

BRIDGING THE GAP BETWEEN PROFESSIONALISM AND DIGITAL INFRASTRUCTURE

Zornitsa Atanasova

Rakovski National Defense College

Abstract. Digital transformation has become a strategic priority for contemporary armed forces, shaping command structures, information flows, and operational effectiveness. Despite institutional ambitions for modernization, the degree to which digital infrastructure effectively supports professional performance remains an empirical question. This study examines the perceived level of digitalization within the Bulgarian Armed Forces in 2025 and analyzes its relationship to organizational effectiveness.

The research is based on a representative sociological survey conducted among active military personnel. Quantitative data assess the perceived digitalization of computer/general equipment and military equipment, while qualitative responses explore issues related to process automation, communication interoperability, and technological modernization. Descriptive statistics and thematic content analysis were employed to interpret the findings.

The findings suggest the existence of a structural gap between professionalism and digital infrastructure. While professional commitment and accumulated expertise currently sustain organizational performance, reliance on human adaptability as a compensatory mechanism may limit long-term sustainability and leadership transformation. The study contributes to the broader debate on digital transformation in military organizations by framing technological modernization as a prerequisite for sustainable operational effectiveness.

Keywords: Digital transformation; Military leadership; Digital infrastructure; Professionalism; Organizational effectiveness; Situational awareness; Command and control (C2); Cyber capability; Defense modernization; Organizational resilience.

1. Introduction

Digital transformation is widely recognized as a strategic priority in contemporary defense systems. Military organizations increasingly operate in environments shaped by networked communication, cyber threats, and accelerated decision cycles. In such contexts, digital infrastructure is expected to enhance coordination, information processing, and operational effectiveness. Strategic planning documents emphasize modernization of communication systems, interoperability, and technological integration as prerequisites for sustainable military capability.

However, the practical implementation of digital transformation does not always progress at the same pace as institutional ambition. This discrepancy raises an important empirical question: to what extent does existing digital infrastructure effectively support professional performance within military organizations?

The present study addresses this issue by examining perceptions of digitalization in the Bulgarian Armed Forces in 2025. Using data from a representative sociological survey among active service members, the research focuses on two key evaluative dimensions: the perceived level of digitalization of computer/general equipment and the digitalization of military equipment. These indicators are analyzed alongside qualitative reflections concerning process automation, communication systems, and technological modernization.

The findings reveal a consistent pattern. The perceived level of digital infrastructure remains below the neutral midpoint of the evaluative scale, particularly regarding military equipment. At the same time, indicators related to professional task performance demonstrate relative stability. Factor analysis further differentiates between “Quality of Work Performance” and “Contribution of Digitalization to Effective Performance,” suggesting that professional competence and technological enablement represent analytically distinct dimensions.

This divergence indicates the existence of a structural gap between professionalism and digital infrastructure. Organizational performance appears to be sustained primarily through accumulated expertise, discipline, and established routines rather than through technologically integrated systems. While such compensatory dynamics may ensure short-term stability, they raise questions about long-term sustainability, leadership adaptability, and readiness for digitally intensive operational environments.

By empirically examining this imbalance, the study contributes to the understanding of digital transformation not merely as a technological process, but as an organizational condition directly affecting leadership, coordination, and strategic resilience.

2. Theoretical Framework

In recent decades, digitalization has evolved into a strategic driver reshaping national defense systems and redefining the operational environment. Contemporary military operations are characterized by continuous information flows, automated command and control (C2) systems, and emerging hybrid and cyber threats. High technologies fundamentally transform command practices, requiring leaders capable of operating in digitally mediated, network-centric environments. Cyber operations and information warfare increasingly influence strategic priorities, creating a demand for officers with digital literacy and cyber competence. Flexible, network-enabled leadership models progressively challenge traditional hierarchical command structures, while expectations toward digital leadership emphasize autonomy, technological integration, transparency, and coordination.

2.1. Conceptual Foundations of Military Digital Transformation and Leadership

At the conceptual level, digitalization is initially defined as the conversion of analog into digital data; however, contemporary scholarship frames it as a structural driver of broader organizational transformation (Shafiq & Mujawar, 2021). Digital transformation refers to the integrated embedding of digital technologies into organizational practices, strategies, and structures, resulting in systemic change in how institutions operate and create value (Pereira, Cardoso, Sá, & Faria, 2022). It is not a discrete technological upgrade but a continuous and strategic reconfiguration of organizational architecture and culture. Procedurally, digitalization increases system integration, complexity of configurations, and interdependence among organizational actors (De Boisboissel, 2021). It enhances efficiency, accelerates operational processes, and expands innovation capacity (De Boisboissel, 2021; Andriole, 2018). Substantively, digital platforms enable real-time communication, remote coordination,

and the removal of geographical constraints, while simultaneously introducing risks of information overload, uncertainty, and interpretive ambiguity (Lindh, 2022).

These general organizational tendencies acquire specific strategic significance in the military domain. Leading contemporary armies invest in integrated communication and information infrastructures that enable network-based operations, real-time command, and interoperability across multinational frameworks. In the Bulgarian context, strategic planning documents explicitly prioritize the modernization of communication and information capabilities, the development of cyber defense capacities, and interoperability with NATO and the European Union. The Plan for the Development of the Bulgarian Armed Forces to 2026 emphasizes the establishment of integrated C2 systems and the conduct of operations in digital and information environments. Artificial intelligence is identified as a strategic enabler, with policy provisions for the development and deployment of autonomous and semi-autonomous systems, AI-supported decision-making, and real-time operational management. These strategic orientations align with broader international trends toward technologically dominated and hybrid operational environments.

Within this evolving context, informational infrastructure functions as a foundational condition for situational awareness. Situational awareness (SA) is defined as the process of perceiving environmental elements, comprehending their meaning, and projecting their future states. The widely accepted three-level model proposed by Endsley (1995, 1998, 1999) conceptualizes SA as consisting of perception (Level 1), comprehension (Level 2), and projection (Level 3). At Level 1, operators identify relevant objects, attributes, and dynamics in the environment. At Level 2, these elements are integrated into a coherent representation aligned with operational objectives. At Level 3, the decision-maker anticipates future developments based on the synthesized understanding of the situation. This final level is critical in dynamic and high-risk military environments, where anticipatory decision-making determines operational success (Endsley, 1995; 1999).

Situational awareness is central to military C2 systems, whose design aims to selectively present operational information in ways that facilitate understanding and optimal action. In military theory, SA corresponds to the “Observe” and “Orient” phases of the OODA loop (Observe–Orient–Decide–Act). Achieving superiority in situational awareness enables commanders to accelerate decision cycles, shape the operational environment, and effectively enter and disrupt the opponent’s OODA loop, thereby gaining tactical dominance. Conversely, the loss of situational awareness leads to loss of initiative and strategic disadvantage.

Contemporary extensions of Endsley’s framework further integrate technological enablers into the situational awareness process. Munir, Aved, and Blasch (2022) propose an enhanced model incorporating mission-level inputs from strategic and operational command and integrating artificial intelligence–supported decision-making and dynamic resource management. In this architecture, multiple sensors continuously collect environmental data, which are fused to eliminate redundancy before being processed within the three-level SA core. AI systems generate decision-support recommendations based on integrated data and projected developments; however, final authority remains with commanders, who evaluate AI inputs in light of contextual judgment (Munir, Aved, & Blasch, 2021; 2022). Thus, digital infrastructure, sensor fusion, and AI-supported analytics directly strengthen the perception, comprehension, and projection capacities that define situational awareness.

The effectiveness of such digitally enabled command systems ultimately depends on the technological literacy and cognitive competence of military leaders. Leadership research emphasizes that digital transformation requires multidimensional competencies combining technical, strategic, and people-oriented skills (Andriole, 2018; Tekic & Koroteev, 2019). Academic debates highlight the dual role of leaders in managing technological change while fostering organizational acceptance of innovation (Gardner et al., 2010; Kirkland, 2014). The concept of e-leadership captures this shift toward leadership enacted through and within digital environments (Avolio et al., 2000; Avolio et al., 2014), although the field remains theoretically fragmented (Schwarzmüller et al., 2018).

Müller (2024), building on the Competing Values Framework (Cameron & Quinn, 2006), identifies four archetypes of leadership competencies in digital transformation—challenger, bricoleur, organizer, and competitor—each reflecting different orientations toward flexibility, stability, internal integration, and external positioning (Tekic & Koroteev, 2019). Across these archetypes, technological foresight, strategic communication, and innovation orientation (Singh & Hess, 2017; Sousa & Rocha, 2019; Kane et al., 2019; Cortellazzo et al., 2019; Shoop et al., 2015; Imran et al., 2020), process optimization and resource alignment (Prince, 2017; Grigore & Coman, 2018; Ravarini et al., 2020; Benaroch & Chernobai, 2017), collaborative integration (Roman et al., 2019; Aksal, 2015; van Wart et al., 2019), and strategic data utilization (Valentine & Stewart, 2015; Coertze & von Solms, 2014; Peppard et al., 2011; Gadasina et al., 2017) are consistently emphasized.

In the military context, these competencies translate into technological literacy and informational leadership. Leaders must master IT tools and manage complex information flows without generating overload or suppressing innovation. Maintaining a functional balance between control and autonomy becomes central to effective command (Valentine & Stewart, 2015; McMaster, 2011). Cognitive competence—encompassing analytical reasoning, adaptive thinking, and the ability to synthesize large volumes of operational data—must be integrated with technological competence to ensure that digital systems enhance situational awareness rather than constrain decision-making.

In sum, digital transformation in contemporary armed forces represents a systemic reconfiguration of the operational environment, informational infrastructure, and leadership competencies. Integrated communication networks, AI-enabled decision support, and advanced C2 architectures strengthen situational awareness across perception, comprehension, and projection levels (Endsley, 1995; 1999; Munir, Aved, & Blasch, 2022). However, their strategic effectiveness depends on cognitively and technologically competent leaders capable of interpreting complex data, preserving initiative within the OODA cycle, and sustaining operational advantage in digitally intensive security environments.

2.2. International Military Experience in Digital Transformation

Military digital transformation is not limited to acquiring modern equipment but depends on integrating technology, organization, cybersecurity, interoperability, personnel skills, and leadership. Estonia and Ukraine illustrate two contrasting models: Estonia's planned, resilience-based approach and Ukraine's rapid, combat-driven adaptation.

The Estonian experience: institutional integration and cyber resilience

Estonia's highly digitalized society enables strong integration between public administration and defence but also creates vulnerability to cyber disruptions, as shown by the 2007 attacks (Czosseck et al., 2011). In response, cyber defence became a core element of national security, embedded in structures, planning, training, and international cooperation.

The establishment of a Cyber Command under the Defence Forces highlights that cybersecurity is treated as an operational capability (Estonian Ministry of Defence, 2026). Estonia also invests in human capital through cyber conscription, combining military training with technical expertise, and integrates civilian specialists via the Cyber Defence Unit (Kaska et al., 2013).

Participation in NATO cyber exercises and testing environments further strengthens interoperability and preparedness. The key lesson is that digital resilience requires integrated systems, continuous learning, and cooperation. However, high digital dependence also increases vulnerability, requiring redundancy and the ability to operate under degraded conditions.

The Ukrainian experience: operational adaptation and digitally enabled command

Ukraine's digital transformation has been shaped by ongoing conflict, leading to rapid innovation, decentralized development, and close cooperation between users and developers. A key example is the DELTA system, which integrates battlefield data to support situational awareness, planning, and coordination (Ministry of Defence of Ukraine, 2024).

DELTA and related systems shorten decision cycles by linking sensors, command elements, and weapons. They support decentralized command but also risk encouraging excessive control by higher levels. Ukraine's model shows that effective digitalization often emerges from tactical-level innovation and continuous feedback.

Participation in NATO interoperability exercises demonstrates the importance of aligning national systems with allied standards (NATO ACT, 2025). However, rapid development also creates challenges such as system fragmentation, cybersecurity risks, and dependence on external technologies (Tenenbaum et al., 2026). Information overload is another risk, highlighting the need to transform data into actionable knowledge.

Comparative lessons for military digital transformation

Both cases show that digital transformation must be integrated into the broader organizational system. Interoperability is essential to avoid fragmentation and ensure effective cooperation. Technological modernization must be supported by personnel training and leadership capable of managing digital systems.

Resilience is critical: forces must operate under cyberattacks, disrupted communications, and limited data. Redundancy, modular systems, and alternative procedures are therefore necessary.

These lessons are relevant to the Bulgarian Armed Forces. The limited perceived impact of digital equipment reflects not only technological gaps but also insufficient integration, interoperability, and training. Effective transformation requires a systemic

approach in which technology supports professional competence and mission-oriented command.

3. Methodology

3.1 Research Design

The study is based on a representative sociological survey conducted in 2025 among active military personnel in the Bulgarian Armed Forces. The study is based on a representative sociological survey conducted in 2025 among active military personnel in the Bulgarian Armed Forces. The data analyzed in this article originate from the official report “Motivation of Personnel in Formations of the Bulgarian Armed Forces”, prepared by the Institute for Perspective and Innovation in Defense (IPID), Sofia, November 2025 (Reg. No. SI-29-10294/25.11.2025). (ИПИО, 2025) Data were collected through an anonymous, structured questionnaire administered in field conditions within military formations. Participation was voluntary, and confidentiality was guaranteed in order to ensure candid responses on issues related to digitalization and technological infrastructure.

The sampling model allows the results to be generalized to the broader population of service members with a maximum admissible stochastic error of $\pm 2.5\%$. The present article focuses exclusively on the 2025 dataset and analyzes only the evaluative items concerning the level of digitalization—specifically the digitalization of computer/general equipment and military equipment—together with the open-ended responses addressing digital transformation and process automation. Quantitative data were examined through descriptive statistics, while qualitative responses were analyzed using thematic content analysis.

3.2 Sample

The sample reflects the structural composition of the Bulgarian Armed Forces. Soldiers and sailors constitute the largest group (41.6%), followed by sergeants and warrant officers (35.0%), junior officers (14.3%), senior officers (5.3%), and officer candidates (1.6%). This distribution ensures representation across both command and execution levels.

In terms of service branches, respondents primarily serve in the Land Forces (42.2%), followed by the Air Force (22.7%) and the Navy (16.3%), with additional participation from joint and support commands. The dominant age group is 41–50 years (39.9%), indicating a professionally experienced cohort. Family-related indicators show that a considerable proportion of respondents have young children, providing contextual background for interpreting perceptions of administrative burden and efficiency.

Overall, the sample provides a balanced and representative basis for examining perceptions of digital infrastructure within the Armed Forces in 2025

3.3 Instruments

3.3.1 Quantitative Digitalization Items

The quantitative component relevant to the present study consists of evaluative items measuring the perceived level of digitalization within the military organization. Respondents were asked to assess the degree of digitalization of computer and general equipment used in

routine (peacetime) activities, as well as the level of digitalization of military equipment. These items capture the perceived technological maturity of both administrative and operational domains.

All evaluations were recorded on a five-point Likert-type scale ranging from 1 (“strongly disagree”) to 5 (“strongly agree”), allowing for the assessment of central tendencies and comparative interpretation of perceived adequacy. The focus on these specific indicators reflects the conceptual distinction between professional performance and technological infrastructure that underpins the central argument of the article.

3.3.2 Open-Ended Question on Digitalization

In addition to the structured items, the questionnaire included an open-ended question inviting respondents to express opinions, suggestions, and critical reflections concerning digitalization within their formations. This qualitative component enabled the collection of unstructured data addressing issues such as process automation, communication systems, technological modernization, and administrative burden.

The open responses provide insight into how service members interpret the practical implications of digital infrastructure, particularly in relation to bureaucratic procedures, interoperability of communication systems, and the modernization of equipment. This qualitative dimension complements the quantitative assessments by revealing the underlying organizational concerns associated with digital transformation.

3.4 Data Analysis

The quantitative data were analyzed using descriptive statistical methods, primarily through the calculation of mean values, which allow for the evaluation of the overall perceived level of digitalization. Where applicable, reliability indicators of relevant scales are reported in accordance with standard psychometric practice.

The qualitative responses were examined through thematic content analysis. This procedure involved identifying recurring patterns, grouping them into broader thematic categories, and interpreting their organizational significance. The integration of quantitative and qualitative approaches supports a more comprehensive understanding of the perceived gap between professionalism and digital infrastructure.

4. Results

4.1 Quantitative Results: Perceived Level of Digitalization (2025)

The quantitative findings for 2025 reveal a consistently low evaluation of digital infrastructure within the Bulgarian Armed Forces. The lowest mean scores are associated with the digitalization of computer and general equipment used in routine activities ($M = 2.97$) and, even more prominently, with the digitalization of military equipment ($M = 2.72$). Both values remain below the neutral midpoint of the scale, indicating that respondents tend to perceive the current level of technological modernization as insufficient.

The interpretation provided in the analytical reports emphasizes that these results point to a structural deficit in technological support and digital transformation. Insufficient digital infrastructure is considered likely to constrain rapid information processing, situational awareness, and overall operational readiness. Although other organizational indicators

demonstrate relative stability, digitalization remains the weakest evaluated dimension, suggesting a persistent imbalance between professional performance and technological enablement.

Taken together, the 2025 data indicate that while the organizational system continues to function through established professional routines, the perceived level of digital maturity does not meet the expectations associated with contemporary military operations. This discrepancy constitutes the empirical foundation for the argument that a gap exists between professionalism and digital infrastructure.

The factor analysis of the perceived organizational effectiveness scale yielded a two-factor structure that conceptually differentiates traditional professional performance from technologically supported effectiveness. The first factor, labeled **“Quality of Work Performance,”** includes items related to effective task execution, the ability to respond adequately to unexpected workload, and the optimal use of available resources. This dimension reflects the core professional capacity of the organization to function efficiently under routine and demanding conditions.

The second factor, defined as **“Contribution of the Level of Digitalization to Effective Work Performance,”** encompasses items assessing the extent to which digital infrastructure supports the execution of tasks within the military formation. This factor captures the perceived technological enablement of organizational performance.

The two factors are moderately correlated ($r = .37^{**}$), indicating a meaningful relationship while preserving conceptual distinctiveness. Both factors demonstrate satisfactory internal consistency, with Cronbach’s alpha coefficients of $\alpha = .75$ for the first factor and $\alpha = .82$ for the second.

This factorial structure empirically supports the analytical distinction between human professional competence and digital infrastructure, which forms the theoretical foundation of the present study.

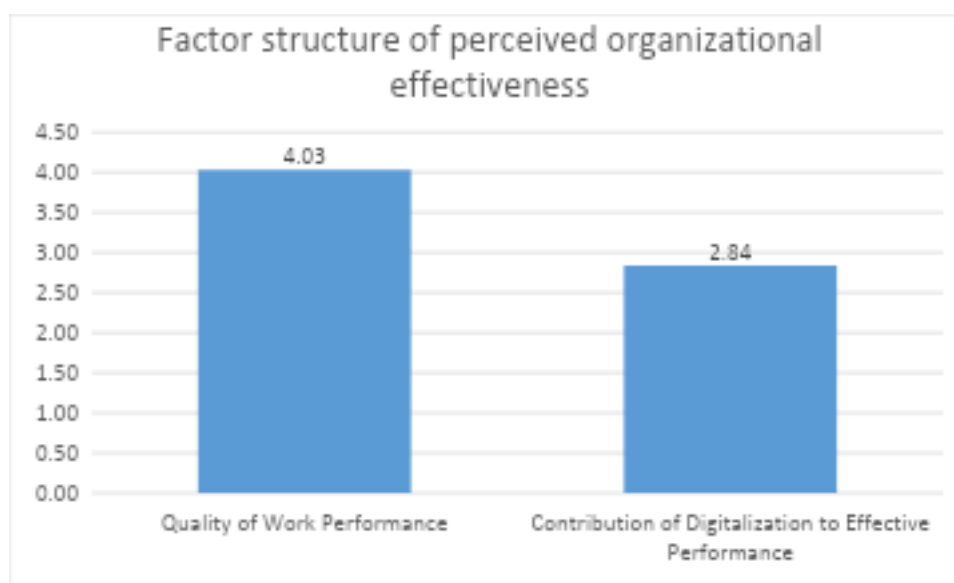


Fig. 1. Factor structure of perceived organizational effectiveness: relationship between “Quality of Work Performance” and “Contribution of Digitalization to Effective Performance.”

4.2 Qualitative Results: Thematic Analysis of Open Responses

The thematic analysis of the open-ended responses reveals a consistent pattern of concerns related to the structural limitations of digital infrastructure. The first dominant theme refers to administrative burden and the lack of process automation. Respondents repeatedly emphasize the need for standardized electronic forms, integrated software systems shared between formations and headquarters, and the introduction of qualified electronic signatures. The absence of unified digital platforms is perceived as generating excessive bureaucracy, time-consuming manual procedures, and duplication of administrative efforts. Digitalization is thus framed not merely as technological modernization, but as a mechanism for reducing bureaucratic pressure and reallocating time toward core operational tasks.

A second theme concerns communication and interoperability deficits. Service members highlight insufficient compatibility of communication systems across different command levels—platoon, company, and battalion—and stress the necessity of interoperability with external institutions. Fragmented communication channels are viewed as a constraint on coordination and operational coherence, particularly in joint or interagency contexts.

The third theme addresses technological obsolescence. Many responses point to outdated equipment, limited availability of modern digital tools, and delayed modernization processes. This perceived lag in technological renewal reinforces the quantitative findings regarding the low evaluation of digital infrastructure.

Finally, a fourth theme relates to training and digital competence. Respondents underline the importance of systematic IT training and the development of digital skills across all rank categories. Younger officers are often described as potential drivers of innovation, suggesting an internal recognition that digital transformation requires both technological investment and generational adaptation. Together, these themes illustrate a shared perception that the gap between professionalism and digital infrastructure is organizational rather than individual in nature.

5. Discussion

5.1 The Structural Gap

The findings point to a clear structural discrepancy between professional capacity and technological enablement. While previous organizational indicators demonstrate sustained levels of commitment, task execution, and institutional loyalty, the digital dimension remains consistently evaluated at a comparatively low level. The mean values for the digitalization of computer equipment and military equipment fall below the neutral midpoint, reflecting a perception of insufficient technological modernization.

This divergence suggests the existence of a structural imbalance rather than a temporary operational fluctuation. Professional performance appears to be maintained through

established routines, experience, and organizational culture, whereas digital infrastructure does not yet function as a fully integrated enabling system. The moderate correlation between the “Quality of Work Performance” factor and the “Contribution of Digitalization” factor further confirms that, although related, professional effectiveness and digital support are not equivalent dimensions. The empirical evidence therefore substantiates the central thesis of a persistent gap between professionalism and digital infrastructure.

5.2 Professionalism as a Buffer

In the absence of sufficiently developed digital systems, professionalism appears to function as a compensatory mechanism. Organizational resilience is sustained through discipline, accumulated expertise, and adaptive coordination practices. Service members continue to demonstrate high levels of task commitment and loyalty, suggesting that human capital compensates for structural technological deficits.

However, reliance on professionalism as a buffer carries inherent risks. The reported levels of workload, constant concentration demands, and technical requirements indicate increasing cognitive and operational strain. When digital infrastructure fails to streamline processes and reduce administrative friction, the burden shifts to individual effort and informal coordination. Over time, such compensatory dynamics may lead to fatigue, reduced efficiency, and diminished sustainability of performance. Thus, professionalism ensures short-term stability but cannot substitute for systemic digital modernization in the long term.

5.3 Leadership Implications

The limited digital environment has direct implications for military leadership. Contemporary leadership models emphasize information processing, situational awareness, and technologically mediated coordination. When digital infrastructure is underdeveloped, the leader’s capacity to function as an informational integrator is constrained. Decision-making processes become more dependent on manual data collection and hierarchical transmission, limiting the realization of information-based leadership.

Moreover, the transition toward distributed or shared leadership presupposes reliable digital communication platforms that enable horizontal coordination and rapid role exchange. Inadequate digital systems restrict this flexibility, reinforcing traditional hierarchical patterns and reducing opportunities for adaptive team-based leadership. The qualitative findings regarding communication incompatibility and administrative fragmentation further support this conclusion.

Finally, insufficient digital support increases the cognitive load placed on leaders and subordinates alike. When technological systems do not adequately structure information flows, individuals must compensate through additional monitoring, coordination, and interpretation. This heightened cognitive demand may affect both decision quality and psychological endurance in complex operational environments.

Taken together, the discussion highlights that the gap between professionalism and digital infrastructure is not merely technical but strategic. It affects organizational sustainability, leadership transformation, and the future capacity of the Armed Forces to operate effectively in a digitally intensive security environment.

6. Conclusion

The findings of the present study indicate that the gap between professionalism and digital infrastructure is not incidental but structural in nature. The consistently low evaluations of digitalization, particularly with regard to computer equipment and military systems, suggest that technological modernization has not yet reached a level commensurate with the operational and leadership demands of a contemporary security environment. While organizational resilience and professional commitment remain strong, the reliance on human adaptability as a compensatory mechanism cannot be regarded as a sustainable long-term strategy.

From a practical perspective, the results underscore the necessity of an integrated digital strategy that aligns technological investment with organizational processes and leadership development. Digitalization should not be treated as a series of isolated technical upgrades, but as a coordinated transformation encompassing administrative automation, interoperable communication systems, and structured modernization of operational equipment. The qualitative data clearly point to the burden imposed by fragmented procedures and insufficient automation, reinforcing the need for unified digital platforms that reduce bureaucratic friction and enhance efficiency.

Furthermore, investment in communication infrastructure is essential for enabling coordination across command levels and ensuring interoperability in joint and interagency contexts. Equally important is the systematic development of digital leadership competencies. In a digitally mediated operational environment, leaders must possess not only traditional command skills but also the capacity to manage information flows, interpret technological outputs, and foster adaptive team dynamics.

The experience of Estonia and Ukraine confirms that sustainable military digital transformation requires more than technological modernization. It depends on interoperable infrastructure, cyber resilience, continuous personnel development, organizational learning, and leaders capable of integrating digital systems without weakening professional judgment and decentralized initiative. For the Bulgarian Armed Forces, closing the identified gap between professional effectiveness and digital support therefore requires a systemic approach in which technology strengthens mission command, situational awareness, and operational adaptability, while preserving the capability to operate under disrupted or degraded technological conditions.

In conclusion, the identified gap between professionalism and digital infrastructure reflects a strategic vulnerability rather than a temporary organizational shortcoming. Professionalism continues to sustain performance, yet it cannot substitute for systemic technological enablement. Digitalization, therefore, should be understood not merely as technical modernization, but as a prerequisite for sustainable organizational effectiveness and for the transformation of military leadership in the digital era.

REFERENCES

- Andriole, S. J. (2018) "Skills and Competencies for Digital Transformation," in *IT Professional*, vol. 20, no. 6, 78-81., doi: 10.1109/MITP.2018.2876926
- Aksal, F. A. (2015). Are headmasters digital leaders in school culture? *Egitim ve Bilim*, 40 (182), 77–86.

Avolio, B. J., Kahai, S., and Dodge, G. E. (2000). E-leadership: implications for theory, research, and practice. *Leader. Q.* 11, 615–668. doi: 10.1016/S1048-9843(00)00062-X

Avolio, B. J., Sosik, J. J., Kahai, S. S., and Baker, B. (2014). E-leadership: reexamining transformations in leadership source and transmission. *Leader. Q.* 25, 105–131. doi: 10.1016/j.leaqua.2013.11.003

Benaroch, M., & Chernobai, A. (2017). Operational IT failures, IT valuedestruction, and board-level IT governance changes. *MIS Quarterly*, 41(3), 729–762.

Cameron, K., & Quinn, R. (2006). Diagnosing and changing organizational culture. Based on the Competing Values Framework, Personnel Psychology (2006),doi:10.1111/j.1744-6570.2006.00052_5.x

Coertze, J., & Von Solms, R. (2014). January). The board and CIO: The IT alignment challenge (pp. 4426–4435). IEEE.

Cortellazzo, L., Bruni, E., & Zampieri, R. (2019). The role of leadership in a digitalized world: A review. *Frontiers in Psychology*, 10, 1938.

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2011). Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. *International Journal of Cyber Warfare and Terrorism*, 1(1), 24–34. doi: 10.4018/ijcwt.2011010103.

.De Boisboissel, G. (2021). New technologies and decision-making for the military. In: *Advances in decision making*. (Ed.) Fausto Pedro García Márquez. DOI: 10.5772/intechopen.98849. <https://www.intechopen.com/chapters/77502>.

.Endsley, M.R (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Hum. Factors J. Hum. Factors Ergon. Soc.* 1995, 37, 32–64. [CrossRef]

Endsley, M.R (1999). Situation Awareness in Aviation Systems. In *Handbook of Aviation Human Factors*; Garland, D.J., Wise, J.A., Hopkin, V.D., Eds.; Lawrence Erlbaum Associates Publishers: Mahwah, NJ, USA, 1999; pp. 257–276.

Estonian Ministry of Defence. (2026). Cyber security. Ministry of Defence of the Republic of Estonia.

<https://www.kaitseministeerium.ee/en/estonian-national-defence/structure-and-principles/cyber-security>. (visited on 19.07.2026)

Gardner, W. L., Lowe, K. B., Moss, T. W., Mahoney, K. T., and Coglisier, C. C. (2010). Scholarly leadership of the study of leadership: a review of 72 The leadership quarterly's second decade, 2000–2009. *Leader. Q.* 21, 922– 958. doi: 10.1016/j.leaqua.2010.10.003

Gadasina, L., Ivanova, V., & Lezina, T. (2017). Company managers competences adjustment within the frames of business digital transformation. *Journal*

Grigore, A.-M., & Coman, A. (2018). The hourglass effect: Leadership transformations in the digital era. In I. Popa, C. Dobrin, & C. Ciocoiu (Eds.). In *Proceedings of the 12th international management conference: Management perspectives in the digital era* (pp. 603–610).

Imran, F., Shahzad, K., Butt, A., & Kantola, J. (2020). Leadership competencies for digital transformation: Evidence from multiple cases. *Advances in Intelligent Systems and Computing*, 1209, 81–87

Kane, G. C., Phillips, A. N., Copulsky, J., & Andrus, G. (2019). How digital leadership is (n't) different. *MIT Sloan Management Review*, 60(3), 34– 39.

Kaska, K., Osula, A.-M., & Stinissen, J. (2013). The Cyber Defence Unit of the Estonian Defence League: Legal, policy and organisational analysis. NATO Cooperative Cyber Defence Centre of Excellence.

Tenenbaum, É., Kostiuk, B., Patiuk, D.-M., & Shapochkina, A. (2026). Mapping the MilTech war: Eight lessons from Ukraine's battlefield. *Focus stratégique*, No. 132. Institut français des relations internationales.
https://www.ifri.org/sites/default/files/2026-02/ifri_tenenbaum_et_al_miltech_war_ukraine_2026_0.pdf.

Lindh, P. (2022). Military leadership and technology. In which ways do military leaders perceive technology as support or limitation in their leadership? Department of Security, Strategy and Leadership. 1LL053: Basic course III in Leadership under demanding conditions. <https://www.divaportal.org/smash/get/diva2:1632222/FULLTEXT01.pdf>.

McMaster, H. R. (2011). Foreword. In E. Shamir (Ed.), *Transforming command: the pursuit of mission command in the U.S., British and Israeli armies* (need pp). Stanford, California: Stanford University Press

Ministry of Defence of Ukraine. (2024). Rustem Umerov: The DELTA system led to the destruction of enemy equipment valued at more than \$15 billion. <https://mod.gov.ua/en/news/rustem-umerov-the-delta-system-led-to-the-destruction-of-enemy-equipment-valued-at-more-than-15-billion>. (visited 19.07.2026)

NATO. (2023). Russian war against Ukraine: Lessons learned curriculum guide. Defence Education Enhancement Programme.
<https://www.nato.int/content/dam/nato/webready/documents/deep/231208-RusWar-Ukraine-Lessons-Curriculum-Guide-en.pdf>.

NATO Allied Command Transformation. (2025). Federated interoperability. North Atlantic Treaty Organization. <https://www.act.nato.int/activities/federated-interoperability/>.

Peppard, J., Edwards, C., & Lambert, R. (2011). Clarifying the Ambiguous Role of the CIO. *MIS Quarterly Executive*, 10(1), 31–44.

Prince, K.A. (2017). Industrie 4.0 and leadership. *Proceedings of the International Conference on Electronic Business (ICEB)*, 132–139.

avarini, A., Locoro, A., & Martinez, M. (2020). Digital transformation projects maturity and managerial competences: A model and its preliminary assessment. *Lecture Notes in Information Systems and Organisation*, 33, 261–272.

Roman, A. V., van Wart, M., Wang, X. H., Liu, C., Kim, S., & McCarthy, A. (2019). Defining e-leadership as competence in ICTmediated communications: An exploratory assessment. *Public Administration Review*, 79(6), 853–866.

Schwarz Müller, T., Brosi, P., Duman, D., and Welp, I. M. (2018). How does the digital transformation affect organizations? Key themes of change in work design and leadership. *Manage. Revue* 29, 114–138. doi: 10.5771/0935-9915-2018-2-114

Shafiq, M., & Mujawar, S. B. S. (2021). Influence of digitalization on leadership: The case of Sandvik in Sweden. Student thesis, Master degree. University of Gävle, Sweden.

Shoop, J., Lyytinen, K., & Boyatzis, R. E. (2015). The Critical Competencies of Successful

Singh, A., & Hess, T. (2017). How chief digital officers promote the digital transformation of their companies. *MIS Quarterly*, 16(1), 1–17.

Sousa, M. J., & Rocha, A. (2019). Skills for disruptive digital business. *Journal of Business Research*, 94, 257–263.

Tekic, Z., & Koroteev, D. (2019). From disruptively digital to proudly analog: A holistic typology of digital transformation strategies. *Business Horizons*, 62(6), 683–693.

Valentine, E., & Stewart, G. (2015). Enterprise business technology governance: Three competencies to build board digital leadership capability. In *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2015-March, 4513–4522. *Information Systems (ACIS)*, 1–10.

van Wart, M., Roman, A., Wang, X. H., & Liu, C. (2019). Operationalizing the definition of e-leadership: Identifying the elements of e-leadership. *International Review of Administrative Sciences*, 85(1), 80–97.

Институт за перспективни изследвания в отбраната (ИПИО). (2025).

Доклад за резултатите от представително социологическо изследване на тема: „Мотивация на личния състав във формированията от въоръжените сили на Република България“. София: ИПИО, ноември 2025 г. Рег. № СИ-29-10294/25.11.2025 г.

Zornitsa Atanasova

Rakovski National Defence College

Sofia, Bulgaria

email: z.y.atanasova@rndc.bg