

2.4 Depth

The depth of military operations extends operations in time, space, or cognitive sense. Multi-domain operations allow teams to maximize effectiveness in the human, physical, and information dimensions. By leveraging deeper planning and thinking, teams

can achieve better situational awareness, decision-making, coordination, and rapid adaptation. This approach also increases efficiency and effectiveness by sharing information and resources. As a result, forces can adapt quickly to changing circumstances and achieve their goals more quickly and accurately.

Ultimately, MDOs are critical to maintaining strategic advantage on the battlefield and ensuring mission success. In addition to their importance in warfare, MDOs significantly impact national security and global stability. By harnessing the power of technology and information, military forces can better understand their adversaries and respond more effectively to emerging threats. They also enable greater cooperation between different forces and with allied nations and other partners. This cooperation is essential to build trust and promote peace in an increasingly complex and interconnected world. Ultimately, the success of MDOs depends on the ability of military leaders to integrate different capabilities and technologies into a coherent strategy that supports overall mission objectives. However, with careful planning and execution, these operations can help ensure the safety and security of people worldwide.

The depth of military operations requires a comprehensive understanding of the operational environment and the ability to adapt to changing circumstances. It also requires effective communication and cooperation with civilian agencies, international partners, and local communities to achieve common goals and minimize potential negative impacts. In addition, military operations must be conducted in accordance with international law and human rights norms to preserve legitimacy and avoid undermining the values they seek to protect. In addition, a clear exit strategy and post-conflict reconstruction plan are essential to ensure long-term stability and prevent a relapse into conflict.

2.5 Data-centric command posts

Data-centric command posts are replacing network-centric ones and relying on the help of data processing, security, and operations specialists. Such an approach allows commanders to adapt and tailor command and control systems based on specific operational requirements and managerial preferences. The as-a-service (aaS) model outsources maintenance and enables rapid adoption of new technologies and mobility. Military units can leverage cloud services to improve operational capabilities, gain global access to critical information and applications, reduce costs, and collaborate more effectively. As technology advances, the aaS model is expected to become more prevalent in military operations, enabling militaries to stay ahead of emerging threats and maintain their information superiority on the battlefield. As technology evolves, the aaS model will likely become even more important for military organizations that want to maintain their competitive edge in an increasingly complex and dynamic global environment.

The adoption of the aaS model will bring significant benefits to modern warfare. With its cost-effective and on-demand approach, militaries can access state-of-the-art technologies and expertise without investing in expensive infrastructure or training programs. This can reduce the burden on military budgets and improve the speed and efficiency of operations. The aaS model also allows for greater cooperation and interoperability between the different branches of the military and with international partners. This will facilitate joint missions and enhanced information sharing, essential for successful outcomes in today's complex security environment. Looking ahead, it is clear that the aaS model will play a critical role in shaping the future of military operations. As a result, data-centric command posts are becoming increasingly important, enabling military leaders to make informed decisions in real-time based on the vast amounts of data available.

Cloud computing could also revolutionize the way military organizations operate. By leveraging cloud services, militaries can enhance their operational capabilities and gain global access to critical information and applications. With cloud computing, military forces can streamline operations, reduce costs and stay at the forefront of new technologies and mobility. As a result, militaries can adapt quickly to changing circumstances and use resources more efficiently, ultimately leading to better mission outcomes. Cloud computing also enables military organizations to improve their collaboration and information-sharing capabilities. By storing data and applications in the cloud, different units and branches can easily access and exchange information in real-time, leading to faster decision-making and better coordination. Cloud services also provide enhanced cybersecurity measures to protect sensitive military data from unauthorized access or cyber threats.

The military's use of cloud computing also enables efficient resource allocation. Military organizations can scale up or down computing resources and optimize their operations and resource utilization. Such flexibility also allows for easier integration of new technologies and systems, enabling rapid innovation and modernization. Cloud computing also facilitates data analysis and intelligence, providing military personnel with actionable insights and predictive capabilities.

Moreover, it enables proactive decision-making and strategic planning, ultimately enhancing the overall effectiveness of the mission. Additionally, the cloud offers improved disaster recovery capabilities, ensuring that critical data and applications are backed up and accessible even during unexpected disruptions or attacks. Cloud computing revolutionizes military operations by providing a secure, collaborative, cost-effective, and technologically advanced platform for information management and decision support.

3 INFOCOMMUNICATION SOLUTIONS

5G networks are a key communications solution to support the above capabilities, providing faster and more reliable connectivity for military personnel and information gathering and sharing assets in the field. This allows them to share critical information and

coordinate their operations more effectively, ultimately leading to better results on the battlefield. In addition, deploying 5G networks can also facilitate using emerging technologies, such as artificial intelligence and autonomous systems, to improve real-time situational awareness and decision-making capabilities.

A 5G standalone private network is a wireless communications network specifically designed for an organization or group, with full configuration, security, and management. Autonomous private networks use 5G technology to provide high-speed, low-latency connectivity for mission-critical communications applications and IoT devices. They can also provide wireless connectivity in remote industrial facilities, mining operations, and military bases where public networks are unavailable or unreliable.

Deploying 5G autonomous private networks to equipment supporting command and control in military operations requires careful planning and consideration. This includes conducting a feasibility study, defining the network architecture, selecting the appropriate spectrum, deploying and configuring the network infrastructure, and conducting a network architecture study. In addition, it is essential to ensure the security and resilience of the network as it will handle sensitive and classified information.

Regular network maintenance and monitoring will also be necessary to address any problems or vulnerabilities that may arise. Regular monitoring and evaluation of network performance can identify potential problems and ensure the network meets its objectives. Security measures, such as data encryption and access control, can be used to protect the network from potential threats. Regular testing and monitoring are needed to guarantee optimal performance and to detect potential problems. Once devices are installed, the network must be tested, optimized, maintained, and updated.

Network maintenance should be planned to meet the changing needs of, for example, military operations, ensuring that the network can handle the increasing amount of data generated by the deployed devices and remain secure against potential threats. For assets supporting military command and control, deploying a 5G autonomous private network has both potential advantages and disadvantages. Benefits include increased security, reliability, resilience, high-speed connectivity, reduced latency, and dependability. Organizations can tailor the network to their needs, including creating dedicated coverage areas, managing device connections, and optimizing bandwidth for different purposes. However, prospective drawbacks include the need for specialized equipment and infrastructure. In deciding whether to deploy a standalone 5G private network for command and control support devices in a military environment, it is essential to weigh the potential benefits and potential drawbacks, such as limited coverage, interference, implementation complexity, high deployment costs, inadequate network coverage, and regulatory concerns. 5G networks use higher frequencies, making them more susceptible to interference from other electrical equipment in many regions that have not yet been deployed (Tóth, 2022).

These developments will enable allied forces to stay at the forefront of the constantly evolving theatre of war and maintain their competitive edge. Military private 5G networks can also improve communication and coordination between different units and forces, enabling seamless integration and interoperability. Furthermore, the high bandwidth and low latency of 5G networks can support the transmission of large amounts of data, enabling faster and more accurate intelligence and analysis. This can greatly enhance the effectiveness of military operations and provide commanders with timely and actionable information.

Additionally, private 5G networks offer enhanced security measures, ensuring that sensitive military communications and data remain protected against potential cyber threats. The advanced encryption protocols and robust authentication mechanisms of 5G networks provide a secure and reliable communications infrastructure for military operations. Furthermore, private 5G networks enable faster and more efficient data transfer, allowing military personnel to share critical information and make informed decisions in real-time. This improved connectivity can ensure interoperability, significantly improving situational awareness and coordination between different units and ultimately improving the overall effectiveness of military missions.

For 5G, it is important to stress the performance and efficiency requirements of 5G mobile communication systems. Key performance indicators include user experience ratio, link density, latency, spectrum efficiency, and system energy efficiency. For military applications, priority, latency, reliability, user rate, mobility, connection density, security classification, and energy efficiency are defined as eight categories, as shown in Table 1.

Table 1 Key performance indicator system for 5G military applications

Key Performance Indicator	Feature	Value
Priority	The priority of the 5G network scheduling resources can be determined according to the priority assigned by the military mission priority, which can be dynamically adjusted in real-time according to the mission flow or the battlefield environment.	High: Real-time military tasks in the battlefield Middle: Cooperative training exercises Low: Logistical asset support tasks
Latency	It refers specifically to end-to-end delay, i.e., the time it takes for a terminal to send data to another endpoint to receive data while executing military tasks. The remote control service of an unmanned combat platform has higher requirements.	The 5G end-to-end delay should be less than 1 ms.
Reliability	It can provide reliable services for specific military missions under defined conditions and functions. It determines the reliability of	Weapon systems: 99.999% Command and control systems: 99.9%

	the network in the execution of military missions.	Service support systems: 99%
User rate	This is the guaranteed user speed under the actual load on the system. The user includes the fighter and the personnel support equipment and the radar and other sensors, missiles, and different weapon platforms.	The top speed of 5G can be up to 20 Gbit/s in the right conditions.
Mobility	It describes the maximum mobile speed supported under the given Quality of Service (QoS) and seamless transmission conditions. The target is high-speed moving objects such as aircraft, ships, and land combat vehicles. 5G focuses on overcoming Doppler shift and frequency switching.	High: >200 km/h Medium: 20-200 km/h Low: <20 km/h
Connection density	It represents the total number of online terminals supported per unit area. Online means that the terminal communicates with a given QoS level, especially in combat or military material support scenarios where several sensors are distributed and interconnected.	High: >1000 km2 Medium: 100-1000 km2 Low: <100 km2
Security classification	It refers to the level of security of the military services. They are logically separated according to their security level.	High: Secret Medium: Restricted Low: Unclassified
Energy efficiency	It represents the amount of data that can be sent and received per unit of energy used on the network and terminal equipment sides. This is primarily for the needs of the IoT, such as weapon sensors, surveillance systems and unmanned vehicles.	High: Weapon control systems Medium: Surveillance assets Low: Remote control

Source: Liao, Ou, 2020

CONCLUSION

The Russian-Ukrainian conflict has highlighted that today's military operations are based on a completely different basis than those of the past decades. The focus is on multi-domain operations, and the entire command and control structure must be adapted accordingly. A fundamental step in this process is the transformation of the headquarters system, which will support commanders in meeting the challenges they face with these new capabilities. This will require the creation of command posts that are sufficiently mobile and flexible to adapt to a rapidly changing operational environment.

Accordingly, they must be equipped with capabilities that can provide relevant information at any time, even during rapid redeployments and relocations. An excellent solution is to use cloud computing to integrate all data collection tools to provide commanders with the necessary information. The computing power of the cloud can contribute to a fast and accurate analysis of large amounts of incoming data so that the information available is always the most reliable. A communications solution for this

environment could be a private 5G network providing a robust, high-speed, reliable, and secure communications environment for cloud-based command and control systems.

This private 5G network would provide seamless connectivity between data collection devices and the cloud, enabling real-time information transfer. In addition, introducing advanced encryption protocols and authentication mechanisms would guarantee the security of sensitive data. Leveraging the power of 5G technology, commanders would have access to a highly responsive and low-latency network, facilitating rapid decision-making processes. This would significantly increase the effectiveness of military operations, as commanders could receive and analyze real-time data from multiple sources simultaneously. Thanks to the low latency provided by 5G, they could quickly assess the situation on the ground and make timely and informed decisions. Furthermore, this private 5G network would also support the deployment of autonomous vehicles and drones, allowing commanders to conduct intelligence and surveillance more efficiently. Seamless connectivity between the data collection devices and the cloud would ensure secure, uninterrupted, and undelayed transmission of information.

They all contribute to commanders having access to all information in the right place, at the right time, and in the right format, which means that they do not necessarily have to lead their troops from a fixed command post but can do so from their command vehicle, for example, ensuring a high degree of mobility and flexibility. This flexibility is key in modern warfare, where the battlefield constantly changes, and commanders must adapt quickly. Access to real-time information enables them to make informed decisions on the ground, adjusting their strategy and tactics as necessary. In addition, the ability to drive from command vehicles allows commanders to be closer to the action, giving them a better understanding of the situation on the ground. This proximity also allows faster communication and coordination with their teams, increasing operational effectiveness. In addition, having all information available in the right format ensures that commanders can easily analyze and interpret data, identifying patterns and trends that are key to success. By leveraging technology and advanced communications systems, commanders can effectively lead their teams in a dynamic environment while maintaining high situational awareness. This integration of information and mobility enables commanders to react quickly and decisively, ultimately increasing their effectiveness on the battlefield.

ACKNOWLEDGMENT

Project no. TKP2021-NVA-16 has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development, and Innovation Fund, financed under the TKP2021-NVA funding scheme, financed under the TKP2021-NVA funding scheme.

This research is supported by the National Media and Infocommunications Authority of Hungary.

REFERENCES

BEAGLE, M. – SLIDER, J. C. – ARROL, M. R. The Graveyard of Command Posts. *Military Review*. May-June 2023, p. 10-24.

FOX, A. C. On the Principles of War: Reorganizing Thought and Practice for Large-Scale Combat Operations. *Land Warfare Paper* 138 / June 2021, p. 1-18.

LIAO J. – OU, X. 5G Military Application Scenarios and Private Network Architectures. *2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications(AEECA)*. 2020, p. 726-732. DOI: https://doi.org/10.1109/AEECA49918.2020.9213507

NATO's Allied Joint Doctrine (AJP-01), Source: https://www.gov.uk/government/publications/ajp-01-d-allied-joint-doctrine

PERKINS, D. G. Multi-Domain Battle the Advent of Twenty-First Century War. *Military Review*. November-December 2017, p. 8-13.

RUSSELL, S. – ABDELZAHER, T. – SURI, N. Multi-Domain Effects and the Internet of Battlefield Things. *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*. Norfolk, VA, USA, 2019, p. 724-730.

TÓTH, A. The Use of 5G in Military Cloud of Things Solutions. *AARMS* Vol. 21, No. 3, 2022, p. 5–20.

Andras TOTH, PhD
1101 Budapest, Hungaria krt. 9-11. Hungary
toth.hir.andras@uni-nke.hu

Tibor FARKAS, PhD
1101 Budapest, Hungaria krt. 9-11. Hungary
farkas.tibor@uni-nke.hu