Cybersecurity and Law

2026 Nr 1(15)

DOI: 10.35467/cal/219843

Protection and Cybersecurity of Command Posts in Contemporary Armed Conflicts

Ochrona i cyberbezpieczeństwo stanowisk dowodzenia we współczesnych konfliktach zbrojnych

Krzysztof WYSOCKI
Akademia Sztuki Wojennej
ORCID: 0000-0002-0527-6976
E-mail: k.wysocki@akademia.mil.pl

Marcin ZAWODNIAK
Akademia Sztuki Wojennej
ORCID: 0000-0002-5737-4850
E-mail: mzawodniak@mon.gov.pl

Abstract

Contemporary armed conflicts have confirmed that Command Posts (CPs) have become one of the most vulnerable elements of the C2 system, particularly under conditions of integrated kinetic, cyber, and electromagnetic effects. The experiences of Ukraine from 2022–2025 demonstrate that traditional, static, and high-emission Command Posts are incapable of survivability in an environment saturated with ISR sensors and automated targeting systems. The aim of this article is to analyze the determinants of CP protection and cybersecurity in multi-domain operations and to identify key factors for their survivability. Results indicate that effective protection requires a systems approach combining mobility, dispersion, electromagnetic signature reduction, active cyber defense, and the integration of MILDEC and OPSEC. The importance of nodal ADC2 architecture, the utilization of fixed infrastructure and cloud environments, as well as the reorganization of staff processes, has also been confirmed.

Keywords

Command Posts, cybersecurity, Multi-Domain Operations, camouflage, force protection

Streszczenie

Współczesne konflikty zbrojne potwierdziły, że Stanowiska Dowodzenia (SD) stały się jednym z najbardziej wrażliwych elementów systemu C2, szczególnie w warunkach zintegrowanych efektów kinetycznych, cybernetycznych i elektromagnetycznych. Doświadczenia Ukrainy z lat 2022–2025 pokazują, że tradycyjne, statyczne i wysokoemisyjne Stanowiska Dowodzenia nie

są w stanie przetrwać w środowisku nasyconym czujnikami ISR i zautomatyzowanymi systemami celowniczymi. Celem niniejszego artykułu jest analiza czynników determinujących ochronę SD i cyberbezpieczeństwo w operacjach wielodomenowych oraz identyfikacja kluczowych czynników wpływających na ich przetrwanie. Wyniki wskazują, że skuteczna ochrona wymaga podejścia systemowego łączącego mobilność, dyspersję, redukcję sygnatur elektromagnetycznych, aktywną cyberobronę oraz integrację MILDEC i OPSEC. Potwierdzono również znaczenie węzłowej architektury ADC2, wykorzystania infrastruktury stacjonarnej i środowisk chmurowych, a także reorganizacji procesów sztabowych. Wnioski dowodzą, że jedynie zintegrowany, wielowarstwowy model ochrony umożliwia utrzymanie ciągłości dowodzenia i ogranicza podatność PK na skoordynowane działania przeciwnika.

Słowa kluczowe
stanowiska dowodzenia, cyberbezpieczeństwo, operacje wielodomenowe, kamuflaż, ochrona wojsk

Introduction

Contemporary armed conflicts have confirmed that Command Posts (CPs) have become one of the most vulnerable elements of the Command and Control system. The traditional paradigm of their protection based on camouflage, dispersion, and engineering measures proves insufficient against integrated fires, multispectral reconnaissance, and effects in the cyber domain. Examples from Ukraine, particularly from the Chornobaivka region, have demonstrated the scale of the threat to static command structures: Russian command posts were repeatedly destroyed by precision strikes, leading to the disorganization of the command system and loss of battle management capabilities[1]. The loss of army or division-level headquarters as a result of a single missile strike has become synonymous with a lack of survivability and non-adaptability of command structures to multi-domain threats.

Concurrently, wartime experiences confirm the growing importance of cyberspace and the electromagnetic spectrum as warfighting domains. In the new doctrinal approach (NATO, USA), Command Posts are viewed as multi-domain nodes (All-Domain Command and Control – ADC2), which must combine operational, cyber, and information functions[2]. This entails the necessity to ensure continuity of communication systems operations, resilience to jamming and cyberattacks, and the capability to function in urbanized environments[3]. The urban environment becomes simultaneously an operational and a concealing space enabling the hiding of electromagnetic signatures, but also increasing exposure to detection by civilian sensors and ISR (Intelligence, Surveillance, Reconnaissance) systems.

Research conducted at U.S. Army and NATO training centers indicates that maintaining command capabilities requires combining mobility with dispersion and the integration of physical-cyber protection. Modern Command Posts should be characterized by the capability for dynamic displacement, signature emission

[1] M. Beagle, J. C. Slider, M. R. Arrol, The Graveyard of Command Posts: What Chornobaivka Should Teach Us about Command and Control in Large-Scale Combat Operations, Military Review Online Exclusive, March 2023.
[2] AFMAN 10-207: Command Posts (AFGM 2025-01), Department of the Air Force, Headquarters United States Air Force, Washington D.C., 13 March 2025.
[3] R. L. Wolfel, A. Richmond, J. Ridgeway, Dense Urban Environments: The Crucible of Multi-Domain Operations, Military Review, January–February 2021, p. 22-30.

reduction, and survivability under conditions of intensive adversary engagement[4]. Consequently, the concept of utilizing fixed infrastructure reinforced concrete buildings, underground and tunnel facilities as “hard” Command Posts, resilient to kinetic and electronic effects, is returning[5].

Analysis of the experiences of the Armed Forces of Ukraine shows that Command Post protection must be considered as a multi-layered system, encompassing physical, information, and cyber domains. Survivability, mobility, and multispectral camouflage have become co-equal pillars of effective command[6]. From a theoretical perspective, this phenomenon fits into the broader transformation of warfare, characterized by the blurring of boundaries between the cyber, information, and kinetic battlefields[7].

An analysis by the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) for the years 2022–2024 indicates that cyberspace has become a fully-fledged theater of operations, strictly linked with kinetic and information operations. Within three years of the invasion's commencement, the Russian Federation conducted over 9,000 cyber incidents, including over 2,000 of a destructive nature, targeting Ukraine's energy, telecommunications, and state administration infrastructure. Particularly significant was the coordination of cyberattacks with missile strikes and disinformation operations, which confirmed the development of the concept of integrated information-cyber operations[8].

The aim of the article is to analyze contemporary determinants of protection and cybersecurity of Command Posts in the context of multi-domain conflicts, with particular emphasis on the experiences of the Armed Forces of Ukraine from 2022–2025. The article identifies key factors determining survivability and resilience of Command Posts to adversary engagement in the physical, electromagnetic, and cyber domains.

The main research problem addresses the question: *what factors determine the effectiveness of protection and cybersecurity of Command Posts in conditions of contemporary armed conflicts* and *how can the integration of physical, information, and cyber domains increase their survivability?*

The article adopts the hypothesis that effective protection and cybersecurity of Command Posts in conditions of contemporary armed conflicts require the implementation of an integrated protection system, combining engineering fortification, organizational solutions, and advanced cyber defense and information management tools. It is assumed that only such an approach based on synergy between CP mobility, electromagnetic signature reduction, system redundancy, active cyber defense, and MILDEC and OPSEC measures enables the maintenance of command continuity and increases the resilience of control structures to adversary engagement. This hypothesis reflects the contemporary pursuit by NATO armed forces to implement the

[4] M. N. Slusher, Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience, Defense Analysis White Paper, May 2025.
[5] C. A. Broyles, C. Richter, Concrete Command: Why Combat Training Centers Should Prioritize Training on Urban Command Posts, Military Review, July-August 2023, p. 12-18.
[6] MIL-HDBK-1013/1A: Design Guidelines for Physical Security of Facilities, Department of Defense, Washington D.C., 15 December 1993.
[7] Lessons Learned from the Ukrainian Territorial Defense Forces: Command Post Survivability, Center for Army Lessons Learned (CALL), (No. 24-862), Fort Leavenworth 2024.
[8] War and Cyber: Three Years of Struggle and Lessons for Global Security, Analytical Report State Service of Special Communications and Information Protection of Ukraine (SSSCIP), Kyiv 2025, p. 3-16.

All-Domain Command and Control (ADC2)[9] concept as a basis for building information and operational superiority.

Literature Review

Literature regarding the protection and cybersecurity of Command Posts in conditions of contemporary armed conflicts is dispersed across several research streams: classical approaches to command and CP organization, analyses of CP survivability in an ISR-saturated environment, studies on Multi-Domain Operations (MDO) and All-Domain Command and Control (ADC2), as well as works concerning camouflage, MILDEC, OPSEC, and cyber defense. In recent years, publications referring to the experiences of the Russo-Ukrainian war, pointing to the systemic nature of engagement against adversary Command Posts, have gained particular importance.

The starting point for understanding the role of Command Posts in contemporary military operations are doctrinal and analytical publications devoted to their organization and functioning. In *Army Techniques Publication 6-0.5*[10], cited and commented on by, among others, A. S. Cecil and K. Butler in the publication *Command Post Operations*, a Command Post is defined as a location where the commander and staff perform their duties, and the essential function of the Command Post is supporting the commander in executing the mission command philosophy by ensuring the continuity of the planning, coordination, and synchronization process of combat operations[11]. The authors note that problems with effective cooperation between different types of Command Posts (Main, Tactical, Mobile) lead to command gaps, loss of situational awareness, and vulnerability to adversary engagement.

In the U.S. Air Force approach, the *AFMAN 10-207* doctrine, updated in 2025, indicates that command is increasingly perceived as a multi-domain process, and Command Posts as nodes of the All-Domain Command and Control (ADC2) system, requiring not only appropriate infrastructure preparation but also high personnel training standards and qualifications for Mission Ready/Combat Mission Ready status[12]. This document emphasizes the importance of process standardization, information management, and qualifications in the Command and Control Operations specialty, which directly translates into the command system's resilience to jamming and counteraction against cyber threats.

In analytical literature, a significant supplement to the doctrinal approach are works devoted to the organization of Command Posts in practice. Cecil and Butler, based on observations from Warfighter-type exercises, identify chronic problems with personnel staffing, unclear roles of liaison officers and specialized personnel, and undefined division of tasks between different Command Posts in brigade and divisional structures. They point out that ineffective internal organization directly translates into an elongation of the decision cycle, which, under conditions of adversary counteraction in the electromagnetic and cyber domains, may lead to a loss of command capability[13].

---

[9] NATO Allied Command Transformation, Joint All Domain Command and Control and Multi-Domain Operations, NATO ACT. Available online: https://www.act.nato.int/article/joint-all-domain-c2-and-mdo/ (Accessed: November 16, 2025).

[10] See: ATP 6-0.5: Command Post Organization and Operations, published by the Headquarters, Department of the Army, in March 2017.

[11] Cf.: A. S. Cecil, K. Butler, Command Post Operations, Military Review Online Exclusive, April 2018.

[12] See: AFMAN 10-207, op.cit.

[13] See: A. S. Cecil, K. Butler, op.cit.

A second important stream of literature consists of analyses devoted to CP survivability on the contemporary, "transparent" battlefield. An emblematic example is the article by M. Beagle, J. C. Slider, and M. R. Arrol, dedicated to the "graveyard of command posts" in the Chornobaivka region, where Russian command posts were repeatedly destroyed by coordinated strikes of Ukrainian fire assets utilizing data from an extensive ISR system. The authors show that the traditional model of large, tent-based Command Posts, generating significant electromagnetic and thermal signatures, is incompatible with the realities of contemporary large-scale operations. The conclusion is the need to transition to a model of distributed, mobile, and lower-signature C2 (Command and Control) nodes, capable of functioning under conditions of persistent reconnaissance[14].

Similar conclusions are formulated in the *Center for Army Lessons Learned* (CALL) report devoted to the survivability of Command Posts of the Ukrainian Territorial Defense Forces (TDF). It draws attention to the necessity of combining organizational measures (frequent displacement of CPs, decentralization of command functions) with technical ones (emission control, use of fixed infrastructure, limiting CP size) and with actions in the information and cyber domains[15].

A significant source regarding the broader context of contemporary operations is the work of M. N. Slusher titled *Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience*, which treats the war in Ukraine as a turning point in the development of forms of warfare, pointing to the key role of autonomous systems, information operations, electronic warfare, and logistics system resilience[16].

A significant supplement to the body of work regarding CP survivability are publicist-analytical analyses concentrating on the practical experiences of the US Army and allied nations. In the article *Command Post Threats Beyond the Electromagnetic Spectrum*, it was noted that contemporary Command Posts are exposed not only to classical threats in the electromagnetic spectrum (Electronic Intelligence – ELINT, Signals Intelligence SIGINT, emission geolocation) but also to a whole set of "non-electromagnetic" signals indicating their location: increased logistical traffic, characteristic profile of smartphone activity in social media, personnel movement patterns, or traces in the terrain where CP elements have been deployed[17].

The article *Army Scrambles to Make Command Posts Survivable* (was one of the first warnings that the expanded, tent-based Command Post of the U.S. Army had become a "magnet" for adversary fire. The text describes early attempts to increase survivability through size reduction, shortening setup times, and introducing more mobile network solutions[18]. Conversely, the publication *It's Time to Fix the Command Post* constitutes a critical analysis of the organizational culture surrounding Command Posts. The author points to bloated structures, an excessive number of devices, "fetishization" of elaborate IT systems, and the disappearance of simple, analog

[14] Cf.: M. Beagle, J. C. Slider, M. R. Arrol, op.cit.
[15] See: Lessons Learned from the Ukrainian Territorial Defense Forces: Command Post Survivability, Center for Army Lessons Learned (CALL) (No. 24-862), Fort Leavenworth 2024.
[16] M. N. Slusher, Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience, Defense Analysis White Paper, May 2025.
[17] J. P. Rivera, Command Post Threats Beyond the Electromagnetic Spectrum, NCO Journal, October 2024.
[18] Cf.: S. Magnuson, Army Scrambles to Make Command Posts Survivable, National Defense Magazine, https://www.nationaldefensemagazine.org/articles/2017/12/1/army-scrambles-to-make-command-posts-survivable [Accessed: November 17, 2025].

command procedures. He postulates a transition to smaller, mission-oriented posts, with a clear division of functions and emphasis on mobility and emission discipline[19].

In the publication *The Commander's Place on the Battlefield*, the classical dilemma of the commander's location in combat disposition under conditions of contemporary, multi-domain operations was addressed. The author indicates that the physical presence of the commander in a large, static Command Post increases their vulnerability to a strike and may lead to paralysis of the C2 system in the event of the post's destruction. At the same time, excessive separation of the commander from the Command Post limits their ability to command complex staff processes[20].

The article by Marek Wrzosek titled *Challenges of Contemporary Command and Future Military Operations* places the above problems in the broader context of future operations pointing to information overload, shortening of decision cycles, and the growing complexity of the combat environment, which force the design of Command Posts as structures that are simultaneously information-efficient and capable of survival under conditions of intensive adversary engagement[21].

A separate block of literature concerns CP functioning in an urbanized environment. R. L. Wolfel, A. Richmond, and J. Ridgeway in the article *Dense Urban Environments: The Crucible of Multi-Domain Operations* present densely built-up urban areas as a specific "crucible" of multi-domain operations, where numerous layers overlap military, social, economic, information, and cyber[22].

This thought is developed by C. A. Broyles and C. Richter in the publication *Dense Urban Environments: The Crucible of Multi-Domain Operations* arguing that combat training centers should prioritize training the organization and protection of "concrete" Command Posts in an urbanized environment[23].

In Polish literature concerning the analyzed subject matter, a significant place is occupied by the works of Bartłomiej Terebiński, in which the author systematically analyzes issues of information security, military communications, and cyber aspects of command systems. In the monograph *Bezpieczeństwo informacji na początku trzeciej dekady XXI wieku – wybrane aspekty* [Information Security at the Beginning of the Third Decade of the 21st Century – Selected Aspects], Terebiński notes that the modernization of Command Posts and control systems in the Polish Armed Forces requires simultaneous consideration of: ICT infrastructure, the impact of digital ecosystems on the functioning of command structures, and threats resulting from the growing role of AI technology, sensors, and automation[24]. In another work, *Zagrożenia dla systemu łączności na współczesnym polu walki* [Threats to the Communications System on the Modern Battlefield], the author points to specific threats to Command Posts resulting from, inter alia, automation, integration of operational domains, and heterogeneous communications infrastructure emphasizing that their detection and

---

[19] M. Greenberg, It's Time to Fix the Command Post: Optimizing Headquarters' Mobility, Survivability, and Interoperability for the Future Fight, Modern War Institute at West Point, https://mwi.westpoint.edu/its-time-to-fix-the-command-post-optimizing-headquarters-mobility-survivability-and-interoperability-for-the-future-fight/ [Accessed: November 17, 2025].

[20] See: A. Kohli, The Commander's Place on the Battlefield, The RUSI Journal, Vol. 169, No. 4, 2024, p. 78-88.

[21] Cf.: M. Wrzosek, Challenges of contemporary command and future military operations, Scientific Journal of the Military University of Land Forces, Vol. 54, Nr 1(203), 2022, p. 35–51.

[22] R. L. Wolfel, A. Richmond, J. Ridgeway, Dense Urban Environments: The Crucible of Multi-Domain Operations, Military Review, January-February 2021, p. 24-32.

[23] C. A. Broyles, C. Richter, Concrete Command: Why Combat Training Centers Should Prioritize Training on Urban Command Posts, Military Review, July-August 2023, p. 12-19.

[24] B. Terebiński, Bezpieczeństwo informacji na początku trzeciej dekady XXI wieku – wybrane aspekty, Akademia Sztuki Wojennej, Warszawa 2023.

neutralization is possible only through a systems view that combines technical, organizational, and process aspects[25].

In Polish subject literature, the works of Krzysztof Wysocki are of significant importance for research on CP protection and camouflage. In the publication *Maskowanie jako antyfora rozpoznania* [Camouflage as Counter-Reconnaissance][26], the author presents the concept of camouflage as a complex system of effects, the goal of which is to limit the possibility of reconnaissance by the adversary through signature reduction across the entire electromagnetic spectrum, not just in the optical sphere[27]. In the second publication *Współczesne uwarunkowania maskowania stanowisk dowodzenia* [Contemporary Determinants of Command Post Camouflage] the author together with Ewelina Jastrzębska emphasize the necessity of integrating optical, engineering, electromagnetic, and organizational camouflage as the only effective way to counter the adversary's multispectral ISR means, such as IMINT (Imagery Intelligence), SAR (Synthetic Aperture Radar), SIGINT (Signals Intelligence), MASINT (Measurement And Signature Intelligence). The authors indicate that contemporary Command Posts saturated with digital devices, communication systems, and sensors generate a strong electromagnetic signature at the level of the individual soldier, subunit, and the entire formation, leading to a significant increase in vulnerability to detection and strike[28].

In English-language literature, issues of camouflage, MILDEC, and OPSEC appear in the context of CP survivability as an element of "signature management". Beagle et al.[29] and the authors of CALL[30] reports indicate that a lack of effective camouflage and emission management leads to a situation where Command Posts become "ostentatious" targets for precision fire assets. Therefore, strict integration of physical camouflage, dummy operations, disinformation, and cyber and electromagnetic protection within a single, coherent CP protection concept is postulated.

The analysis of English-language literature regarding the *Cyber Resilience of Command Post Systems* of NATO and the USA was conducted in several areas.

The first stream of analyses concentrates on the vulnerability of NATO command and communication systems to cyber threats and the necessity of their systemic modernization. The most important work in this area is the report *Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems*, in which it was demonstrated that the Alliance's C3 (Command, Control and Communication) infrastructure still relies on solutions inherited from the Cold War, characterized by low resilience to contemporary cyber operations[31]. The authors point to, among others, the risk of data manipulation, disruption of information flow, supply chain attacks, and the phenomenon of "entanglement" of conventional and nuclear systems, which in extreme conditions may lead to unintended escalation. Key conclusion: modernization

---

[25] B. Terebiński, P. Kamieński, Zagrożenia dla systemu łączności na współczesnym polu walki, Przegląd Sił Zbrojnych 5/2022, p. 41-49.

[26] K. Wysocki, Maskowanie jako antyfora rozpoznania, [in:] K. Wysocki, W. Kuchta (eds.), Techniczne i organizacyjne aspekty współczesnego maskowania, ASzWoj, Warszawa 2022, p. 205-250.

[27] Ibidem.

[28] K. Wysocki, E. Jastrzębska, Współczesne uwarunkowania maskowania stanowisk dowodzenia, Przegląd Sił Zbrojnych nr 2/2021, p. 66-77.

[29] See: M. Beagle, Beagle et al., The Graveyard of Command Posts..., op. cit.

[30] Lessons Learned from the Ukrainian…, op. cit.

[31] A. Inverarity, A. Unal, Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems, Chatham House, London 2020, p. 5-18.

of C3 systems requires not only a technical update but primarily the introduction of cyber resilience already in the design phase (*security by design*).

The second important area of research is the resilience of US command systems, especially in the context of functioning in an environment with significant jamming. The document *Weathering the Cyber Storm* emphasizes the necessity of transforming the approach to C2 protection from a perimeter model to a model of continuous, dynamic resilience, encompassing automation of response, decentralization of network nodes, flexible data rerouting, and integration of cyber and EW at the tactical level[32]. This thesis finds confirmation in the doctrinal document *FM 3-12 Cyberspace and Electronic Warfare Operations*, which indicates that maintaining freedom of action in cyberspace and the electromagnetic spectrum constitutes a necessary condition for the survival and effective functioning of Command Posts[33].

The last stream of literature is devoted to building multi-domain situational awareness (MDO) and integrating data from the cyber, information, electromagnetic, and kinetic domains. In the work by Conti, Nelson, and Raymond *Towards a Cyber Common Operating Picture* (COP), it was demonstrated that the lack of a coherent "Cyber COP" causes commanders to possess an advanced situational picture in the kinetic domain but operate in a "blind zone" in the cyber domain[34].

Particularly insufficiently recognized is the national dimension including the possibility of adapting solutions resulting from the experiences of the Armed Forces of Ukraine and NATO doctrines to the organizational, equipment, and legal realities of the Polish Armed Forces. In this context, this article fits into the existing body of work but simultaneously fills the indicated gap by proposing a conceptual model of integrated protection and cybersecurity of Command Posts in conditions of contemporary armed conflicts.

General Remarks – Results and Discussion

Analysis of the experiences of the Armed Forces of Ukraine and research results from NATO and the USA confirm that contemporary Command Posts function in an environment very heavily saturated with ISR sensors, SIGINT, SAR, IMINT systems, and integrated precision strike effectors. Research results indicate unequivocally that the traditional model of large, static, and highly emissive Command Posts is incapable of survival under conditions of simultaneous kinetic, electromagnetic, and cyber engagement. The case of the so-called "graveyard of command posts" in the Chornobaivka region, described by M. Beagle and co-authors, shows that consolidated, tent-based Command Posts become an easy target for integrated adversary targeting, based on multispectral reconnaissance and precision long-range fire[35]. Conversely, the CALL report regarding the survivability of Command Posts of the Territorial Defense Forces of Ukraine confirms that lack of mobility, excessive size, and high electromagnetic signature of Command Posts lead to a rapid decline in survivability capability, regardless of their level of physical protection[36].

---

[32] See: S. T. Wieland, Weathering the Cyber Storm: The Military's Resiliency to Cyber Attacks in Future Warfare, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama, June 2012.
[33] Cf.: FM 3-12 Cyberspace and Electronic Warfare Operations, Headquarters, Department of the Army, Washington D.C. 2021.
[34] G. Conti, D. Raymond, J. Nelson, Towards a Cyber Common Operating Picture, [in:] 2013 5th International Conference on Cyber Conflict, K. Podins, J. Stinissen, M. Maybaum (Eds.), NATO CCD COE Publications, Tallinn 2013.
[35] Cf.: M. Beagle, J. C. Slider, M. R. Arrol, op.cit.
[36] See: Lessons Learned from the Ukrainian…, op.cit.

These results indicate that the primary determinant of Command Post survivability is the combination of mobility, dispersion, and signature minimization electromagnetic, thermal, and informational. In this context, the traditional paradigm of a "large Command Post as a coordination center" proves inadequate for the realities of multi-domain conflicts.

The SSSCIP report from 2022–2025 unequivocally proves that the Russian Federation employs a coordinated strike system in which cyberattacks, EW actions, penetration of ICT networks, jamming of ISR sensors, and missile strikes are integrated into a single targeting process, directed inter alia at Command Posts[37]. *Wiper*-type cyber operations, communication jamming, attacks on ICT infrastructure, and disinformation actions are planned to lead to the temporary "blinding" of the C2 system just before the execution of a kinetic strike. Data from Ukraine show that even well-fortified command facilities lose operational value if persistent degradation of their ICT systems and communication networks occurs.

In US doctrinal documents, especially *FM 3-12 Cyberspace and Electronic Warfare Operations*, it is emphasized that maintaining freedom of action in cyberspace and the electromagnetic spectrum constitutes a necessary condition for the effectiveness and survivability of Command Posts[38]. Combined with recommendations contained in the *Army Futures Command Protection Concept 2028*, it can be stated that Command Post protection must be understood as a systemic and multi-layered function, which must be built simultaneously in four spaces: physical, informational, electromagnetic, and cyber[39]. This concept unequivocally indicates that the traditional, passive approach to protection ceases to be sufficient, and the future operational environment saturated with adversary ISR means, multi-domain long-range effectors, and automated targeting tools requires a transition to active, preemptive, and integrated protection, based on constant signal analysis, threat dynamics, and the capability for rapid reconfiguration of command systems. Implementation of *all-domain protection* becomes key, encompassing, among others, dispersion of CP nodes, system mobility, network and sensor redundancy, continuous emission assessment, and integration of anti-access, anti-radiation, counter-drone, cyber-defense, and information actions. The document also indicates that Command Post protection cannot be treated as a "local" task, executed exclusively at the brigade or division level, but as an element of a coordinated multi-echelon architecture, in which all CP nodes from posts deployed in the "field", through rear posts, to strategic-level Command Posts function within a single, coordinated logic of protection and maintenance of so-called *critical capabilities, assets and activities* (*CCAAs*)[40]. The analysis results therefore confirm that the integration of domains physical, informational, and cyber is not an additional option, but a necessary condition for the survival of the contemporary C2 system, which is exposed to simultaneous kinetic, radio-electronic, and cyber engagement. Only such a systems approach enables the limitation of the adversary's ISR advantage, the breaking of their A2/AD capabilities, and the minimization of Command Post vulnerability to the effects of long-range fire assets, drones, cyberattacks, and electromagnetic jamming. The *Army Futures Command Protection Concept 2028* unequivocally emphasizes that future multi-domain operations will require the capability to coordinate protection in near-real-time, combine sensors and

[37] Cf.: War and Cyber…, op.cit.
[38] See: FM 3-12 Cyberspace and Electronic…, op.cit.
[39] Army Futures Command Concept for Protection 2028, U.S. Army Futures Command, AFC Pamphlet 71-20-7, 7 April 2021.
[40] Ibidem.

effectors of all domains, and conduct active defense, the goal of which is maintaining information and decision superiority necessary for Command Post functioning[41].

Results of the analysis of a series of American publications regarding Command Post transformation confirm that electromagnetic signature reduction and CP miniaturization are treated in the US Army as a strategic priority, not merely a technical problem. In the article *Army Wants to "Reimagine" Electromagnetic Signature Management*[42], it is indicated that contemporary Command Posts generate excessive emission both in the radio band and in the digital layer which in battlefield conditions saturated with ISR sensors makes them "glowing beacons" for the adversary. Subsequent texts *The Army Wants Smaller Command Posts – But First It Needs Great Software*[43] and *Army Scrambles to Make Command Posts Survivable*[44] emphasize that the solution is not merely introducing new communication means, but deep doctrinal-organizational reform: miniaturization and dispersion of Command Posts, shortening setup and tear-down times, simplifying staff processes, and basing them on lighter, cloud-based software solutions. Finally, the articles *Signature Management Is Key Tenet of Army's Digital Transformation*[45] and *The Need for Speed: Technological Advances Require Agile Command Posts* place the problem of signature reduction within the broader digital transformation of the army combining emission management with process automation, resource virtualization, cloud utilization, and the construction of "agile command posts" capable of operating in a decision cycle shorter than the tempo of adversary engagement.

A significant group of results is provided by research and analyses devoted to Command Post electromagnetic signature reduction. Articles and reports regarding Command Post transformation in the US Army emphasize that protection effectiveness is determined to the greatest degree by: signature reduction (EMCON, limiting the number of devices, emission management automation), increasing mobility, and the capability for continuous dispersion[46]. Publications describing the subject matter indicate that departing from large, tent-based Command Posts in favor of smaller, mobile, and redundant C2 nodes allows for reducing the probability of detection and destruction, while simultaneously shortening the setup and tear-down time of the post.

Supplementing the above observations with the legal dimension, L. A. Parker in the work *US Military Legal Doctrine and the Emerging Wartime Cyber Environment* notes that the evolution of Command Posts their miniaturization, dispersion, utilization of civilian infrastructure, and application of advanced signature management

---

[41] Ibidem.

[42] Army Wants to "Reimagine" Electromagnetic Signature Management, DefenseScoop, https://defensescoop.com/2023/10/11/army-wants-to-reimagine-electromagnetic-signature-management/ [Accessed: November 21, 2025].

[43] The Army Wants Smaller Command Posts – But First It Needs Great Software, Defense One, https://www.defenseone.com/defense-systems/2023/12/ army-wants-smaller-command-posts-first-it-needs-great-software/392878/ [Accessed: November 21, 2025].

[44] Army Scrambles to Make Command Posts Survivable, National Defense Magazine, https://www.nationaldefensemagazine.org/articles/2017/12/1/arm y-scrambles-to-make-command-posts-survivable [Accessed: November 21, 2025].

[45] Signature Management Is Key Tenet of Army's Digital Transformation, DefenseScoop, https://defensescoop.com/2023/08/17/signature-management-is-key-tenet-of-armys-digital-transformation/ [Accessed: November 22, 2025].

[46] The Army wants to reduce electronic signatures of its command posts, C4ISRNET, https://www.c4isrnet.com/battlefield-tech/it-networks/2020/08/11/ the-army-wants-to-reduce-electronic-signatures-of-its-command-posts [Accessed: November 23, 2025].

generates new challenges from the perspective of the Law of Armed Conflict[47]. The author indicates that, on one hand, smaller and better-camouflaged CPs make unambiguous identification and classification of targets difficult for the adversary, which may limit the risk of disproportionate strikes. On the other hand, advanced signature management techniques and locating C2 elements near or inside civilian infrastructure (e.g., urban facilities, telecommunication networks) may complicate the assessment of object status, increase the risk of collateral damage, and generate interpretational disputes regarding the principles of distinction and proportionality.

During the armed conflict in Ukraine, Ukrainian troops developed a set of Tactics, Techniques, and Procedures (TTP) aimed at increasing the resilience and survivability capability of Command Posts under conditions of intensive adversary engagement. The most significant actions in this scope include, among others: appropriate selection of command point locations (platoon, company) at a distance of 2 to 5 km from the line of contact, and in the case of higher-echelon posts even up to 10 km, to limit the risk of detection and engagement; introduction of strict electromagnetic discipline regimes to minimize signal emission and electromagnetic signature; as well as maintaining high mobility and capability for CP relocation in a short time, depending on the dynamics of the tactical situation. These solutions allowed for limiting the effectiveness of adversary reconnaissance, including that conducted utilizing unmanned aerial systems, and reducing vulnerability to indirect fire and electronic warfare system engagement[48].

In Polish literature, especially in the works of K. Wysocki and E. Jastrzębska, it is emphasized that Command Post camouflage in visual, engineering, and electromagnetic dimensions - is effective only when supported by dummy-disinformation actions and rigorously executed OPSEC, encompassing, among others, information flow control, discipline in the operation of communication means, and limitation of activity patterns detectable by the adversary[49]. Contemporary reconnaissance means, utilizing data correlation from multiple sensors (IMINT, SIGINT, OSINT, MASINT), are capable of reconstructing the Command Post picture even with limited radio emission. These results unequivocally confirm that effective protection in the electromagnetic domain must be coupled with the reorganization of staff, logistical, and engineering processes and thus with a deep transformation of the entire culture of Command Post functioning.

Analysis of contemporary armed conflicts, particularly Ukrainian experiences from 2022–2025, unequivocally indicates that the concept of centralized, static Command Posts has lost operational value. In an environment of intensive battlefield saturation with ISR sensors, SIGINT/ELINT capabilities, and precision fire assets, every Command Post with a fixed location rapidly becomes identifiable and vulnerable to neutralization. Under conditions of multi-domain conflict, CP survival depends not on their physical resilience, but on the capability for continuous maneuver, dispersion, and electromagnetic signature reduction. The urbanized environment - due to its dense infrastructure, built-up areas, and diverse technical structure offers unique possibilities for concealment, camouflage, and dispersion of C2 elements. Simultaneously, it forces

[47] E. Bobenrieth, S. Watts, US military legal doctrine and the emerging wartime cyber environment, International Review of the Red Cross, Vol. 107, Nr 928, 2025, p. 311–334.
[48] See: S. Ullrich, S. Moriarty, Lessons Learned from the Ukrainian Territorial Defense Forces: Command Post Survivability, Special Report No. 24-862, Center for Army Lessons Learned (CALL), Fort Leavenworth, February 2024.
[49] K. Wysocki, E. Jastrzębska, op.cit.

the application of more advanced methods of command organization, integrating physical, informational, and electromagnetic security.

Conclusions flowing from the analysis of multi-domain conflicts point to the necessity of doctrinal recognition of distributed Command Posts as the basic model of C2 organization in an urban environment. This requires preparing armed forces to create modular, redundant structures capable of autonomous operation and rapid location change. Key is the development of a set of TTPs encompassing civilian infrastructure adaptation, conducting technical assessments of urban objects, and planning CP component deployment considering multispectral camouflage, electromagnetic discipline, and information security. Concurrently, it is necessary to invest in technologies enabling distributed command jam-resistant communication means, independent power sources, systems operating in the cloud, and support tools for mobile C2 structures.

Both the experiences of the Armed Forces of Ukraine and analyses by NATO and the USA confirm that effective protection and cybersecurity of Command Posts require the implementation of an integrated protection system combining engineering fortification, Command Post mobility and dispersion, electromagnetic signature reduction, C2 system redundancy, active cyber defense, and coherent utilization of MILDEC and OPSEC. Only such an approach enables the maintenance of command continuity and increasing the resilience of control structures to coordinated adversary engagement. Simultaneously, it aligns with the development direction of the All-Domain Command and Control (ADC2)[50] concept, which treats the Command Post as a multi-domain node functioning simultaneously in physical, informational, electromagnetic, and cyber space.

Literature

AFMAN 10-207, Command Posts (AFGM 2025-01), Department of the Air Force, Headquarters United States Air Force, Washington D.C.

Army Futures Command Concept for Protection 2028, U.S. Army Futures Command, AFC Pamphlet 71-20-7.

Beagle, M. Slider, J.C. Arrol, M.R., The Graveyard of Command Posts: What Chornobaivka Should Teach Us about Command and Control in Large-Scale Combat Operations, Military Review Online Exclusive 2023.

Bobenrieth, E. Watts, S., US military legal doctrine and the emerging wartime cyber environment, „International Review of the Red Cross" 2025, vol. 107, no. 928.

Broyles, C.A. Richter, C., Concrete Command: Why Combat Training Centers Should Prioritize Training on Urban Command Posts, „Military Review" 2023.

Cecil, A.S. Butler, K., Command Post Operations, Military Review Online Exclusive 2018.

Conti, G. Raymond, D. Nelson, J., Towards a Cyber Common Operating Picture [in:] Podins, K. Stinissen, J. Maybaum, M. (Eds.) 2013 5th International Conference on Cyber Conflict, Tallinn: NATO CCD COE Publications 2013.

FM 3-12 Cyberspace and Electronic Warfare Operations, Headquarters, Department of the Army, Washington D.C.

Inverarity, A. Unal, A., Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems, London: Chatham House 2020.

Kohli, A., The Commander's Place on the Battlefield, „The RUSI Journal" 2024, vol. 169, no. 4.

Magnuson, S., Army Scrambles to Make Command Posts Survivable, „National Defense Magazine" 2017, https://www.nationaldefensemagazine.org/articles.

[50] AFMAN 10-207: Command Posts…, op.cit.

MIL-HDBK-1013/1A, Design Guidelines for Physical Security of Facilities, Department of Defense, Washington D.C.
NATO Allied Command Transformation, Joint All Domain Command and Control and Multi-Domain Operations, NATO ACT.
Pegg, C. Smith, P. The Need for Speed: Technological Advances Require Agile Command Posts, Association of the United States Army.
Rivera, J.P., Command Post Threats Beyond the Electromagnetic Spectrum, „NCO Journal" 2024.
Signature Management Is Key Tenet of Army's Digital Transformation, DefenseScoop.
Slusher, M.N., Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience, Defense Analysis White Paper 2025.
Ullrich, S. Moriarty, S., Lessons Learned from the Ukrainian Territorial Defense Forces: Command Post Survivability, Special Report No. 24-862, Center for Army Lessons Learned (CALL), Fort Leavenworth 2024.
Terebiński, B., Bezpieczeństwo informacji na początku trzeciej dekady XXI wieku – wybrane aspekty, Warszawa 2023.
Terebiński, B. Kamieński, P., Zagrożenia dla systemu łączności na współczesnym polu walki, „Przegląd Sił Zbrojnych" 2022, no. 5.
Wieland, S.T., Weathering the Cyber Storm: The Military's Resiliency to Cyber Attacks in Future Warfare, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama 2012.
Wolfel, R.L. Richmond, A. Ridgeway, J., Dense Urban Environments: The Crucible of Multi-Domain Operations, „Military Review" 2021.
Wrzosek, M., Challenges of contemporary command and future military operations, „Scientific Journal of the Military University of Land Forces" 2022, vol. 54, no. 1(203).
Wysocki, K., Maskowanie jako antyfora rozpoznania, [in:] Wysocki, K. Kuchta, W. (eds.), Techniczne i organizacyjne aspekty współczesnego maskowania, Warszawa 2022.
Wysocki, K., Jastrzębska, E. Współczesne uwarunkowania maskowania stanowisk dowodzenia, „Przegląd Sił Zbrojnych" 2021, no. 2.
Zalewski, J. Dzierżyński, D. G. Wojna informacyjna w odbudowie rosyjskiej mocarstwowości, Warszawa 2019.