INFO FLASH
Finabel
The European Land Force
Commanders Organisation

FINABEL - THE EUROPEAN LAND FORCE COMMANDERS ORGANISATION

OCTOBER 2024

INFOFLASH

COMMAND AND CONTROL INSIGHTS FROM UKRAINE

WRITTEN BY

VICTORIANO VICENTE BOTELLA BERENGUER

EDITED BY

DIMITRA PATERAKI

SUPERVISED BY

BELÉN PADRÓN SALINAS

Introduction

In an era where the nature of warfare is increasingly characterised by the implementation of technological advancements and shifting geopolitical dynamics, the importance of effective Command and Control (hereby C2) systems on the battlefield has never been more critical. Russia's full-scale invasion of Ukraine in 2022 set off the current conflict, which has illustrated how C2 structures may influence the results of contemporary combat. Understanding the lessons from this armed conflict is important for developing armed forces prepared for the future as European countries confront the possibility of hybrid threats and multi-domain operations.

This paper draws thorough conclusions on the role of C2 dynamics in Ukraine and its implications for European land forces. It provides an analysis of the role of C2 in military operations and further investigates the dynamics of C2 systems from both Russian and Ukrainian forces on the ground. This article offers valuable insights for enhancing C2 systems in European multi-domain allied military operations.

I. The Importance of Command and Control in the Battlefield

C2 is generally viewed as a specialised function with its techniques, concerns, and terminology, operating independently from other activities. However, C2 integrates all military activities and actions to create a meaningful whole (US Marine Corps, 2018). No single part of war is more important than C2. While C2 alone cannot launch an attack, destroy a target, or organise a resupply mission, none of these detrimental warfighting responsibilities could happen without it (US Marine Corps, 2018). In essence, it constitutes the basis for all military actions (US Marine Corps, 2018).

Military C2 systems help military organisations plan, execute, assess, and coordinate actions by integrating the key functions of Command and Control (Popa, 2020). According to NATO, C2 is the exercise of authority and direction by a designated commander over assigned troops to achieve the force's mission (Curts & Campbell, 2006). This process involves a commander using troops, equipment, communications, facilities, and procedures to plan, direct, coordinate, and control forces to complete their tasks (Curts & Campbell, 2006).

C2 systems allow coordinated actions across complex and dynamic conflict settings (Athans, 1987). They enable commanders to direct and control forces, reflecting the hierarchical military nature of a commander over his subordinates (Curts & Campbell, 2006; US Marine Corps, 2018).

Control involves ongoing input from the situation to the commander, allowing them to alter and modify their actions based on real-time information (US Marine Corps, 2018).

Military C2 systems help military organisations plan, execute, assess, and coordinate actions by integrating the key functions of Command and Control (Popa, 2020). According to NATO, C2 is the exercise of authority and direction by a designated commander over assigned troops to achieve the force's mission (Curts & Campbell, 2006). This process involves a commander using troops, equipment, communications, facilities, and procedures to plan, direct, coordinate, and control forces to complete their tasks (Curts & Campbell, 2006).

C2 systems allow coordinated actions across complex and dynamic conflict settings (Athans, 1987). They enable commanders to direct and control forces, reflecting the hierarchical military nature of a commander over his subordinates (Curts & Campbell, 2006; US Marine Corps, 2018). Control involves ongoing input from the situation to the commander, allowing them to alter and modify their actions based on real-time information (US Marine Corps, 2018). This feedback highlights the gap between desired outcomes and current conditions; it enables commanders to react to changing conditions, seize opportunities, address emerging issues, change plans, and refocus resources (US Marine Corps, 2018).

Michael Athans (1987) argues that C2 systems necessitate novel approaches to distributed decision-making, especially in uncertain situations. These systems are intended to handle various forces, equipment, and communication structures, allowing military leaders to carry out operations efficiently. Therefore, C2 spans a wide variety of activities, all aided by advanced technology and organisational frameworks (Athans, 1987). The development of resilient distributed C2 systems presents significant opportunities for advancing control theory in both military and civilian contexts (Athans, 1987).

II. C2 Structures of Ukrainian and Russian Forces

Since Russia's full-scale invasion of Ukraine, C2 dynamics have played a critical role in influencing war results for both sides. The invasion, intended to rapidly depose the Ukrainian government, has evolved into a lengthy struggle, with Russia focusing on Eastern and Southern Ukraine after failing to conquer Kyiv early on. In this environment, the Ukrainian and Russian commanders have taken diverse approaches to C2, reflecting their various military philosophies, technological capabilities, and strategic objectives.

On the one hand, the Ukrainian Armed Forces (UAF) revised their C2 framework to emphasise decentralisation and flexibility.

Since the annexation of Crimea in 2014, Ukraine has undertaken considerable military changes, many of which have tried to conform to NATO norms and standards (Dieanu, 2022). Such changes include modernising command structures and giving lower-level commanders additional authority on the battlefield (Dieanu, 2022). The UAF's decentralised C2 structure has shown to be particularly successful in responding quickly to battlefield events since it allows decision-making to occur at numerous levels (Sanders, 2023).

In contrast, Russia's C2 model has mostly followed a traditional, hierarchical structure, which constitutes a risk factor (Merkx, 2023). The strict, top-down style of Russian C2 has hampered adaptation and caused communication breakdowns, particularly during the initial phases of the invasion. Russian troops have battled with logistics and inadequate coordination, resulting in operational failures and a lack of combat cohesiveness (Merkx, 2023). This rigidity has been exacerbated by corruption and low morale among Russian personnel, thus diminishing their efficacy.

The conflict's C2 dynamics have been significantly influenced by technological and cyber elements. Ukraine's satellite communication technologies have enabled dependable and secure communications even when traditional infrastructure has been disrupted (Kroenig & Starling, 2023). Cyber warfare has been a constant part, with both sides launching assaults aimed at damaging the other's communications and infrastructure. Both parts have used cyber operations for disruption, influence, and espionage, with Ukraine having received significant Western technology assistance, improving its intelligence, surveillance, and reconnaissance (ISR) capabilities (Grossman et al., 2023; Kroenig & Starling, 2023).

Overall, the discrepancy between Ukrainian and Russian approaches to C2 systems implies larger contrasts in military doctrine and adaptation. While the UAF's decentralised and electronically integrated C2 has increased battlefield flexibility, Russia's more hierarchical model has experienced several obstacles, restricting its capacity to react to the unfolding war. The use of technological advancement in the cyber and satellite sectors has emphasised the strategic relevance of effective C2 in modern-day combat.

III. Lessons from the Ukrainian Battlefield

The fighting on Ukrainian soil continues to teach Western armies vital lessons, notably about interoperability and C2 capabilities. As European armies increasingly engage in international coalitions and confront constantly developing threats, improving C2 structures becomes critical. The Russian 'Special Operation' in Ukraine, which combines conventional and hybrid warfare, has highlighted the importance of agility, information integration, and robust communication networks in C2. Therefore, this section will try to portray key takeaways for European allies.

Lesson 1: Decentralisation vs. Centralisation of Command

The Ukrainian war has highlighted the critical balance between decentralised and centralised command arrangements in modern warfare, particularly in multi-front wars when adaptation and speed are detrimental. Decentralised command systems, as mentioned, have allowed Ukrainian troops the ability to quickly react to rapidly changing combat situations, enabled via 'The Delta system' – a cloud-based Delta situational awareness system (Rosengren, 2023). This system was created to offer situational awareness in real-time, organise defence troops, and gather, analyse, and display data on hostile troop movements (Rosengren, 2023). Additionally, the system gathers data from sensors and open and secret sources to present a complete picture of the current fighting space, which is summarised and shown on an intuitive digital map (Rosengren, 2023). The adaptability offered thanks to 'The Delta system' has been extremely helpful to Ukraine's resistance, allowing units to change operational plans in real-time and move from defensive operations in Kyiv to counteroffensives in the South and East (Rosengren, 2023; Zabrodskyi et al., 2022). The liberty afforded to local commanders has enabled the UAF's troops to exploit Russian weaknesses, particularly when Russian soldiers experienced logistical failures and mismanagement (Hackett & Nagl, 2024)

In contrast, Russia's highly centralised command system has been stiff and reluctant to adjust. The hierarchical architecture of Russian C2 systems has hampered their capacity to adapt to dynamic battlefield events, notably during Ukrainian counteroffensives, resulting in severe losses and lost territory (Jones, 2022). Failure to react quickly worsened operational inefficiencies and contributed to Russia's deteriorating strategy, as its troops became entangled and unable to effectively oppose the UAF's tactics (Hackett & Nagl, 2024).

.

For European commanders, the lessons from Ukraine highlight the significance of flexibility within C2 systems. In fast-paced, complex contexts, the capacity to delegate decision-making to lower levels while maintaining strategy coherence is critical. To retain operational flexibility, modern military operations require a combination of centralised control and distributed execution. As a result, European forces must emphasise the development of adaptable C2 systems capable of quickly adapting to changing situations, ensuring that strategic aims stay aligned even while tactical choices are taken independently at lower command levels.

Lesson 2: Importance of Intelligence and Communication Networks

The Ukrainian battlefield has showcased the need for intelligence and real-time communication in C2 efficiency. The UAF has greatly benefited from modern intelligence-sharing networks, notably those provided by Western partners, who have continuously provided satellite imaging, real-time drone feeds, and signals intelligence (SIGINT) (Grossman et al., 2023; Rosengren, 2023).

The combination of these capabilities has enabled Ukraine to identify and counter Russian operations with pinpoint accuracy, frequently utilising drones and satellite-based surveillance to target Russian locations and supply routes (Davis Jr., 2023).

Furthermore, the fight has demonstrated the importance of secure and robust communication networks for ensuring C2 continuity during wartime. The UAF depended on encrypted communication networks, which ensured continuous satellite connection even in places where traditional infrastructure had been destroyed (Rosengren, 2023; Davis Jr., 2023). For European ground forces, this emphasises the significance of investing in interoperable, secure communication systems capable of withstanding both cyberattacks and physical disturbances. Providing real-time data flow between multinational units is crucial for maintaining coherent operations, particularly in joint or coalition settings (NATO, 2023).

Lesson 3: Integration of Conventional and Unconventional Tactics

Contemporary warfare is not limited to conventional tactics but rather necessitates a hybrid strategy that combines traditional military operations with unconventional tactics. The UAF have skilfully used a variety of unconventional tactics, including the deployment of local militias and resistance squads to thwart Russian advances (Dieanu, 2022). For instance, Ukrainian partisan forces have played an important role in guerrilla-style ambushes and attacks on Russian supply lines, posing considerable logistical issues for Russian soldiers (Dieanu, 2022).

Furthermore, the use of cyber capabilities during the conflict, both defensive and offensive, has shaped the battlefield dynamics. Despite early predictions of a massive Russian cyber "shock and awe" campaign, the effectiveness of Russian cyber operations has been mitigated by Ukrainian cyber defences, which are reinforced by international cooperation with cybersecurity specialists and private sector businesses (Lonergan et al., 2023). Cyber defence collaborations play a vital role in thwarting notable instances like the attempted assault on Ukraine's power system by Russia's GRU-linked Sandworm group (Lonergan et al., 2023).

Ukraine's Computer Emergency Response Team, with the help of the Slovakia-headquartered cyber firm ESET, were able to stop the attack before it happened (Lonergan et al., 2023); they were able to identify the attack early on, disable any dangerous code, and neutralise the threat (Proska et al., 2023). This prompt action demonstrated both international collaboration and Ukraine's developing cyber defence capabilities.

The war in Ukraine has demonstrated the growing significance of cyberwarfare in contemporary conflicts by using cyber offensives to interfere with the enemy's communication and logistical networks. These incidents show how crucial it is for European allies to continue to integrate cyber operations into their larger military plans and prioritise cyber resilience. Evidently, cyber capabilities have been proven and will continue to be vital.Ukraine's Computer Emergency Response Team, with the help of the Slovakia-headquartered cyber firm ESET, were able to stop the attack before it happened (Lonergan et al., 2023); they were able to identify the attack early on, disable any dangerous code, and neutralise the threat (Proska et al., 2023). This prompt action demonstrated both international collaboration and Ukraine's developing cyber defence capabilities. The war in Ukraine has demonstrated the growing significance of cyberwarfare in contemporary conflicts by using cyber offensives to interfere with the enemy's communication and logistical networks. These incidents show how crucial it is for European allies to continue to integrate cyber operations into their larger military plans and prioritise cyber resilience. Evidently, cyber capabilities have been proven and will continue to be vital.

Concluding Remarks: Strategic Recommendations

The present study has analysed the role of C2 systems in the Ukrainian battlefield and considered valuable insights for European commanders. By comparing and contrasting Russia's and Ukraine's C2 systems and dynamics, the article has found that Russia's more inflexible, hierarchical approach was strategically surpassed by the UAF's decentralised, adaptable C2 structures. Upholding operational performance in complex and dynamic circumstances requires modernising C2 systems with real-time intelligence, secure communications, and flexible command structures. However, one must acknowledge that the conclusions obtained in this article might not apply to other contexts and, therefore, cannot be over-generalised.

Still, European armies should prioritise the creation of distributed C2 structures, uphold investments in cyber resilience, and ensure that intelligence is shared seamlessly across national borders to improve strategic preparedness. The decentralised strategy of Ukraine and other adaptable C2 models might enlighten European forces to sustain their operational dominance in dynamic threat contexts such as the one at hand in this article.

Bibliography

Athans, M. (1987). Command and control (C2) theory: A challenge to control science. IEEE Transactions on Automatic Control, 32(4), 286–293. https://doi.org/10.1109/tac.1987.1104607

Bachmann, S. D., & Gunneriusson, H. (2015, October 7). Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere. Ssrn.com. https://ssrn.com/abstract=2670527

Borsari, F. (2024, October). Ukrainian Lessons for the Age of Automated Warfare. CEPA. https://cepa.org/article/ukrainian-lessons-for-the-age-of-automated-warfare/

Crombe, K., & Nagl, J. A. (2023). A Call to Action: Lessons from Ukraine for the Future Force. The US Army War College Quarterly: Parameters, 53(3). https://doi.org/10.55540/0031-1723.3233

Curts, R., & Campbell, D. (2006). Rethinking Command & Control. Curts & Campbell. https://apps.dtic.mil/sti/tr/pdf/ADA461640.pdf

Davis Jr., G. B. (2023, March 16). The future of NATO C4ISR: Assessment and recommendations after Madrid. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-future-of-nato-c4isr-assessment-and-recommendations-after-madrid/

Dieanu, A.-C. (2022). The Role of Ukrainian Special Operations Forces within the War in Ukraine. International Scientific Conference "STRATEGIES XXI," 18(1), 220–228. https://doi.org/10.53477/2971-8813-22-26

Grossman, T., Kaminska, M., Shires, J., & Smeets, M. (2023). The Cyber Dimensions of the Russia-Ukraine War. In ECCRI. European Cyber Conflict Research Initiative. https://eccri.eu/wp-content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf

Hackett, M. T., & Nagl, J. A. (2024, August 29). A Long, Hard Year: Russia-Ukraine War Lessons Learned 2023. US Army War College - Publications. https://publications.armywarcollege.edu/News/Display/Article/3890256/

Itugbu, Dr. S. (2023). Russia's Strategic Failure in Ukraine. International Journal of Research and Innovation in Social Science, VII(VII), 881–895. https://doi.org/10.47772/ijriss.2023.70768

Jones, S. G. (2022, June 1). Russia's Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare. Www.csis.org. https://www.csis.org/analysis/russias-ill-fated-invasion-ukraine-lessons-modern-warfare

Kroenig, M., & Starling, C. G. (2023). U.S. Lessons from Russia's War on Ukraine. Asia Policy, 30(2), 64–74. https://doi.org/10.1353/asp.2023.0018

Lonergan, E. D., Smith, M. W., & Mueller, G. B. (2023). Evaluating Assumptions About the Role of Cyberspace in Warfighting: Evidence from Ukraine*. 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), 85–102. https://doi.org/10.23919/cycon58705.2023.10182101

Merkx, G. W. (2023). Russia's War in Ukraine: Two Decisive Factors. Journal of Advanced Military Studies, 14(2), 13–33. https://muse.jhu.edu/article/909028

NATO. (2023, December). Russian War against Ukraine Lessons Learned Curriculum Guide - English version. NATO. https://www.nato.int/cps/en/natohq/topics_221175.htm

Olmo, F. J. (1999). Defense Technical Information Center. In DTIC (pp. 1–25). Faculty of the Naval War College - Department of the US Navy. https://apps.dtic.mil/sti/citations/ADA363260

Popa, C. (2020). Command and Control Systems – Modern Structures, Equipment and Technologies. Defense Resources Management in the 21st Century, 15/2020, 226–232. https://www.ceeol.com/content-files/document-965494.pdf

Proska, K., Wolfram, J., Wilson, J., Black, D., & Lunden, K. (2023, November 9). Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. Google Cloud Blog. https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/

Rice, A. J. (1997). Command and Control: The Essence of Coalition Warfare. The US Army War College Quarterly: Parameters, 27(1). https://doi.org/10.55540/0031-1723.1817

Rosengren, O. (2023, February 3). Network-centric Warfare in Ukraine: The Delta System. Grey Dynamics. https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system/

Sardiello, L. C., Carlos A. (2004). Effect of Modern C2 Assets on Risk Management of Joint Operational Warfare. In DTIC (pp. 1–18). Faculty of the Naval War College - Department of the Navy of the United States of America.
https://apps.dtic.mil/sti/citations/ADA422731

US Marine Corps. (2018). Command and Control .
https://www.marines.mil/Portals/1/Publications/MCDP%206.pdf

Zabrodskyi, M., Watling, D. J., Danylyuk, O. V., & Reynolds, N. (2022, November 30). Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022. RUSI.
https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022

.