https://doi.org/10.52651/sam.j.2026.1

SCIENCE & MILITARY

No 1 | Volume 21 | 2026

SCIENCE & MILITARY

The rationale for publishing this periodical by the Armed Forces Academy of General Milan Rastislav Štefánik is to enable the authors to publish their articles focused on particular scientific issues in the following areas: Military science, Natural Sciences, Engineering and Technology. Original scientific articles will be published twice a year.

Published by: Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic. IČO 37 910 337. Registered No: EV 2061/08. ISSN 1336-8885 (print). ISSN 2453-7632 (online).
DOI: https://doi.org/10.52651/sam.j.2026.1
Printed by: EDIS-Publishing House UNIZA, Univerzitná ul. 8215/1, 010 26 Žilina, Slovak Republic.
Published biannually. The subscription rate for one year is 10,80 €.
The Journal Science & Military is included in following multiple databases: EBSCO. ProQuest Central: PQ Science Journals; PQ Military Collection; PQ Computing; PQ Telecommunications; Illustrata; Forthcoming Technology; Research Database (TRD) full text packages.

Address of the editorial office
Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic
Phone: +421-960-423065 E-mail: redakcia@aos.sk, https://www.aos.sk/katedry/science-military

DOI: https://doi.org/10.52651/sam.j.2026.1

SCIENCE & MILITARY

No 1 | Volume 21 | 2026

Dear readers,

Publishing is currently one of the key performance indicators for individuals and institutions. University faculty members, researchers, and doctoral students are evaluated not only on their teaching or professional work but also on their ability to generate new knowledge and communicate it effectively through scientific publications.

For doctoral students, scientific papers provide a gateway to the international scientific community. Publishing during doctoral studies allows students to receive expert feedback, build professional contacts, and establish their scientific identity. In addition, it is an important prerequisite for the successful completion of their studies, secure postdoctoral jobs, and their participation in international research projects.

For university teachers, publishing is an essential part of their professional growth. Research results are taken into account in habilitation and inauguration proceedings, accreditation of study programmes, and allocation of grants. High-quality publications also enhance the institution's prestige and boost its international competitiveness.

However, publishing alone is not enough. It is equally important that published results resonate within the scientific community. Citations are one of the most significant indicators of scientific impact. They confirm that the published research was relevant, useful, and contributed to the further advancement of knowledge. Several bibliometric studies indicate that articles published under an open-access model generally achieve greater visibility and often a higher number of citations than articles available only through subscription. Open access allows a wider circle of researchers to read, share, and cite scientific papers without restrictions, thereby naturally increasing their impact. Citations, however, cannot be viewed merely as a numerical indicator. They are evidence that the research has entered the scientific discourse and has become part of the ongoing process of creating and expanding knowledge. The importance of citations is also reflected in the evaluation of scientific journals. One of the best-known bibliometric indicators is the Journal Impact Factor (JIF), which represents the average number of citations of articles published in a given journal over a specified period. Although it is an important indicator of a journal's visibility and prestige, it must be interpreted with caution. The impact factor can be a useful tool for navigating the publishing landscape, but it should not be the sole criterion for evaluating the quality of research. When selecting a journal, authors should also consider its academic focus, target readership, the quality of the peer-review process, and the accessibility of published results.

That is why the journal Science & Military recognises its responsibility within the system of scientific communication. Its goal is not only to provide a forum for publishing research findings in the field of military science, but also to promote high-quality scientific publishing, adherence to ethical principles in research, and the open dissemination of knowledge. The journal's ambition is to contribute to the development of professional discourse and to create a platform for the exchange of scientific experience and knowledge between the domestic and international professional communities.

Dear readers, let me briefly introduce the contents of the current issue of the journal:

The first among the peer-reviewed papers in this issue is the article titled ***"Multimodal Biometric Access Control System with Liveness Detection and Speaker Verification"*** *written by Martin Révay, Jakub Kaňuk and Marek Benčík. The presented article deals with an infrastructure free- augmented reality navigation prototype for complex military interiors, combining ARCore tracking, a Visual Positioning System (VPS), and a navigation mesh from a 3D scan to deliver real-time, first person guidance.*

The authors Štefan Gašo and Marián Babjak wrote the paper titled ***„Methods for Mitigating the Impact of Behavioural Profiling and Social Engineering on Mobile Network Users".*** *The article analyses how commercial 4G/5G mobile networks and end-user devices affect the security of military communications and the exposure of personnel through behavioural profiling and social engineering. It describes the specific risks arising from the parallel use of private and service mobile devices by professional soldiers and identifies gaps in current practice within the Slovak Armed Forces.*

Among the papers in this issue, you can find the article written by Marek Benčík, Dominika Dudášiková and Martin Révay titled ***„Tactical Simulator for C2 Training and Real-Time NATO-Compatible Data Distribution".*** *This paper presents a browser-native tactical simulator designed for seamless integration with military command and control (C2) systems. A key part of the simulator is a mathematical formation-control model that preserves the relative geometry of multi-unit groups during movement and directional changes.*

The series of articles is closed with the paper titled ***„Interior Navigation Using Augmented Reality: Design and Implementation of a VPS-Based Prototype"*** *written by Martin Révay, Ivo Kuľha and Marek Benčík. This paper presents the design and implementation of a multimodal biometric access control system intended for environments with increased security requirements. The proposed solution integrates face recognition with liveness detection, role-based access control, and a second authentication factor based on speaker verification with a spoken challenge–response mechanism.*

I hope you will enjoy reading this issue.

Prof. Dipl. Eng. Marcel HARAKAĽ, PhD.
Chairman of the Editorial Board

Reviewers

DOI: https://doi.org/10.52651/sam.a.2026.1.5-13

MULTIMODAL BIOMETRIC ACCESS CONTROL SYSTEM WITH LIVENESS DETECTION AND SPEAKER VERIFICATION

Martin RÉVAY, Jakub KAŇUK, Marek BENČÍK

Abstract: This paper presents the design and implementation ofv a multimodal biometric access control system intended for environments with increased security requirements. The proposed solution integrates face recognition with liveness detection, role-based access control, and a second authentication factor based on speaker verification with a spoken challenge–response mechanism. The system is implemented as a client–server web application using standard camera and microphone hardware, while all biometric processing is performed locally within on-premise infrastructure. The contribution of the paper lies in the practical integration of visual and acoustic biometric modalities into a unified authentication workflow and in the discussion of operational constraints such as latency, resistance to presentation attacks, and data protection.

Keywords: Biometric authentication; face recognition; liveness detection; speaker verification; multimodal authentication; access control.

1 INTRODUCTION

Modern access control systems deployed in environments with elevated security requirements must ensure not only reliable user identification, but also verification of the user's physical presence and authorization to enter a protected area. Traditional authentication mechanisms based on knowledge (passwords) or possession (access cards) are vulnerable to loss, sharing, or misuse, which has motivated the increasing adoption of biometric technologies in institutional security systems.

Face recognition has become one of the most widely used biometric methods in contactless authentication due to its natural mode of interaction and compatibility with commodity imaging hardware. However, its practical deployment faces several challenges, including sensitivity to acquisition conditions, the possibility of false matches, and susceptibility to presentation attacks such as printed photographs or digital display spoofing. For this reason, face recognition alone is generally insufficient for security-critical applications.

One effective strategy to improve system robustness is the use of multimodal authentication, which combines multiple independent biometric traits or authentication factors. The inclusion of liveness detection helps mitigate common spoofing attacks, while a second factor, such as speaker verification, further increases confidence in the authentication decision. Equally important is the separation of identity recognition from authorization logic, ensuring that successful biometric identification does not implicitly guarantee access privileges.

The objective of this paper is to present the design and implementation of a multimodal biometric access control system that integrates visual and acoustic biometric modalities into a unified authentication workflow. The proposed solution is implemented as a client–server application with fully local biometric processing, with particular emphasis on practical deployment, operational constraints, and compliance with security and privacy requirements in on-premise environments.

2 RELATED WORKS

This section reviews relevant research related to biometric authentication in access control systems, with a particular focus on multimodal approaches, face recognition with liveness detection, and speaker verification as a second authentication factor. The reviewed literature aims to summarize the current state of the art, identify prevailing research directions, and highlight limitations of existing solutions that motivated the design choices of the system presented in this paper.

2.1 Biometric Authentication and Multimodal Approaches

Biometric authentication has become an important alternative to traditional access control mechanisms, particularly in security-critical applications. While unimodal biometric systems based on a single trait can achieve high accuracy under controlled conditions, their robustness is limited in real-world environments due to noise, acquisition variability, and deliberate spoofing attempts [1]. As a result, multimodal authentication approaches combining multiple independent biometric traits have been widely investigated to improve system reliability and reduce false acceptance and rejection rates [2], [3].

Multimodal systems are especially attractive in high-security scenarios, where higher confidence in identity verification is required. Existing studies explore various fusion strategies at the feature, score,

or decision level [4]. However, many of these works primarily focus on recognition performance and do not sufficiently address practical deployment aspects such as system architecture, latency, or privacy preservation.

Access-control mechanisms have traditionally been addressed within broader system and network-security frameworks, emphasizing explicit separation between authentication, authorization, and policy enforcement layers [15]. These principles are directly applicable to biometric access systems, where successful identity recognition alone must not imply access permission.

Multimodal biometric authentication extends this concept by combining heterogeneous evidence sources to increase robustness against failures and attacks that commonly affect unimodal solutions.

2.2 Face Recognition and Presentation Attack Detection

Face recognition is one of the most widely deployed biometric technologies in contactless authentication systems. Significant advances have been achieved through deep learning-based face representations, which enable highly discriminative facial embeddings [5]. Nevertheless, face recognition systems are vulnerable to presentation attacks, including printed photos, replayed videos, and three-dimensional masks.

To mitigate these threats, presentation attack detection (PAD), also referred to as liveness detection, has become a crucial component of modern face recognition systems. Survey studies describe a wide range of approaches, from hand-crafted texture analysis to deep learning-based spatio-temporal models [6], [7]. Despite these advances, generalization to unseen attacks and deployment under constrained hardware conditions remain open challenges.

Real-world image-based recognition systems must operate under varying illumination, noise, and acquisition conditions. Practical object-recognition systems demonstrate that reliable decision-making requires robust feature extraction combined with lightweight inference pipelines [16]. Similar constraints apply to face-based access-control terminals, where presentation-attack detection exploits visual artifacts instead of idealized input data.

2.3 Speaker Verification as a Second Authentication Factor

Speaker verification is a behavioural biometric modality frequently used as an additional authentication factor. Modern systems based on deep speaker embeddings achieve strong performance under controlled conditions [8]. However, real-world performance is affected by environmental noise, microphone quality, and mismatches between enrolment and test recordings [9].

To enhance security, challenge–response mechanisms are often employed, combining speaker verification with speech content verification to reduce vulnerability to replay attacks [10]. Several studies recommend the integration of speaker verification as a second factor in multimodal systems, particularly for access control applications requiring contactless and user-friendly interaction [11].

Limitations of single-factor authentication mechanisms have been demonstrated in the context of interface-level and input-device attacks [17]. These findings motivate the adoption of biometric and multi-factor authentication schemes, where speaker verification combined with challenge–response mechanisms reduce reliance on transferable credentials and increases resistance to replay attacks.

2.4 Summary and Research Gap

While prior work addressed access control at the network level [15], explored real-time visual recognition under operational constraints [16], and analysed vulnerabilities of single-factor authentication [17], limited attention has been paid to the practical integration of multimodal biometrics, liveness detection, and authorization logic within a single deployable access-control terminal. This paper addresses this gap by presenting an on-premise multimodal biometric system that integrates visual and acoustic authentication with explicit access-level enforcement. In contrast to many existing works that address only a single biometric modality or focus on algorithmic performance, the proposed system emphasizes system-level integration and operational deployment constraints.

3 SYSTEM DESIGN AND METHODOLOGY

The objective of the system design was to develop a multimodal access control solution that combines multiple biometric mechanisms while maintaining practical deployability and strict requirements for local processing of sensitive data. The proposed design follows a system-level perspective with a clear separation between identity recognition, access authorization, and multi-factor authentication. This separation enables flexible security policy enforcement and reduces the risk of unauthorized access in real-world operational environments.

3.1 Design Requirements and Principles

A fundamental design principle of the proposed system is the adoption of **a multimodal authentication** strategy that combines visual and acoustic biometric modalities. Face recognition was selected as the primary identification modality

due to its contactless nature, intuitive user interaction, and compatibility with commodity imaging hardware. Speaker verification was incorporated as a secondary authentication factor to address increased security requirements and strengthen overall decision confidence.

An important design decision was the inclusion of **liveness detection** directly within the identification stage. This component acts as a protective layer against common presentation attacks and ensures that subsequent authentication steps are executed only for a physically present subject. By integrating liveness verification as a prerequisite rather than a post-processing step, the system follows a fail-fast design strategy that reduces unnecessary computational load during invalid or malicious interactions.

Another key requirement was the implementation of **fully on-premise biometric processing**, avoiding reliance on external cloud-based services. This decision reflects deployment constraints in institutional and security-sensitive environments, where off-site transmission of biometric data is unacceptable from both security and privacy perspectives.

The selected biometric components were implemented using lightweight embedding-based models suitable for CPU-based inference, with all models deployed locally and initialized at server startup to minimize latency.

3.2 System Architecture

The overall architecture of the proposed system is illustrated in Fig. 1. The solution is implemented as a client–server web application, where the client component is responsible for user interaction and audiovisual data acquisition, and the server performs biometric processing and decision logic.

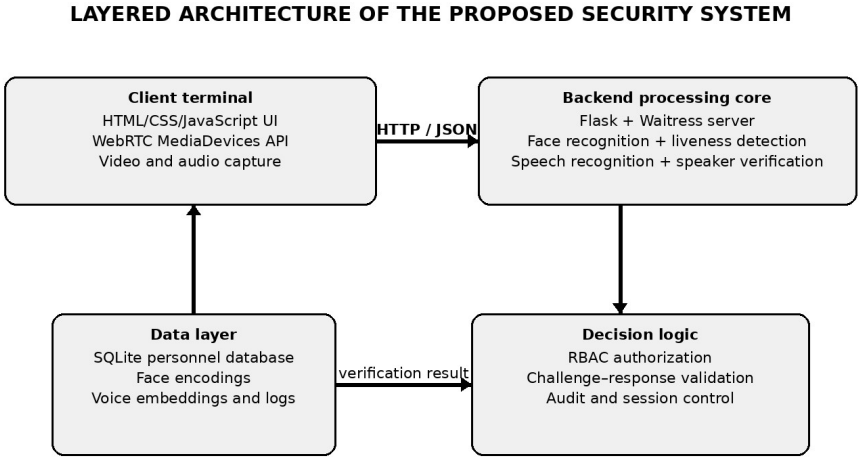

Fig. 1 Layered architecture of the multimodal biometric access control system
Source: author.

The architecture follows a modular layered design, separating the client interface, application logic, biometric inference components, and persistent data storage. This separation improves maintainability, allows independent updates of biometric models, and supports secure handling of sensitive data.

The relationships between personnel records, biometric templates, and authorization attributes are captured in the system data model shown in Fig. 2. The model explicitly separates identity information from access privileges, ensuring that successful biometric identification does not implicitly grant authorization.

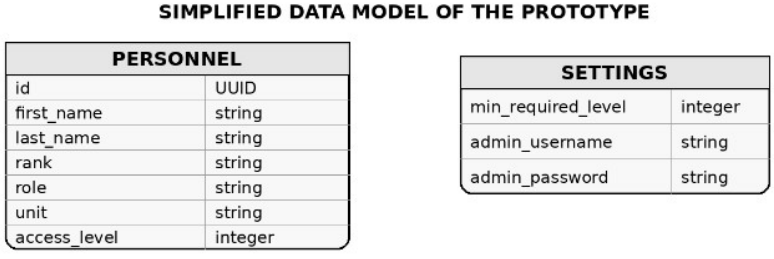

Fig. 2 Simplified data model illustrating the separation of identification and authorization data
Source: author.

3.3 Authentication Workflow

The sequential execution of the multimodal authentication process is summarized in Fig. 3. The workflow starts with image acquisition and face recognition, combined with parallel liveness evaluation of the captured facial sample. The system applies a fail-fast strategy, terminating the process immediately if no live face is detected.

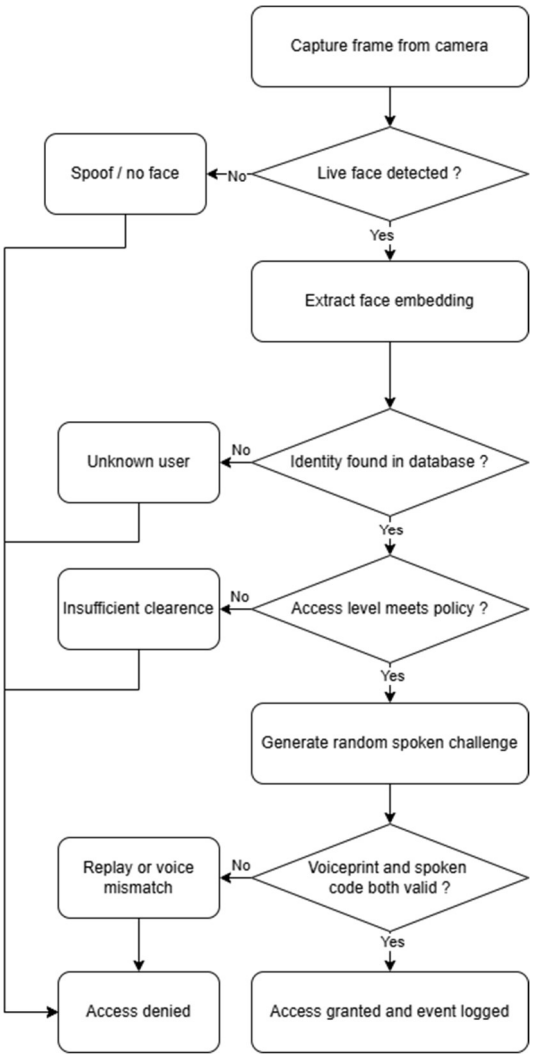

Fig. 2 Decision workflow of the multimodal authentication process
Source: author.

After successful visual identification, the system evaluates the user's authorization level against the required security threshold. Only authorized users proceed to the second authentication phase, in which a dynamically generated spoken challenge is issued.

The final access decision is based on the combined outcome of visual recognition, liveness verification, authorization validation, and acoustic authentication.

4 SYSTEM IMPLEMENTATION

This section describes the technical realization of the proposed multimodal biometric access control system. The implementation follows the architectural principles introduced in the previous section and adheres to the authentication workflow illustrated in Fig. 3.

4.1 Client-Side Implementation

The client component is implemented as a browser-based application responsible for user interaction and audiovisual data acquisition using standard device APIs. This approach enables simple deployment on common terminal devices without requiring specialized hardware or proprietary software.

The client manages a state-driven authentication flow, transitioning between idle, visual capture, second-factor authentication, and final decision states in accordance with the workflow shown in Fig. 3. Image frames are sampled discretely rather than streamed continuously to minimize server load and ensure real-time responsiveness.

4.2 Server-Side Processing and Application Logic

The server component constitutes the computational core of the system and exposes endpoints corresponding to individual authentication phases. It handles data decoding, session management, biometric inference, and access control decisions.

All computationally intensive models are initialized at server startup and retained in memory to reduce inference latency. The server maintains transient authentication state between visual and acoustic phases, ensuring continuity of the workflow depicted in Fig. 3.

4.3 Visual Biometric Processing Pipeline

The visual pipeline begins with decoding incoming image data and performing face localization. A facial embedding is extracted and compared against stored reference templates, while liveness detection is performed in parallel to mitigate presentation attacks.

A fail-fast strategy is applied: if liveness verification fails, the authentication process is immediately terminated without executing further steps defined in the workflow (Fig. 3), improving both computational efficiency and security.

Face recognition is based on fixed-length facial embeddings extracted from detected face regions and compared using a distance-based similarity metric, while liveness detection relies on a compact classification model optimized for real-time execution.

4.4 Acoustic Pipeline and Second-Factor Authentication

After successful visual identification and authorization, the system generates a random spoken challenge. The client records the response, which is normalized and analysed on the server. Two parallel checks are performed: verification of the spoken challenge content and speaker verification based on voice embeddings.

Access is granted only if all stages of the multimodal process illustrated in Fig. 3 are successfully completed. Speaker verification employs embedding-based voice representations combined with speech-content verification to enforce the challenge–response constraint.

4.5 Data Storage and Security Measures

The system adopts a hybrid data storage strategy, separating structured user records from biometric templates. Raw biometric data are not stored beyond the processing phase. Authentication attempts are logged for audit purposes, while user-facing feedback remains intentionally limited to prevent information leakage.

5 RESULTS AND DISCUSSION

This section presents the functional evaluation of the implemented prototype and discusses its behaviour under realistic deployment conditions. The assessment focuses on authentication flow, user interaction, system responses to abnormal situations, and identified limitations rather than quantitative optimization of biometric thresholds. The presented figures illustrate typical system states observed during functional testing and are intended to demonstrate decision logic and user interaction rather than quantitative performance metrics.

5.1 Authentication Flow and User Interaction

In its initial state, the terminal operates in standby mode while continuously monitoring the area in front of the camera to detect user presence. Once a face is detected, the system initiates the visual authentication stage, which includes face localization, biometric feature extraction, and parallel liveness verification of the presented facial sample.

User interaction is designed as a fully contactless process, in which the system automatically transitions between authentication states without requiring manual input. Visual state indicators provide clear feedback on the progress of authentication while intentionally concealing internal decision thresholds and confidence values.

Liveness detection is an integral part of the visual authentication stage and aims to identify non-live facial presentations. Fig. 4 illustrates a practical example of a 2D presentation attack conducted using a facial photograph displayed on a mobile device positioned in front of the terminal camera. In this scenario, the system correctly classifies the displayed face as a non-live presentation, identifies the spoofing attempt, and does not associate the captured subject with a recognized identity.

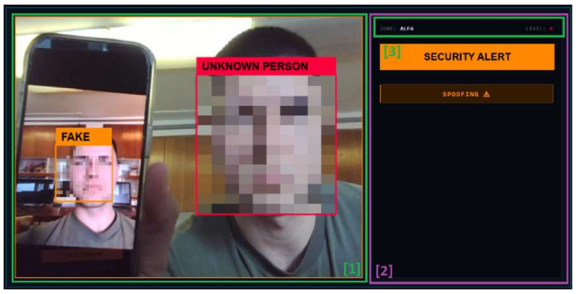

Fig. 3 Detection of a 2D presentation attack
Source: author.

Upon detecting such anomalous behaviour, the system immediately terminates the authentication process and transitions into a protective state, which is indicated by a security alert in the user interface. This response prevents further processing of the input data and demonstrates the system's ability to mitigate common spoofing attempts without relying on specialized sensors or additional hardware.

After successful liveness verification and visual identification, the system automatically transitions to the second authentication factor. This stage is activated only if the identified user also satisfies the authorization requirements defined for the protected zone. The user interface in this state is illustrated in Fig. 5.

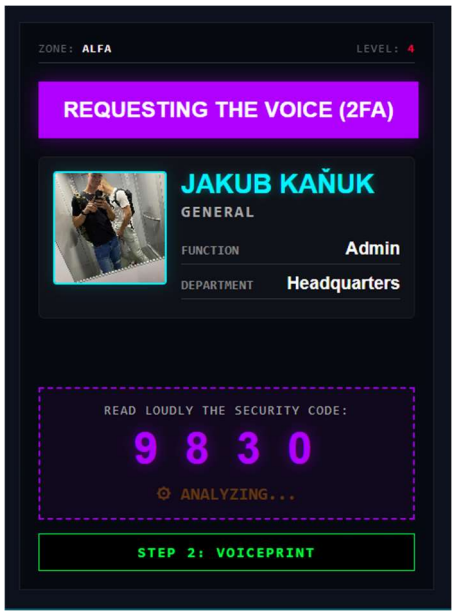

Fig. 4 Second authentication phase – spoken challenge (2FA)
Source: author.

The interface explicitly indicates the transition to voice-based verification and presents a dynamically generated numerical challenge that the user is required to speak aloud. At the same time, the system displays the current processing status and the next step of the authentication sequence. Displayed identity and organizational attributes serve to provide contextual confirmation and do not influence the biometric decision process itself.

The inclusion of a second authentication factor significantly enhances overall system security by coupling biometric speaker verification with a dynamic challenge bound to real-time user interaction. This approach effectively reduces the risk of replay attacks and prevents misuse of previously captured audio samples.

After successful verification of the spoken challenge and speaker identity, the authentication process transitions into its final decision stage. If all biometric modalities and authorization conditions are satisfied, the system explicitly confirms access approval, as illustrated in Fig. 6.

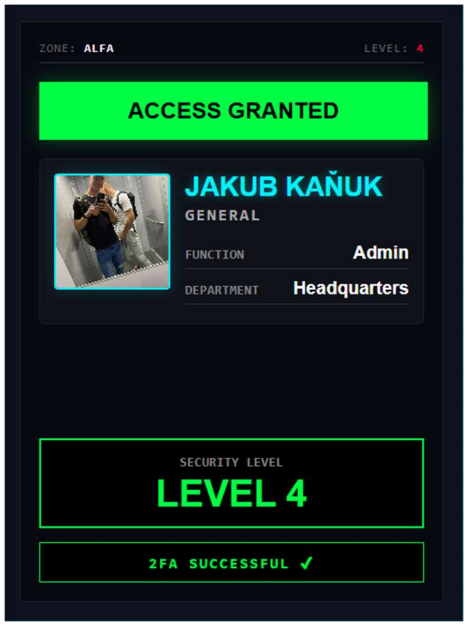

Fig. 5 Successful authentication – access granted
Source: author.

In this state, the user interface provides clear and unambiguous feedback without requiring further user interaction. The displayed security level and confirmation of successful second-factor authentication indicate that the complete authentication chain has been executed without detecting anomalies.

This terminal state represents the end of the authentication workflow and corresponds to the point at which downstream access-control actions may be triggered, such as unlocking a physical entry point or granting access to a protected system.

5.2 Resistance to Presentation Attacks

The liveness detection mechanism employed in the system relies on the analysis of visual artifacts that emerge during non-live face presentations. These artifacts are a physical consequence of light interaction with printed media or digital display devices and differ significantly from the visual characteristics of a live human face.

Fig. 7 provides a systematic comparison of the two most common types of 2D presentation attacks: printed photographs and digital displays. Printed images typically exhibit specular reflections, uneven illumination, and saturated regions, while screen-based presentations generate moiré interference patterns, aliasing effects, and pixel-grid periodicity. Such artifacts are absent in images captured from live facial presentations.

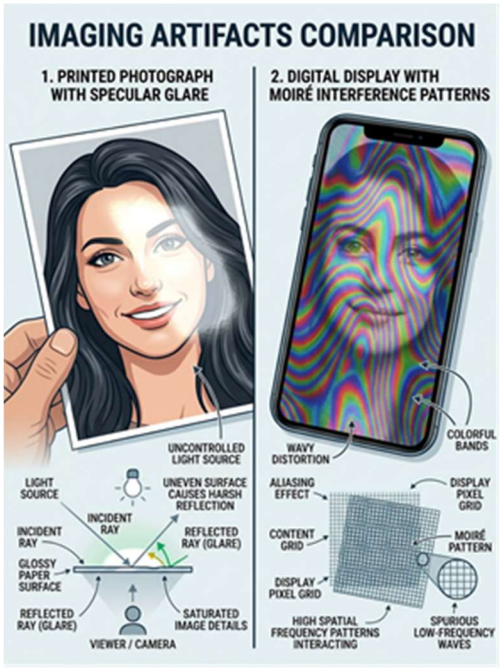

Fig. 6 Visual artifacts in 2D presentation attacks
Source: author.

These visual characteristics form the basis of the liveness detection decision process and enable early identification of presentation attacks, as demonstrated in the practical spoofing scenario shown in Fig. 4. Although the system is not designed to counter advanced three-dimensional mask attacks, it demonstrates sufficient robustness against the most prevalent 2D spoofing techniques encountered in real-world access control scenarios.

5.3 Access Control Enforcement and Failure States

The system is designed to strictly separate biometric identification from the final access decision. Even when visual identification and authorization requirements are satisfied, access may still be denied if the second authentication factor

fails. Fig. 8 illustrates a scenario in which the user fails the spoken challenge during the second authentication stage. Although the system successfully identifies the user and confirms the required security level, an incorrect spoken code results in immediate access denial. In this state, the user interface provides clear feedback while intentionally concealing internal decision details.

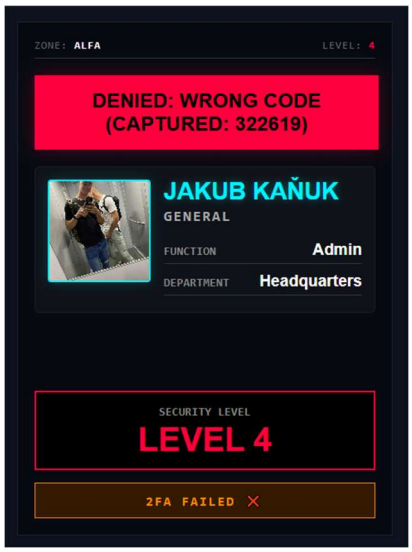

Fig. 7 Failed speaker verification – access denied
Source: author.

This behaviour reduces information leakage risks and ensures robust system operation in situations caused by user error, adverse acoustic conditions, or attempted replay attacks.

In addition to individual authentication failures, the system evaluates the overall security context of the protected area. Access is denied whenever the authentication chain is not successfully completed or when the resulting authentication level does not meet the required security threshold.

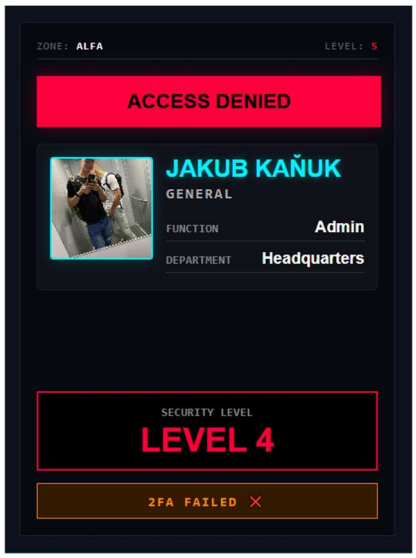

Fig. 8 Access denied due to failed authentication
Source: author.

Fig. 9 illustrates a global access denial state in which the system explicitly reports failed authentication without disclosing detailed internal causes. This design prevents leakage of sensitive information about decision logic and reduces the feasibility of adaptive attacks based on system feedback.

In this state, the user interface provides a clear and consistent decision outcome while maintaining uniform feedback across different failure scenarios, including user error, acoustic disturbances, or detected anomalies.

6 CONCLUSION AND FUTURE WORK

This paper presented the design and implementation of a multimodal biometric access control system that integrates face recognition, liveness detection, speaker verification, and role-based access control. The proposed solution was developed with a strong emphasis on on-premise biometric processing, architectural modularity, and practical applicability in environments with elevated security requirements.

The implemented prototype demonstrated the ability to execute a complete multi-factor authentication workflow with intuitive contactless interaction and clear user feedback. Functional evaluation showed that combining visual and acoustic biometric modalities with liveness detection improves system robustness against common presentation and replay attacks compared to unimodal approaches. Moreover, the explicit separation of identification, authentication, and authorization enables flexible access control policies without implicitly granting privileges based solely on biometric similarity.

At the same time, several limitations were identified. The performance of face recognition and liveness detection remains sensitive to image quality, lighting conditions, and camera characteristics, while speaker verification accuracy is affected by acoustic noise, microphone quality, and enrollment conditions. As the primary focus of this work was system integration and operational feasibility, the prototype was not subjected to large-scale statistical evaluation of biometric error rates suchas FAR and FRR.

Future work may therefore focus on extended experimental validation using a larger and more diverse user population, comprehensive performance evaluation under varying environmental conditions, and the integration of more advanced liveness detection techniques with partial resistance to three-dimensional presentation attacks. Additional development directions include tighter coupling with physical access control hardware, enhanced audit and monitoring features, and further refinement of administrative workflows.

In conclusion, the presented system provides a practical and extensible foundation for layered

biometric access control solutions in closed institutional environments where security, privacy preservation, and independence from cloud services are of primary importance.

Acknowledgement

The paper has been supported by the outputs of the research project "NI4200642 – Complex scientific research and testing laboratory for command and control systems (hC2)" funded by the Ministry of Defence of the Slovak Republic through the inter – ministerial sub – program 06E0I – Research and development in support of state defence.

References

[1] SZELISKI, R. *Computer Vision: Algorithms and Applications.* 2nd ed. Cham: Springer, 2022. Available at: https://doi.org/10.1007/978-3-030-34372-9

[2] SCHROFF, F., KALENICHENKO, D. and PHILBIN, J. "FaceNet: A unified embedding for face recognition and clustering," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2015, pp. 815–823. Available at: https://doi.org/10.1109/CVPR.2015.7298682

[3] JAIN, A.; ROSS, A. and PRABHAKAR, S. An Introduction to Biometric Recognition. In *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004. Available at: https://doi.org/10.1109/TCSVT.2003.818349

[4] ROSS, A. and JAIN, A. Multimodal biometrics: An overview. In *Proc. 12th European Signal Processing Conference (EUSIPCO)*, 2004, pp. 1221–1224.

[5] YU, Z. et al. "Deep learning for face anti-spoofing: A survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2021. Available at: https://doi.org/10.1109/TPAMI.2022.3215850

[6] SHARMA, D. and SELWAL, A. A survey on face presentation attack detection mechanisms: Hitherto and future perspectives," *Multimedia Systems*, vol. 29, pp. 1527–1577, 2023. Available at: https://doi.org/10.1007/s00530-023-01070-5

[7] HUANG, P. K. et al. A survey on deep learning-based face anti-spoofing. *APSIPA Transactions on Signal and Information Processing*, 2024. Available at: https://doi.org/10.1561/116.20240053

[8] LIU, X. *Advances in Deep Speaker Verification: A Study on Robustness, Portability, and Security.* PhD thesis, University of Eastern Finland, 2023.

[9] BAALI, M. et al. SVeritas: A benchmark for robust speaker verification under diverse conditions. In *arXiv preprint*, 2025. Available at: https://doi.org/10.18653/v1/2025.findings-emnlp.516

[10] ALALIYAT, S et al. Speaker verification using machine learning for door access control systems. In *Advances in Intelligent Systems and Computing.* Springer, 2021. Available at: https://doi.org/10.1007/978-3-030-76346-6_61

[11] HMIMOU, Y. et al. Context-aware decision fusion for multimodal access control under contradictory biometric evidence. In *Computers*, vol. 15, no. 4, 2026. Available at: https://doi.org/10.3390/computers15040208

[12] RADFORD, A. et al. Robust speech recognition via large-scale weak supervision. In *Proc. ICML*, 2023.

[13] OpenCV. OpenCV documentation, 2026. [Online]. Available: https://docs.opencv.org

[14] ONNX Runtime. ONNX Runtime documentation 2026. [Online]. Available: https://onnxruntime.ai/docs/

[15] BARATH, J.; DEDERA, Ľ. and HARAKAĽ, M. Network Access Control Technologies for Securing Internal Networks. In *Science & Military*, 2007, vol. 2, no. 2. ISSN 1336-8885.

[16] ŠTEFKA, P. et al. Object Recognition System for the Spinbotics Robotic Arm. [Online]. In *Science & Military,* 2024. Vol. 19, No. 1, pp. 39-44. ISSN 2453-7632. Available at: https://doi.org/10.52651/sam.a.2024.1.39-44

[17] POTOCKÝ, S. and ŠTULRAJTER, J. The Human Interface Device (HID) Attack on Android Lock Screen Non-Biometric Protections. [Online]. *Science & Military* 2022, Vol. 17, No.1, pp. 29-36. ISSN 2453-7632. Available at: https://doi.org/10.52651/sam.a.2022.1.29-36.

Maj Dipl. Eng. Martin **RÉVAY**, PhD.
Armed Forces Academy of General M. R. Štefánik
Department of Informatics
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: martin.revay@aos.sk

Maj Dipl. Eng. Marek **BENČÍK**, PhD.
Armed Forces Academy of General M. R. Štefánik
Department of Informatics
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: marek.bencik@aos.sk

Pte 1st class Bc. Jakub **KAŇUK**
Armed Forces Academy of General M. R. Štefánik
Department of Informatics
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: jakub.kanuk@aos.sk

Martin RÉVAY was born in Močenok, Slovakia in 1987. He received his Eng. (MSc.) at the Armed Forces Academy in Liptovský Mikuláš in 2014. He received his PhD. Degree in Military communication and information systems in 2023. His research interests are focused on command and control systems, virtual and augmented reality. He is currently working as an assistant professor at the Department od Informatics, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš.

Marek BENČÍK was born in Dolný Kubín, Slovakia in 1988. He received his Eng. (MSc.) at the Armed Forces Academy in Liptovský Mikuláš in 2014. He received his PhD. Degree in Military communication and information systems in 2022. He specializes in programming languages and their applications in command and control systems, as well as in modeling and simulation systems. He also focuses on the transfer and processing of sensor data into command and control systems and their proper representation within these systems. He is currently working as an assistant professor at the Department od Informatics, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš.

Jakub KAŇUK was born in Kežmarok, Slovakia in 2000. He received his Bc. at the Armed Forces Academy in Liptovský Mikuláš in 2024. He is a student at the Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš. Within the Department of Informatics, his academic focus is centered on the field of artificial intelligence and its practical applications in modern systems.

DOI: https://doi.org/10.52651/sam.a.2026.1.14-23

METHODS FOR MITIGATING THE IMPACT OF BEHAVIOURAL PROFILING AND SOCIAL ENGINEERING ON MOBILE NETWORK USERS

Štefan GAŠO, Marián BABJAK

Abstract: The article analyses how commercial 4G/5G mobile networks and end-user devices affect the security of military communications and the exposure of personnel through behavioural profiling and social engineering. It describes the specific risks arising from the parallel use of private and service mobile devices by professional soldiers and identifies gaps in current practice within the Slovak Armed Forces. The paper combines an overview of relevant 5G security mechanisms (zero trust, encrypted identifiers, end to end encryption, VPN, eSIM) with an empirical questionnaire survey among 53 professional soldiers to map their habits and security awareness when using mobile devices for private and work purposes. On this basis, it proposes a three pillar model of mitigation measures – user security awareness, hardware rules and software rules – formulated as standard operating procedures for secure and partially covert communication in mobile networks. The aim is to reduce the impact of behavioural profiling and social engineering on military personnel, limit the digital footprint linking private and professional activities, and support the safe integration of commercial mobile technologies into military command and control processes.

Keywords: 5G security; mobile networks; secure communication; military communications; cyber security; behavioural profiling; social engineering; mobile device security; operational security; standard operating procedures.

1 INTRODUCTION

History has shown that military conflicts demand the constant gathering of accurate and urgent information to support the decision-making process of commanders. The rapid transmission of accurate information is key to achieving information superiority on the battlefield. The digital transformation of the battlefield and the integration of artificial intelligence into military conflicts has led to a sharp increase in the need to transmit large volumes of data in near real time. It is clear that, when it comes to planning military operations and campaigns, there are increasing opportunities to use mobile communication networks, with all their advantages and disadvantages. There are many examples from open sources of how the fighting parties in the Russia-Ukraine war are using 3G, 4G, and 5G mobile networks. Mobile end devices are standard equipment for every soldier. An individual on the battlefield becomes a digital sensor. This sensor can obtain valuable information necessary for the decision-making process of commanders and staff. Terminal equipment, on the other hand, poses a clear risk to soldiers. It can cause their own deaths and those of their colleagues, and reveal sensitive information about their own troops to the enemy.

The Slovak Armed Forces currently do not have the analysis of the mobile communications space, the planned deployment of capacities and capabilities in this space, and their subsequent purposeful use during operations. The development of these planning capabilities also raises questions about the secure and covert communication of users from the ranks of the Slovak Armed Forces. It is essential that the confidentiality, integrity and availability of transmitted information is maintained. This is a fundamental requirement for the use of commercial mobile networks and their capabilities.

Digital communication is undoubtedly the primary form of communication used by modern armies on the battlefields of the 21st century to ensure command and control during military operations. Public mobile digital communication, as part of cyberspace, is undoubtedly becoming a key element in military communication. There is indisputable evidence of the integration of commercial architecture into the military communications structure to support both conventional and unconventional forms of communication. Military analyses of the use of mobile communications in emerging 5G systems to support military activities are also nothing new.

The development of public mobile radio communication systems during modern conflicts has fundamentally impacted military communication methods. However, 5G technology has exposed several vulnerabilities in public environments, and individual countries are working to address these issues logistically and technically. We can tell you authoritatively that there are currently only a limited number of 5G technology suppliers worldwide. The right choice of suppliers is key to reducing the risk of hacker attacks in the country or technology supply disruptions due to possible future sanctions. The EU and NATO countries, where there are already several restrictions on the supply of Chinese HUAWEI technologies, are a clear example of this. These countries are facing new challenges in building secure and stable high-speed radio communication systems [1], [2].

2 MITIGATING METHODS FOR USERS

As we set out in the introduction, mobile technologies are already having a decisive impact on military conflicts, shaping the planning process at all levels of command and control. Military planners must monitor commercial communication technologies in ongoing conflicts and implement them. Every action is met with a counteraction. In the age of artificial intelligence and superfast computers, these time blocks are radically shortened. This creates great knowledge pressure on personnel planning communication capabilities during military conflicts. Those involved in the planning process for modern conflicts must analyse the resources deployed within a multi-domain approach. It is an indisputable fact that communication technologies affect almost every area of military art today. The Slovak Armed Forces must take action to address the significant security gap that arises from their current lack of a comprehensive approach to analysing the use of mobile technologies.

Mobile 5G technologies are now a vital part of the battlefield, offering a more secure communications environment that is more resistant to hacker attacks thanks to compliance with standards set for 5G technologies. The zero-trust principle eliminates any trust between individual devices in the network and requires all transmissions between devices to be verified and encrypted. Analysis of known hacker attacks shows that human error is the most common cause of security breaches. It is vital that operations are planned with educated and prepared personnel and that these technologies are used with sufficiently trained personnel, in order to ensure the proper and effective use of 5G technology for the benefit of the Slovak Armed Forces. 5G devices must be used at the individual level in a conflict or military operation. Security rules must be established for their use to prevent unnecessary detection by the enemy.

In the current 4G networks, the security of end devices and networks focuses on four aspects: authentication, integrity, availability, and confidentiality. After initial verification, a device in the network is permanently trustworthy. However, it is clear that end-user privacy requirements are not sufficiently taken into account from a network architecture perspective. It is clear that, from a military point of view, the use of such networks is possible. However, there is no doubt that it carries greater risks of sensitive data being obtained by the enemy. 5G technologies are much more focused on privacy protection and bring new aspects such as traceability, anonymity, disconnectability, and pseudonymity (the use of identifiers that replace the actual identity of the device). 4G technologies rely on centralised trust in the network. 5G technologies do not have this shortcoming. They strictly protect all ongoing communications between individual devices with various levels of encryption and authentication. This significantly increases the protection of the end device against data acquisition by third parties. 5G technology significantly mitigates the enemy's ability to obtain data using IMSI catchers, wiretapping, or Man-In-The-Middle (MitM) attacks. 5G technology is clearly the solution for military use, offering a number of advantages that reduce the enemy's ability to obtain data about our combat activities. However, the enemy will still have access to social engineering techniques, behavioural profiling, and data mining methods. We can assure you that even these techniques and methods can be effectively suppressed simply by using user privacy settings in 5G networks [3].

According to the information provided in the publication [4] some mobile applications and devices collect large amounts of data without the user's consent or knowledge, which is contrary to the developers' privacy policies. Despite these commonly known security issues, users believe that they have little or no responsibility for protecting organizational data stored on assigned mobile devices [4]. The above information was measured among employees of private corporations. We selected a sample of 53 professional soldiers from the ranks of enlisted personnel, non-commissioned officers, and officers, represented in age categories from 21 to 49 years. This was to verify the above information among military personnel. We used questionnaires to survey this sample to determine the actual state of knowledge among members of the armed forces. The research aimed to identify habits in the use of mobile devices for private and work purposes and to identify weaknesses.

Gained information (Fig. 1) confirmed the assumptions that ordinary users do not pay suffic ient attention to information security on end devices and are prone to leaving excessive digital footprints in cyberspace as well as to the pitfalls of social engineering. In the verified sample, up to 83 % of users either used a work mobile phone for work purposes or used a private mobile phone to communicate with family while performing work tasks in domestic and foreign crisis management. Almost 20% of users admitted to also using work devices for private purposes. While 88 % of users said they thought it was important to separate work and private communication, only 11 % said they actually did so.

Only around a third of users knew about behavioural profiling in cyberspace, social engineering, and the associated pitfalls of leaving personal data on the internet. Although almost two-thirds of respondents said they knew about secure ways to communicate via mobile devices, only 7 % used VPN services, and almost 40 % were unfamiliar with end-to-end encryption applications.

Although two-thirds of verified users said they were aware of the risks of not turning off Global

Positioning System (GPS), Bluetooth, and Wi-Fi, only around 55 % physically turn off these interfaces when not in use. Furthermore, as many as 40 % of respondents do not use SIM card security in the form of a code. Almost 60 % of users protect their phones with only a 4-digit numeric code or pattern, methods that are now considered completely inadequate. Four percent of users say they do not use any mobile device security.

Only one-fifth consciously encrypt their mobile device's disk, and only 15 % turn off their devices for at least 30 minutes at least once a week to allow unwanted processes to terminate and new updates to run correctly.

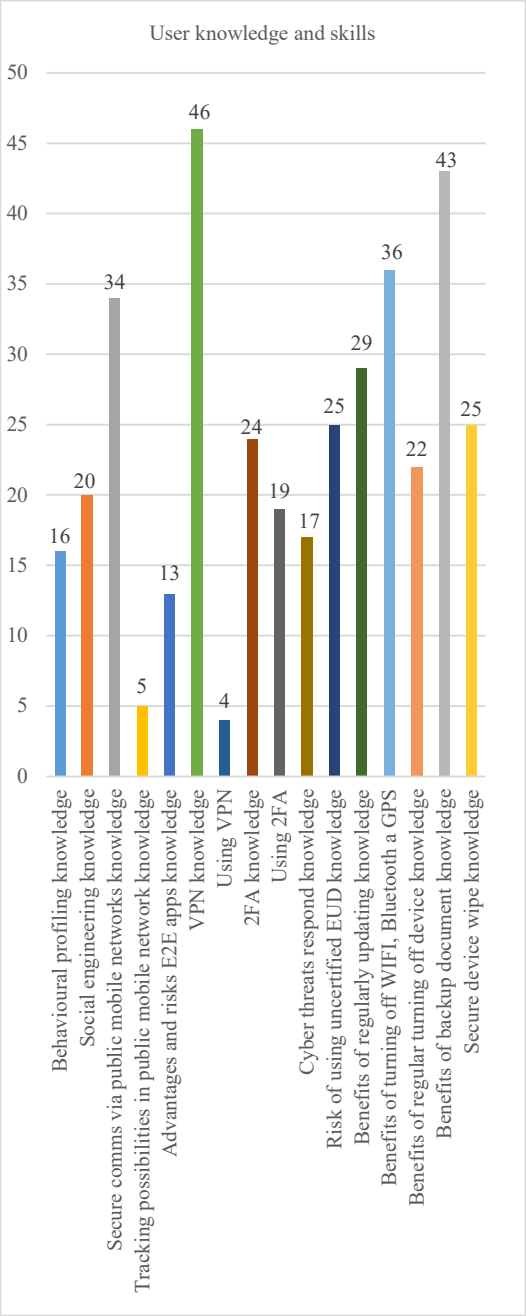

Fig. 1 User knowledge and skills – before using SOP
Source: author.

Although users are familiar with cyber threats such as malware, ransomware, and spyware, they are completely unaware of threats such as vishing and Man-in-the-Middle attacks (MitM). In fact, fewer than a quarter of respondents know how to respond to individual threats, and just 2 % are familiar with measures against vishing and MitM.

The data clearly shows that using GSM networks during combat operations would lead to the unauthorized disclosure of significant information about the armed forces' current or planned military activities by professional soldiers.

Based on results we proposed ways to increase the safe use of these devices and awareness of threats in cyberspace. We summarized these methods in the proposed standard operating procedures. After the SOPs were made available, awareness levels in the required areas arise (Fig. 2). Almost 70 % of respondents were able to recognize the dangers associated with leaving a digital footprint in cyberspace. Up to 90 % of users said they knew how to communicate safely online.

Almost half changed their attitude towards using VPN services, confirming their important role in creating a secure communication environment. Most users were already familiar with end-to-end encryption applications, and 58 % said they had started using these applications for private communications. Before studying the operating procedures, this figure was only 28 %. All users stated that they were aware of the risks of not turning off GPS, Bluetooth, and Wi-Fi. Up to 70 % of them began actively turning off these services when not in use.

Unfortunately, the number of users who did not secure their SIM cards with codes, securing their mobile devices only with 4-digit codes or patterns, or not securing their devices at all, remained almost unchanged.

The proportion of users who began to encrypt the disk on their end device consciously rose to 30 %. Interestingly, although 98% of users confirmed the importance of updating their devices, only 45 % were willing to turn their devices off for at least 30 minutes once a week. Users could clearly identify cyber threats connect with social engineering and behavioural profiling. Over 75 % said they could respond to individual threats within the specified scope of the SOP.

Mitigation of deficiencies in the use of end devices by users/professional soldiers can be ensured through training and education of personnel, focusing on simple security rules for the use of end devices. By educating staff about cyber threats, we will create a stable first pillar necessary for comprehensive protection of end devices. By setting standards for the use of mobile devices, we will create clear rules for users on how to access the hardware and software parts of mobile devices.

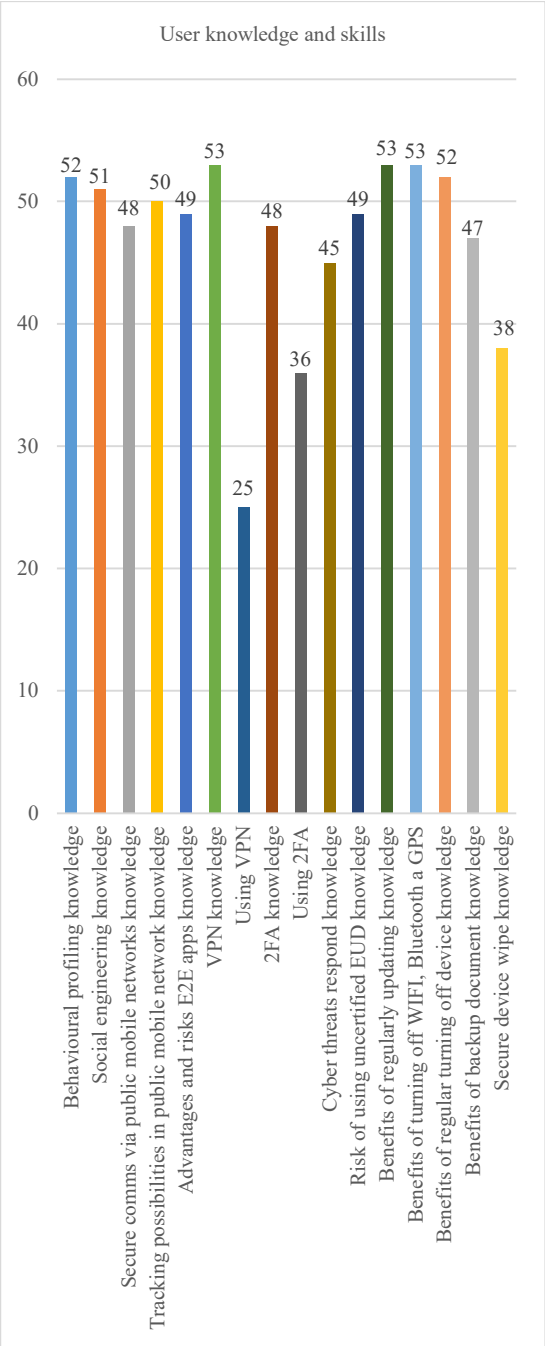

Fig. 2 User knowledge and skills – after using SOP
Source: author.

The proposed rules in standard operating procedures set out ways to secure end devices to enable secure and partially hidden communication in mobile networks and cyberspace based on known threats and practices in 2025. It is important to note that these procedures are only applicable to devices that are not centrally managed by the Slovak Armed Forces. Information intended for user education can definitely be applied in this environment.

Standard operating procedures are a set of measures divided into three pillars (Fig. 3). These are necessary for creating a secure end device that enables secure and hidden communication. This minimises the leaving of personal data in cyberspace. Pillar I, which creates a secure communication environment, assumes that users are educated about cyber threats and the countermeasures that suppress them. Pillars II and III consist of a set of hardware and software measures that must be applied when creating a secure end device and a secure communication environment. The procedures outlined in this article are a proven method of meeting the requirements of all three pillars. These proposals combine well-known measures for protecting users and end devices in cyberspace, adapted to the needs of professional soldiers. The aim is clear: to protect their work and private activities on the internet via mobile networks.

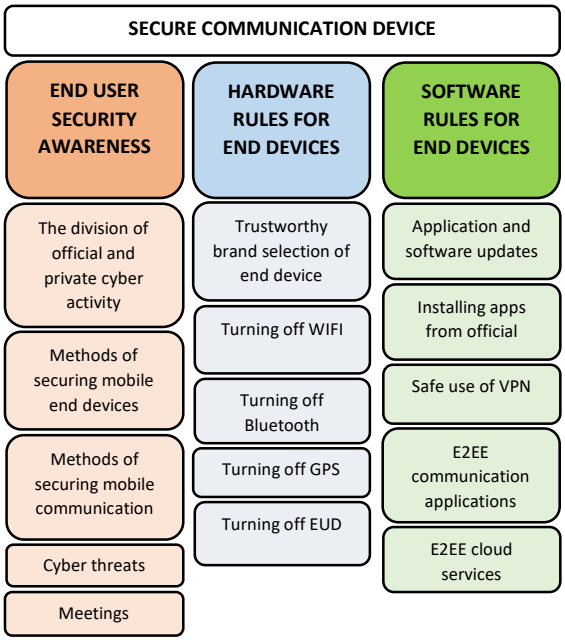

Fig. 3 Security pillars of the mobile end device
Source: author.

The processes outlined here will reduce the potential impact of behavioural profiling and social engineering on users of mobile devices in the Slovak Armed Forces. We will create conditions for the separation of private and work activities. We will make it more difficult for potential adversaries to combine them in their efforts to identify the activities of armed forces members in the areas of domestic crisis management and international crisis management operations. The proposed measures do not define the exact steps for users to take when setting up their end devices. They offer knowledge in areas that need to be monitored and continuously updated so that users can avoid the risks of cyberspace and create a secure communication environment without requiring in-depth technical training.

Behavioural profiling and social engineering are methods that can be used to combine information obtained about users to such an extent that it becomes possible to link private activities with work activities and vice versa. It is therefore vital to take constant

steps to suppress these threats in cyberspace, right at the level of the end-user device.

Behavioural profiling is a method of automated data processing. It collects, analyses and evaluates patterns of behaviour of individuals or groups. The aim is to create a digital profile of them. This process uses statistical and mathematical techniques to identify typical activities, preferences, interests, or risky behaviour patterns based on metadata and other collected data. This method collects metadata in cyberspace and assigns it to individual users to identify their behaviour patterns [5], [6], [7].

Social engineering is a method of manipulating people to obtain sensitive information or force them to perform a specific action that may compromise their security or that of an organisation. This type of attack focuses on human behaviour and psychological weaknesses such as trust, respect for authority, empathy, or a sense of urgency, rather than technical vulnerabilities in systems. Attackers use various techniques to build trust with their victims. They often pose as trustworthy people or institutions. The goal is clear: to obtain passwords, financial data, access to systems, or to perform other actions that benefit the attacker. Social engineering is without doubt one of the most effective tools for obtaining sensitive information. It exploits human nature to be trusting and helpful, often bypassing even technically advanced security measures. It is vital for users with multiple devices and accounts to have consistent separation of identities and strategic data restriction. The following are the best practices according to expert sources [8], [9].

As stated in [10], 72 % of incidents and attacks primarily affect end devices, with 44 % of these triggered through browsers (phishing, redirects). A combination of technical measures and user vigilance has been identified as a means of reducing the success rate of phishing attacks. It has been observed that up to 80% of phishing attacks are initiated by a minority of 4% of users. Training and reporting initiatives have been identified as effective measures for reducing the number of such attacks. Research conducted by the Ponemon Institute [13] indicates that 68 % of organisations encounter endpoint attacks. The study found that two-factor authentication (2FA) and encryption significantly reduce social engineering risks. This finding aligns with the Unit 42 report [10], which identifies social engineering as the most preferred method of initial access for attackers (23 %). Research in [14] demonstrates that technical measures and organisational rules are effective in reducing endpoint risks. The segmentation, anonymization and metadata awareness of data are of particular significance in protecting against the profiling and the dissemination of sensitive data into public cyberspace. [11], [12], [13], [14].

It is essential to maintain a strict separation between one's professional and personal digital activities, as well as to adhere to established security protocols. This approach is fundamental in mitigating the amount of data that can be collected about an individual by external entities.

3 PILLAR I: USER SECURITY AWARENESS

Pillar I is the educational framework that focuses on users and professional soldiers building their knowledge base in areas affecting the security of mobile devices and electronic communications in cyberspace in both their professional and private lives. Mitigating the possibility of identifying the work activities of professional soldiers through their private activities in cyberspace is one of the objectives of this pillar (Fig. 4).

3.1 Basic principles of secure digital communication

Consistent separation of private and professional identities includes the use of separate devices for work and private purposes, as well as independent accounts with different email addresses, phone numbers, and social media profiles, with profiles created only when necessary. If a professional soldier does not need to disseminate information about their work life in cyberspace, they should refrain from doing so without exception. Otherwise, the dissemination of such information must be conditional on minimizing the digital footprint in cyberspace. Minimizing the digital footprint is achieved by using generic names, work contacts, alias email addresses, and virtual payment cards when registering, along with deactivating the collection of analytical data in operating systems and applications.

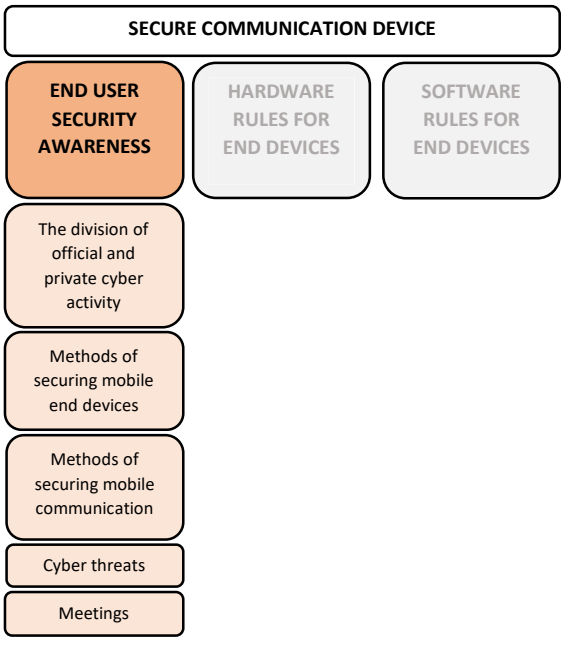

Fig. 4 User security awareness
Source: author.

Metadata, containing information about the location of capture, device type, and file modification history, poses a significant risk of unwitting identification; exposure can be eliminated by turning off unnecessary services (GPS, Bluetooth, Wi-Fi) and pre-sharing by removing metadata from documents. Professional soldiers must have a basic awareness of all these possibilities of leaving digital traces in cyberspace in order to be able to limit and mitigate them.

3.2 Comprehensive security for end devices

User education in end device security is clear: it includes the integration of strong authentication (at least a 6-digit PIN for military environments, automatic locking within 2 minutes), storage encryption (automatic on iOS, manual on Android), regular OS and application updates, installation exclusively from official sources, and mandatory two-factor authentication (2FA) for sensitive services. Professional soldiers must always be aware that their devices contain sensitive information that could help the enemy.

Protection against loss/theft must include several security rules. These must include activating remote lock, locate, and wipe functions (Find My iPhone, Google Find My Device), end-to-end encryption (E2EE) cloud backups, and password changes after an incident.

Before decommissioning a device, it is essential to perform a factory reset or physically destroy it, overwriting any unnecessary data. Antivirus protection is irrelevant on iOS in standard mode thanks to sandboxing and strict App Store controls, while on Android it is recommended as an additional layer against sideloading (the process of installing applications on a mobile device from unofficial sources outside of official stores) and sophisticated threats.

3.3 Advanced mobile communication technologies

A VPN creates an encrypted tunnel that masks your IP address, protects you from eavesdropping on public Wi-Fi, bypasses geoblocks and secures remote access, with a mandatory kill switch. In 5G networks, SUPI (Subscription Permanent Identifier) replaces IMSI and is transmitted exclusively as encrypted SUCI. This neutralises IMSI catchers and reduces the possibilities of behavioural profiling.

eSIM is the solution to the risks of physical tampering, SIM swapping and cloning. It uses a built-in module, remote authentication and audited profiles to enable quick deletion and multi-profile separation. End-to-end encryption secures data on the sender's device with decryption at the recipient's end. This ensures confidentiality, integrity, and resistance to MitM attacks regardless of provider or network.

3.4 Organizational constraints in sensitive negotiations

Mobile devices are stored in lockable cabinets outside meeting rooms to protect against eavesdropping, malware as an entry point, legal breaches, distraction, and AV vulnerabilities. This enhances security culture.

4 PILLAR II : HARDWARE RULES FOR END DEVICES

Hardware rules define physical changes that must be made to devices on a regular basis to prevent cyber attacks and the uncontrolled dissemination of information about users and devices. This chapter does not provide specific procedures and settings for end devices, as these may vary depending on the device and operating system. The chapter provides general information on areas that professional soldiers must consider if they want to create a secure communication environment (Fig. 5).

4.1 Selecting the brand of terminal device

The choice of mobile device manufacturer directly impacts resistance to malware, phishing attacks, data loss and identity theft. Secure devices have three things in common: regular updates, hardware security features, and transparent access to data management. They also limit the collection of user information.

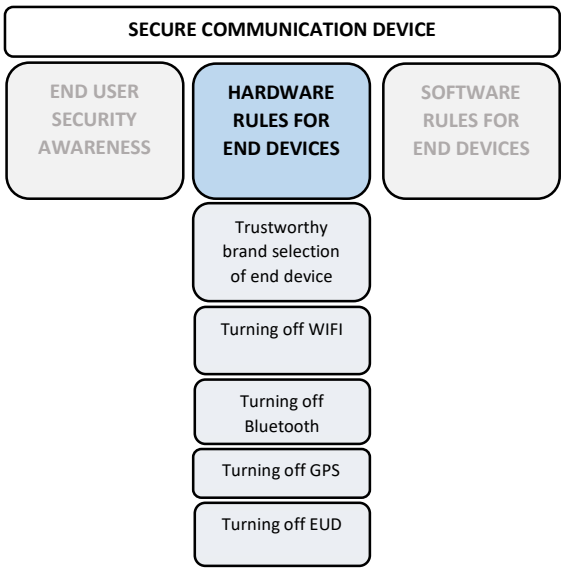

Fig. 5 Hardware rules
Source: author.

Among commercially available platforms, Apple is considered the leader in mobile security. The closed iOS ecosystem, centralized application control, rapid updates, and modules such as Secure Enclave reduce the likelihood of device compromise. In contrast,

Android is an open system with greater variability in security levels, which depend on the manufacturer. Devices such as Google Pixel and Samsung Galaxy provide regular patches, but cheaper brands often lag behind in security support.

An alternative is offered by specialized security phones (e.g., Bittium Tough Mobile, Purism Librem 5, Sirin Labs Finney), which feature hardware kill switches, pre-installed encryption solutions, and advanced access control. They are primarily intended for users working with sensitive information or operating in exposed environments where complete control over data flows is a priority. They are not suitable or affordable for normal private use.

4.2 Turning off WiFi and Bluetooth

Leaving WiFi and Bluetooth wireless interfaces permanently enabled is a major security risk, significantly increasing the device's attack surface (the possibility of unauthorized access to the device). Active interfaces constantly transmit signals that attackers can use to identify or compromise the device.

Attacks such as MitM, bluesnarfing, or bluejacking allow access to data, its modification, or unauthorized monitoring. Automatic connection to public networks poses a risk of intercepting transmitted data. A device with activated interfaces constantly sends information about its location and movement. This facilitates user profiling.

Disabling these interfaces is undoubtedly one of the easiest ways to limit attackers options, reduce energy consumption, and maintain data integrity.

4.3 Turning off GPS

Location services carry significant risks. These include location tracking, loss of privacy and misuse of work or personal information. An active GPS module provides accurate device location data. This can be collected by applications, advertising networks, or malware from a potential adversary.

Removing access to GPS minimizes the possibility of illegitimate tracking, movement profiling, and data collection through compromised applications. This principle is particularly critical in security-sensitive environments—such as the armed forces, diplomatic missions, or research organizations—where the leakage of location data can pose a strategic threat.

Regularly turning off GPS is not only an effective way to prevent cyber attacks, but also a responsible approach to digital privacy.

4.4 Turn the device off regularly

Turn off your mobile device for at least 30 minutes once a week. It's a practical measure with a significant security impact. This simple step is vital for stopping malicious processes that may be active in memory and also supports the application of updates that require a system restart.

From a technical point of view, this clears the operating memory, restores system stability, and reduces excessive energy consumption. From a cyber security perspective, it is important that the shutdown terminates all network connections, eliminating the possibility of ongoing attacks such as zero-click exploits or remote access via vulnerable services.

This habit also provides effective protection against surveillance, as a switched-off device cannot be actively monitored, even by spyware tools. In environments with high security requirements, regular shutdown is considered an essential security standard.

5 PILLAR III: SOFTWARE RULES FOR END DEVICES

Software rules are the most effective way of regulating digital habits. They do this by minimising risks, preventing cyber attacks and the uncontrolled dissemination of information about users and devices. This chapter makes clear the vital importance of regularly updating operating systems and applications to prevent vulnerabilities and cyber attacks. The recommendation is clear: install applications exclusively from official stores (Google Play, App Store) for quality and security control. It addresses VPN selection, emphasizing the importance of strong encryption protocols and the provider's "no-log" policy (Fig. 6).

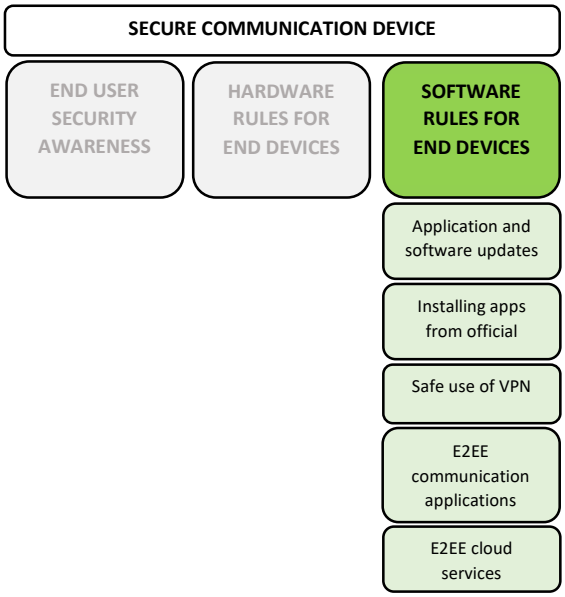

Fig. 6 Security pillars of the mobile end device
Source: author.

5.1 Regular updates

Regular software updates are the most basic and effective preventive measure against known

cyber threats. Developers constantly identify vulnerabilities in operating systems and applications. Security patches remove these bugs and limit the exploitation of vulnerable components.

Ignoring updates increases the risk of malware infection, data loss, or identity compromise. In addition to the security aspect, updates also improve system stability, optimize energy consumption, and extend the life of the device.

Updated software ensures compatibility between applications and new versions of operating systems. This prevents functionality failures and increases user comfort. From a digital hygiene perspective, regular updates must be considered a routine and automated user activity.

5.2 Install apps only from official stores

Official distribution platforms are a fundamental pillar of a secure mobile device ecosystem. This means that they must be used (e.g. Google Play Store, App Store). These platforms implement a multi-stage application verification process that includes both automated and manual testing. This process is designed to detect malicious code, illegitimate permissions, and fraudulent activities.

You must never install applications outside of official channels (known as sideloading). This dramatically increases the risk of malware infection, data leaks, spyware attacks, or financial fraud. Expert analyses confirm that most mobile malware comes from unverified sources [15].

Official stores also offer faster updates, transparency through user ratings, and clear information about how personal data is handled. This improves awareness and control over how apps interact with sensitive data.

5.3 Use the VPN safely

A virtual private network (VPN) is an indispensable tool for protecting communications and anonymizing data transfers. However, its effectiveness depends on choosing a trustworthy provider and the correct technical settings.

The basic criterion is a no-log policy. This means the provider must commit to not keeping records of user activity. Independent audits (e.g. Deloitte, Securitum) verify this. Use WireGuard, OpenVPN or IKEv2. These VPN protocols guarantee a high level of encryption and reliable data transmission.

Using a VPN is essential, especially when connecting to public Wi-Fi networks or working with sensitive information. It is advisable to avoid free VPN services, as they often trade user data or use outdated encryption algorithms.

5.4 Using apps with end-to-end encryption

Applications with E2EE significantly increase the integrity and confidentiality of communications. E2EE ensures that transmitted messages and files are readable only by the participants in the communication and not by the service provider.

However, in addition to technical protection, it is essential to verify the identity of the communication partner, especially when there is suspicion of possible manipulation. Users should monitor the latest findings on the vulnerabilities of individual E2EE platforms and regularly adapt their communication environment to current threats.

The reliability of these applications can be enhanced by verifying public security audits, similar to VPN providers.

5.5 Use of end-to-end encrypted cloud services

End-to-end encryption in cloud systems is the highest standard of data protection during transmission and storage. Data is encrypted directly on the user's device, and the decryption keys remain exclusively in their possession. This model eliminates the need to trust the provider, as neither they nor any third party can see the contents of the files in readable form.

E2EE is essential for protecting against internal incidents, infrastructure compromise, and unauthorized access by the provider's employees. A successful attack on cloud servers is impossible because the data is inaccessible to the attacker due to the absence of keys.

This approach also minimises the impact of ransomware attacks. Without access to the keys, the attacker cannot decrypt the content or use it for extortion. In environments where sensitive information is managed (e.g. in corporate or government systems), the use of E2EE cloud is the most effective strategy for minimizing risk.

6 CONCLUSION

When using mobile technologies to support combat operations, it is essential to ensure communication is based on 5G standards. 5G technologies represent a significant shift in the field of secure and effective communication. They are vital for both civilian and military purposes. Their original development was focused on commercial use, but their features make them ideal for adaptation by the Slovak Armed Forces. These features include high throughput, low latency and advanced security architecture. These technologies provide robust mechanisms such as encryption, anonymisation of identifiers, and zero trust principles. This means that the risks associated with surveillance, eavesdropping, and cyberattacks are minimised.

When using 5G technologies for military purposes, it is essential to focus on three key areas of protection: data, location and identity. Implement mechanisms such as end-to-end anonymisation, identifier encryption and strict access control to effectively minimise the risks associated with

tracking military unit activities. Furthermore, advanced standards set by organisations such as ITU-T and 3GPP provide strong protection for personal and sensitive data, significantly reducing the potential for misuse.

Military end devices must be designed to meet specific requirements for combat operations. As well as securing communications and protecting data, they must provide sufficient performance to process information from the battlefield. They serve not only as means of communication but also as sensors for collecting and transmitting data. The security of these devices is based on three pillars: personnel training, selection of reliable hardware, and deployment of secure software. These pillars provide the foundation for creating robust solutions that can effectively counter common security threats, such as malware, MitM attacks, and attempts to steal sensitive information.

Despite technological advances, humans remain the most vulnerable link in the security chain. Raising awareness and thoroughly training staff are the keys to eliminating known cyber threats and ensuring the proper use of end devices. It is vital to implement operational security rules. This includes separating private and professional life, and using security tools such as VPNs and encrypted communication applications. These measures are essential to ensure security in demanding combat conditions.

It is clear that standard operating procedures must be established for CIS officers in the area of planning and for end-device users. This is the only way to ensure the safe use of mobile technologies. The Slovak Armed Forces have only minimal development in both areas. System administrators who create technical network security make up only a small percentage of the total number of personnel involved. Their education, professional and security awareness is indisputably at a high level. We consider it sufficient. We are convinced that the greatest risks are at the level of network users. Military personnel from the commercial world have habits that do not reflect the strict requirements of the Slovak Armed Forces for securing information transfer. Incorrect planning or working with end devices will cost the Slovak Armed Forces lives or equipment. We regularly see examples of mistakes in the use of mobile networks in the Russian-Ukrainian war.

References

[1] LUCAS, R. 2019. *The EU assesses cyber security and 5G networks.* (Online). Royal United Services Institute for Defence a Security Studies. Available at: https://rusi.org/explore-our-research/publications/commentary/eu-assesses-cyber-security-and-5g-networks [cit. 2024-04-12].

[2] EUEROPEAN UNION. 2019. *EU coordinated risk assessment of the cyber security of 5G networks.* NIS Cooperation Group. (Online). Available at: https://ccdcoe.org/uploads/2019/10/EU-191009-Report-on-coordinated-risk-assessment-of-cybersecurity-o-5G-networks.pdf [cit. 2024-04-12].

[3] LIYANAGE, M.; BUX ABRO A.; AHMAD, I.; GURTOV, A. and YLIANTTILA, M. 2018. *A comprehensive guide to 5G security.* New Jersey: John Wiley & Sons Ltd. 440 pp. ISBN 9781119293040.

[4] HAYES, D.; CAPPA, F. and LE-KHAC, N. A. 2020. An effective approach to mobile device management: Security and privacy issues associated with mobile applications. In *Digital Business.* Vol. 1, no. 1. (Online). 8 pp. Available at: https://www.sciencedirect.com/science/article/pii/S2666954420300016 [cit. 2024-09-10].

[5] LI, F.; WHEELER, R. and CLARKE, N. 2014. *An evaluation of behavioural profiling on mobile devices*. HAS 2014: Human Aspects of Information Security, Assurance and Privacy, Bournemouth, United Kingdom. Lecture Notes in Computer Science, vol 8533. Springer. https://doi.org/10.1007/978-3-319-07620-1_29.

[6] GURUCUL. 2025. *Behavioural analytics cyber security: complete guide to user behavior analysis*. Gurucul Blog. (Online). Available at: https://www.sciencedirect.com/science/article/pii/S2666954420300016 [cit. 2025-11-10].

[7] FIDELIS SECURITY. 2025. *Effective metadata analysis: An essential guide on the process and techniques*. (Online). Available at: https://fidelissecurity.com/cybersecurity-101/network-security/metadata-analysis/ [cit. 2025-06-12].

[8] ESET. 2024. *Sociálne inžinierstvo a kybernetická bezpečnosť*. (Online). Available at: https://www.eset.com/sk/socialne-inzinierstvo-a-kyberneticka-bezpecnost/ [cit. 2025-06-12].

[9] CSIRT. 2024. *Sociálne inžinierstvo*. (Online). Available at: https://www.csirt.gov.sk/socialne-inzinierstvo.html [cit. 2025-06-12].

[10] KIRSCH, Ch.. 2016. *IDC: 70 % of Successful Breaches Originate on the Endpoint*. (Online). Available at: https://www.rapid7.com/blog/post/2016/03/31/idc-says-70-of-successful-breaches-originate-on-the-endpoint/ [cit. 2025-06-12]

[11] PALO ALTO NETWORKS and UNIT 42. 2025. *Global Incident Response Report 2025.* (Online). Available at: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report [cit. 2025-06-12].

[12] HOXHUNT. 2024. *Human Risk Management: The Complete CISO Playbook.* (Online). Available at: https://hoxhunt.com/guide/human-risk-management-playbook [cit. 2025-06-12].

[13] PONEMON INSTITUTE. 2020. *Endpoint Security Statistics.* (Online). Available at: https://www.spyhunter.com/shm/endpoint-security-statistics/ [cit. 2025-06-12].

[14] MORPHISEC. 2020. *Third Annual Study on the State of Endpoint Security Risk.* (Online). Available at: https://engage.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf [cit. 2025-06-12].

[15] ZIMPERIUM. 2025. *2025 Global Mobile Threat Report.* (Online). Available at: https://lp.zimperium.com/hubfs/Reports/2025%20Global%20Mobile%20Threat%20Report.pdf [cit. 2025-11-12].

Lt Col Dipl. Eng. Štefan **GAŠO**
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: stefan.gaso@protonmail.com

Assoc. Prof. Dipl. Eng. Marián **BABJAK**, PhD.
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: marian.babjak@aos.sk

Štefan GAŠO is a communications and information systems officer with a master's degree in Electronic Systems from the Armed Forces Academy in Liptovský Mikuláš, where he is currently in his 4th year of PhD studies. He has served in various command and staff positions from platoon leader to head of CIS branches, including deployments to ISAF and RS Afghanistan as a SOF advisor, and roles in international special operations headquarters as deputy J6. Currently, he is Head of the CIS and Information Security Branch at SVK Special Operations Forces Command (SVK SOFCOM), specializing in planning and management of military CIS and support to special operations forces.

Marián BABJAK received PhD. degree at Military academy in Liptovský Mikuláš in 1997 and Assoc. Prof. degree at Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš in 2022. His research interests are focused on communication systems, especially source and channel coding, modulation, signal processing and signal processing in military application. He is currently working as an associated professor at the Department of Electronics, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš.

DOI: https://doi.org/10.52651/sam.a.2026.1.24-32

TACTICAL SIMULATOR FOR C2 TRAINING AND REAL-TIME NATO-COMPATIBLE DATA DISTRIBUTION

Marek BENČÍK, Dominika DUDÁŠIKOVÁ, Martin RÉVAY

Abstract: This paper presents a browser-native tactical simulator designed for seamless integration with military command and control (C2) systems. The proposed system enables the simulation of tactical unit movement, hierarchical formation control, and generation of geospatial data in real time. NATO interoperability is supported through standardized mechanisms for entity tracking and tactical graphics distribution, including NATO Friendly Force Information (NFFI) and NATO Vector Graphics (NVG). A key part of the simulator is a mathematical formation-control model that preserves the relative geometry of multi-unit groups during movement and directional changes. By executing all computational logic directly on the client side, the simulator enables rapid, installation-free deployment and operation with limited dependence on server infrastructure. The architecture is therefore suitable for training and testing scenarios where real units or full-scale simulation systems are not available. The results indicate that browser-native technologies can effectively support C2 training, interoperability testing, and validation of tactical data flows without deploying physical forces.

Keywords: command and control; tactical visualization; browser-based application; formation control; military simulation.

1 INTRODUCTION

Modern command and control (C2) systems play a crucial role in ensuring situational awareness [12], coordination of units, and decision support in dynamic operational environments. Their importance has significantly increased with the emergence of information warfare and network-centric operations, where the quality, speed, and accuracy of shared information directly influence command effectiveness and force synchronization [1], [2], [11].

From a doctrinal perspective, C2 can be understood as a comprehensive process in which a commander exercises authority and direction over assigned forces to accomplish defined operational objectives [3]. This process encompasses continuous acquisition, processing, and dissemination of information, its visualization in a geospatial context, and the subsequent coordination of unit activities in space and time. Consequently, the effectiveness of C2 is directly dependent on the system's ability to provide an accurate, timely, and comprehensible operational picture.

To meet these requirements, modern C2 systems are designed as complex software solutions integrating geospatial data, unit tracking, and visualization of tactical elements within a common operational picture. These systems emphasize interoperability and standardization, relying on defined communication protocols and data formats within NATO frameworks. However, their effective use in practice often requires specialized workstations, software configuration, and reliable network infrastructure. The importance of information technologies for effective command and control is further emphasized by recent studies focusing on C4ISTAR capabilities and their role in modern military operations [11].

In the context of training and personnel education, there is a need to realistically simulate the behavior of units within such environments. For operators to effectively work with C2 systems, it is essential to provide dynamic data representing unit movement and interaction. In real-world conditions, such scenarios require the deployment of actual units or complex simulation systems, which is both time-consuming and costly. Therefore, it is desirable to have tools capable of generating realistic tactical scenarios without the need for physical deployment of forces.

The sharing of positional data between units within NATO is standardized through Friendly Force Tracking (FFT) systems, defined, in the ADatP-36 standard [6]. These mechanisms enable real-time exchange of unit position data across different C2 systems. For the transmission of more complex tactical elements, such as axes of advance, lines, or obstacles, the NVG standard defined in ADatP-4733 is used [7]. Semantic correctness and structured reporting are ensured through the NATO Message Catalogue (APP-11) [8].

Despite the existence of advanced C2 systems and military simulation tools, there remains a lack of lightweight solutions capable of generating realistic tactical data in compliance with NATO standards while being easily deployable without complex infrastructure. Existing solutions are often tied to specialized platforms or do not allow direct integration into standardized C2 interfaces in the form of interoperable data streams.

This limitation is particularly evident in training, interoperability testing, and validation of data flows, where it is necessary to simulate unit behavior

and interaction in real time without deploying physical forces. The proposed system aims to address this gap.

Based on these considerations, this paper presents the design and implementation of a web-based simulator for tactical units that enables the simulation of unit movement, formation control, and generation of tactical data in compliance with NATO standards. The proposed solution is based on a client-centric architecture, where all simulation logic is executed directly within a web browser without the need for additional software installation.

The main contribution of this work is the design of a mechanism that enables:

- simulation of movement and behavior of tactical units,
- generation and transmission of position data compatible with NFFI to external C2 systems,
- creation and distribution of tactical graphical elements using the NVG standard,
- preservation of formation geometry through a mathematical model of movement control.

The proposed system thus represents an effective tool for training, interoperability testing, and validation of data flows between C2 systems, while reducing the time and financial costs associated with real-world exercises.

2 RELATED WORK

The development of modern command and control (C2) systems and tactical simulation tools is closely linked to requirements for interoperability, data standardization, and efficient processing of geospatial information. This section provides an overview of relevant research directions and technological approaches that form the foundation for the proposed solution.

2.1 C2 Systems and Situational Awareness

Modern C2 systems are designed to support situational awareness, which represents the ability to perceive, interpret, and anticipate the evolution of a dynamic operational environment. The quality of situational awareness depends directly on the effective acquisition, processing, and presentation of information in real time.

Within the context of network-centric operations, information sharing between system elements plays a critical role in improving coordination and synchronization of activities. This principle is implemented through the concept of a Common Operational Picture (COP), which integrates data from multiple sources into a unified visual interface [13].

Research in this area highlights the importance of visualization tools and geospatial technologies in reducing operator cognitive load and enhancing decision-making efficiency. However, most existing solutions assume the use of robust software platforms and centralized system architectures. The role of ICT systems in supporting decision-making processes within tactical command structures has also been emphasized in previous research [14].

2.2 Interoperability and Tactical Data Exchange

Interoperability represents a fundamental requirement of modern military information systems. Within NATO, standardized mechanisms are defined to enable data exchange between different C2 systems regardless of their implementation specifics.

A key mechanism in this domain is Friendly Force Tracking, which enables real-time sharing of positional data through standardized data structures and communication protocols [6]. To ensure consistent interpretation of exchanged information, standardized message catalogues are used to define the structure and semantics of individual data elements [8].

In the context of modern software architectures, distributed and web-based technologies are increasingly being adopted. However, integrating these technologies with established military standards introduces challenges related to the transformation of data between modern formats and traditional structured messaging systems.

2.3 Tactical Symbology and Vector Graphics

Visualization of tactical information is an essential component of C2 systems. Standardized military symbology enables unambiguous interpretation of entities and events on digital maps. These standards define the representation of units, their affiliation, and activities through formalized identification codes [4], [5].

In addition to point-based entities, it is necessary to represent more complex geospatial elements such as lines, areas, and axes of operation. For this purpose, standards enabling the exchange of geometric data in an interoperable format are employed [7].

At the same time, significant progress has been made in web-based geospatial technologies. Modern approaches allow processing and visualization of map data directly within web browsers, reducing dependence on native applications, and increasing system accessibility. However, these technologies are not primarily designed for military standards, which limits their direct applicability in C2 environments.

2.4 Simulation Tools and Identified Gap

Simulation tools used in military environments are typically designed as complex systems intended for detailed modeling of combat operations and training at higher levels of command. These solutions often require specialized hardware, extensive configuration, and are not primarily

focused on seamless integration with existing C2 systems.

From the perspective of training and interoperability testing, there is a need for tools capable of generating dynamic tactical data in a standardized form and enabling straightforward integration with existing systems. Current approaches only partially address the requirement for lightweight, rapidly deployable solutions based on modern web technologies.

This limitation represents the motivation for the proposed solution, which aims to combine simulation capabilities with support for standardized data formats while minimizing technological and infrastructure requirements.

3 SYSTEM ARCHITECTURE DESIGN

The proposed simulator is based on an offline-first architectural paradigm designed to ensure system functionality in environments with limited or unstable network connectivity. This approach, commonly used in modern web-based systems to support resilience and local autonomy, enables the system to operate fully independently of server-side services during simulation and planning tasks. The core design principle is the delegation of computational logic and geospatial processing to the client side, thereby minimizing dependence on external infrastructure and improving system responsiveness.

At the same time, the architecture supports integration with external command and control systems through standardized data interfaces,allowing simulated data to be exchanged when connectivity is available.

3.1 Overall Architecture

The proposed architecture is divided into two main components: a client-side layer implemented within a web browser and a server-side integration layer responsible for communication with external systems (Fig. 1).

Client-Side Layer (Web Browser)

This layer represents the core of the system and includes the user interface, geospatial engine, and application logic implemented in JavaScript. All computations related to unit movement simulation, formation control, and tactical data processing are executed directly in the client's memory. This approach reflects current trends in web-based geospatial applications, where processing is increasingly performed on the client side to improve performance and scalability [10].

The client also manages local data persistence using browser storage, enabling scenario data, unit states, and tactical elements to be stored and retrieved without requiring server communication. This ensures uninterrupted operation even in fully disconnected environments. For fully disconnected operations, the geospatial engine is designed to utilize pre-cached local map tiles or a locally hosted tactical base map, eliminating the dependency on external web map services (WMS).

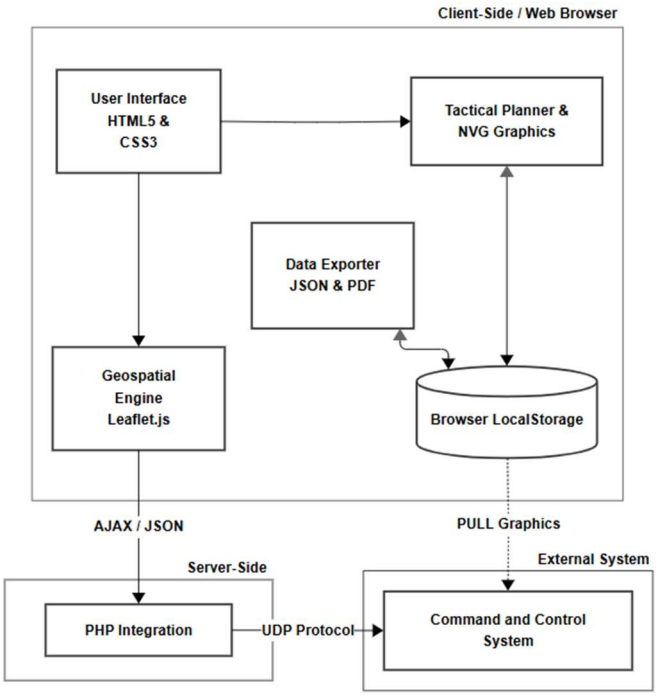

Fig. 9 Overall architecture of the offline-first tactical simulation and C2 integration system
Source: author.

Server-Side Integration Layer

The server-side component is designed as a lightweight integration module without its own simulation or application logic. Its primary role is to act as a protocol translation bridge between web-based communication (HTTP/JSON) and communication mechanisms used by external systems, such as UDP-based data exchange.

This design ensures that all simulation-related functionality remains on the client side, while the server layer is used exclusively for interoperability purposes.

3.2 Data Integration Model

To ensure interoperability with external systems, a dual-channel data integration model is introduced, separating high-frequency positional data from less frequent but more complex tactical information.

Channel 1 – Positional Data (Real-Time Tracking):

Position data generated by the simulator are processed on the client side and transmitted as structured JSON messages to the integration layer. The integration layer transforms these messages into formats compatible with Friendly Force Tracking standards [6] and forwards them using a push-based mechanism to external systems via UDP communication.

Channel 2 – Tactical Graphics:

Geospatial objects such as lines, areas, and axes of operation are generated and managed on the client side and subsequently serialized into the NATO Vector Graphics (NVG) format [7]. These data are exposed through a server endpoint, from which external systems retrieve them using a pull-based mechanism at defined intervals.

The separation of push-based positional updates and pull-based graphical data exchange allows efficient handling of different data types, optimizing communication load while preserving semantic consistency.

3.3 Data Persistence and Export

To minimize dependence on external services and support offline operation, the system utilizes browser-based local storage for scenario persistence. All relevant simulation data, including unit positions, hierarchical structures, and tactical elements, are stored locally within the client environment.

The system provides two primary data export mechanisms:

Scenario Export:

The current simulation state is serialized into a structured JSON format (Fig. 2), allowing scenarios to be saved, transferred, and reloaded without requiring backend processing. This mechanism supports rapid scenario replication and sharing between users.

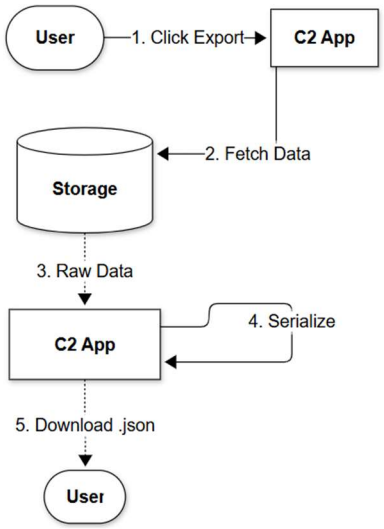

Fig. 2 Client-side workflow for scenario serialization and JSON-based export
Source: author.

Report Generation:

The system enables the generation of tactical reports in PDF format directly on the client side (Fig. 3). Data represented in HTML are transformed into a printable document format, allowing report generation even in fully disconnected environments. This approach ensures that reporting functionality remains available regardless of network conditions.

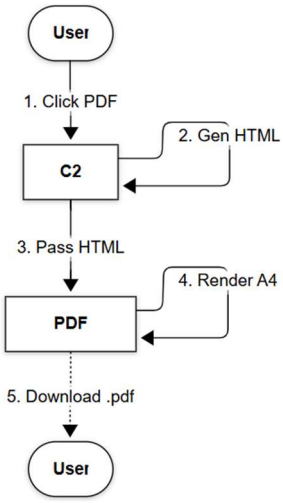

Fig. 3 Client-side workflow for tactical report generation and PDF export
Source: author.

4 PROTOTYPE IMPLEMENTATION

The prototype was implemented as a lightweight browser-based application using a modular JavaScript architecture. The implementation is organized into four main functional components: tactical symbology generation, geodesic route planning and formation control, tactical graphics generation based on the NATO Vector Graphics standard, and temporal synchronization of unit movement.

4.1 Tactical Symbology and SIDC Engine

The system implements a dynamic rendering mechanism for military symbology in accordance with NATO APP-6(C) [4] and MIL-STD-2525C [5]. Each entity is represented by a Symbol Identification Code (SIDC), which is parsed and transformed into a visual symbol.

Visualization is performed using vector graphics directly within the web browser environment, allowing symbols to scale without loss of quality. This approach ensures consistent interpretation of tactical elements across different map zoom levels and avoids the pixelation typically associated with raster-based icons.

4.2 Geodesic Route Planning and Formation Control

The route planning module enables the definition of unit movement between waypoints in a geospatial environment. The distance between two points on the Earth's surface is calculated using the Haversine formula, which accounts for the curvature of the Earth:

$$d = 2r \arcsin\left(\sqrt{sin^2\left(\frac{\Delta\phi}{2}\right) + cos(\phi_1)\, cos(\phi_2)\, sin^2\left(\frac{\Delta\lambda}{2}\right)}\right) \quad (1)$$

where:

- $\varphi 1$, $\varphi 2$ are latitudes,
- $\Delta\varphi$ and $\Delta\lambda$ are differences in latitude and longitude,
- r is the Earth's radius.

The Haversine formula was intentionally selected to optimize client-side computational performance. While this model assumes a spherical approximation of the Earth, which introduces a theoretical geometric deviation of approximately 0.1 % to 0.3 % compared to more complex ellipsoidal models, it is highly efficient for real-time browser-based simulations. In the context of tactical visualization, a 0.1 % deviation corresponds to an error of approximately 1 meter per kilometer of movement, which is negligible for situational awareness and training. Implementing a more computationally intensive model (such as Vincenty's formulae) would significantly increase the overhead on the browser's main thread without providing a substantial operational advantage for tactical map representation.

A key feature of the system is formation control based on the leader-follower principle. In this model, the movement of the lead unit determines the movement of all subordinate units within the formation. Instead of defining separate trajectories for each unit, the operator specifies only the route of the lead unit, while the positions of the remaining units are computed automatically. The overall logic of the route planning and formation control algorithm is illustrated in Fig. 4.

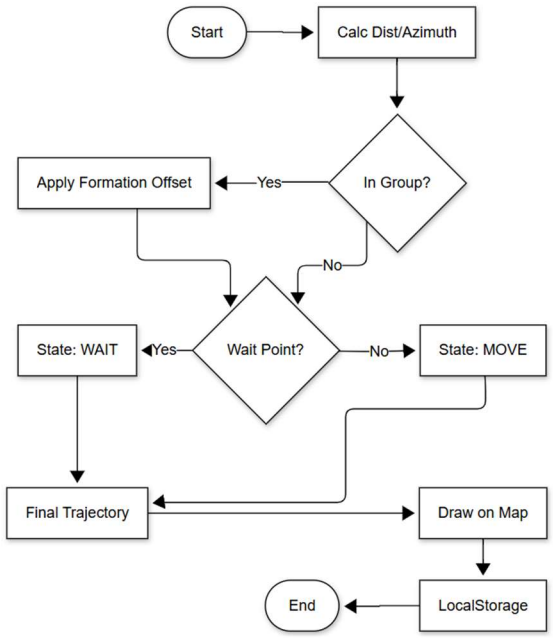

Fig. 4 Flowchart of geodesic route planning and formation control algorithm
Source: author.

The relative position of each subordinate unit is defined by Cartesian coordinates $(dx,\ dy)$, representing their offset from the lead unit. Rather than using a conventional two-dimensional rotation matrix, which may introduce distortions in map-based applications, the offset is transformed into a polar representation:

$$d_f = \sqrt{dx^2 + dy^2} \quad (2)$$

$$\alpha_{final} = \alpha_{lead} + atan2(dy,\ dx) \quad (3)$$

where:

- d_f is the distance from the lead unit,
- α_{lead} is the azimuth of the lead unit,
- α_{final} is the resulting movement direction of the subordinate unit.

The resulting polar vector is then used by the geodesic engine to determine the geographic position of the subordinate unit. This approach

preserves formation geometry during directional changes and reduces the amount of manual input required from the operator. The recalculation of subordinate positions is performed directly on the client side with very low computational overhead, allowing responsive updates during dynamic maneuvers.

Experimental verification showed that subordinate units maintained their relative tactical positions with high precision, with geometric deviation remaining below 0.1 % during dynamic movement. A practical example of this functionality is shown in Fig. 5, where the interface displays both the unit hierarchy and the resulting trajectory of a multi-unit formation.

Fig. 5 User interface of the tactical mission planner demonstrating route definition and unit hierarchy
Source: author.

4.3 NVG Module and Tactical Graphics

The visualization of complex tactical elements is implemented in accordance with the NATO Vector Graphics standard [7]. Unlike point-based objects, these elements require dynamic geometry generation and structured representation.

One example is the construction of an axis-of-advance graphic, where an auxiliary point is derived to define the width of the arrowhead. Let $\Delta\varphi = \varphi_2 - \varphi_1$ and $\Delta\lambda = \lambda_2 - \lambda_1$ denote the differences in latitude and longitude between two reference points:

$$\phi_3 = \phi_1 + (\Delta_\phi \cdot 0.5) - (\Delta_\lambda \cdot 0.15) \quad (4)$$

$$\lambda_3 = \lambda_1 + (\Delta_\lambda \cdot 0.5) + (\Delta_\phi \cdot 0.15) \quad (5)$$

These calculations support consistent reconstruction of tactical graphics across different systems. In contrast to conventional geospatial tools, where such elements may be represented only as visual polylines or polygons, the proposed implementation treats them as structured tactical objects carrying both geometric and semantic meaning.

The resulting graphical elements, including phase lines, axes of operation, and obstacle overlays, are displayed as interactive map layers, as shown in Fig. 6. Their structured representation enables subsequent export and exchange in interoperable form.

Fig. 6 Visualization of tactical vector graphics (NVG) including phase lines, directions of attack, and obstacle overlays
Source: author.

4.4 Tactical Timing and Synchronization Mechanisms

In addition to spatial route planning, the system includes a temporal synchronization mechanism for coordinated unit movement. This functionality is based on so-called wait points, which act as control nodes at which movement may be paused until predefined tactical conditions are satisfied.

The mechanism is implemented using a state machine that switches between the states “MOVE” and “WAIT”. When a unit or formation reaches the proximity threshold of a wait point, movement is suspended while the relative geometry and orientation of the formation are preserved according to the previously calculated geodesic offsets.

This functionality is particularly useful for synchronized maneuvers such as Time-on-Target (ToT) operations, in which multiple formations are required to arrive at a designated objective at the same time from different directions. Automating these transitions reduces the need for manual coordination of individual units while preserving consistent system behavior in environments with limited connectivity.

5 EVALUATION AND TESTING

The performance and interoperability of the proposed simulator were evaluated through a series of functional tests and integration experiments with an external command and control environment. The evaluation focused on three main

aspects: computational performance in offline mode, geometric accuracy of formation movement, and correctness of data exchange using standardized interfaces.

5.1 Functional and Geospatial Performance

Functional testing was conducted in a standard web browser environment to assess system responsiveness under offline conditions. Since all tactical logic and geospatial rendering are executed directly on the client side, operations such as waypoint creation, trajectory updates, formation recalculation, and rendering of tactical elements were performed without reliance on stable network connectivity.

The results indicate that user interactions are processed in real time, with no observable delays during standard operation. This behavior confirms that the system meets the requirements for responsiveness in Disconnected, Intermittent, and Limited (DIL) environments.

5.2 Formation and Movement Accuracy

The accuracy of the geodesic formation control algorithm was evaluated through simulation scenarios involving multi-unit formations performing dynamic maneuvers.

A test scenario consisting of a 5 km route with multiple directional changes, including 90-degree turns, was executed. The relative positions of subordinate units were continuously monitored and compared against their intended formation offsets.

The results show that the deviation remained below 0.1% of the intended offset throughout the simulation. This confirms that the proposed leader-follower approach, combined with geodesic calculations, preserves formation geometry with high precision during movement.

5.3 Integration Correctness and Interoperability

The data integration model was validated through controlled data exchange between the simulator and an external system implementing standard tactical data interfaces.

Two communication channels were evaluated:

- **Push-based positional updates:** Unit position data were transmitted at regular intervals (2 seconds) using UDP-based communication. The receiving system successfully interpreted and displayed the transmitted positions in accordance with Friendly Force Tracking principles [6].
- **Pull-based tactical graphics exchange:** Tactical graphics were serialized into the NATO Vector Graphics (NVG) format [7] and made available via an HTTP endpoint. The receiving system periodically retrieved these data and reconstructed the graphical elements within its geospatial interface.

The evaluation confirmed that both data exchange mechanisms operate reliably and maintain semantic consistency across systems.

5.4 Operational Scenario Result

To validate the system under realistic conditions and verify its end-to-end interoperability, a complex tactical scenario was constructed. The scenario integrated multiple unit hierarchies, planned routes, and various tactical graphics, including obstacles and operational axes, as defined within the browser-based simulator (Fig.7).

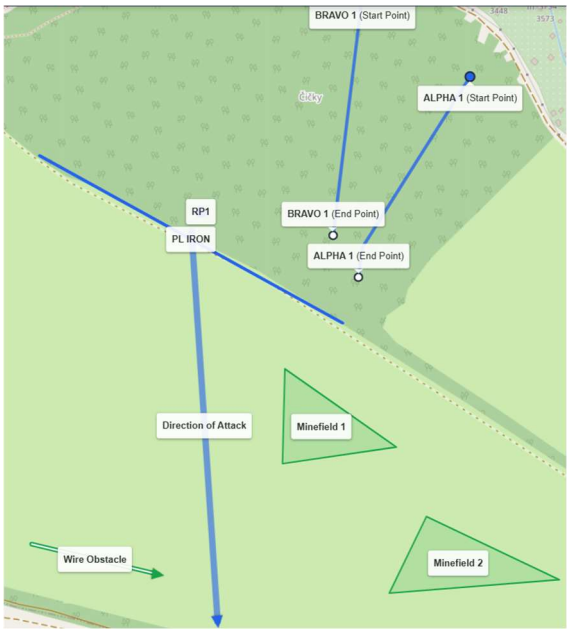

Fig. 7 Integrated tactical scenario showing multi-unit formations, planned routes, and tactical graphics
Source: author.

Subsequently, the comprehensive operational picture was transmitted to the external hC2 environment to validate the dual-channel data integration model. As illustrated in Fig. 8, the hC2 system successfully interpreted and visualized the complete dataset. The entities maintained their correct SIDC classifications and hierarchical affiliations, while the complex NVG layers (lines, areas, and vectors) were accurately reconstructed without geometric distortion.

The scenario demonstrated that the system could manage a dense tactical picture while maintaining consistent behavior in terms of unit movement, graphical representation, and standardized data exchange.

The results indicate that the proposed approach enables effective simulation of coordinated unit movement and tactical planning within a lightweight browser-based environment, while ensuring seamless

and reliable integration with operational military C2 infrastructures.

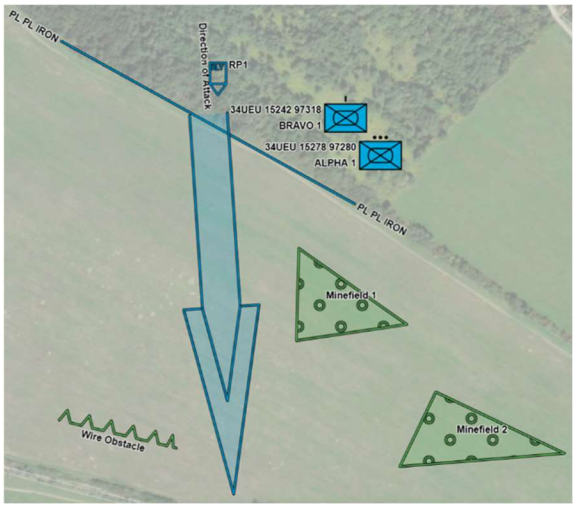

Fig. 8 Interpreted tactical data and NVG graphics rendered in the target hC2 command and control system
Source: author.

6 CONCLUSION

This paper presented the design, implementation, and evaluation of a browser-native tactical simulation system based on a client-centric, offline-first architecture. The results demonstrate that such an approach enables effective simulation of coordinated unit movement and tactical planning without reliance on continuous server connectivity.

The primary contribution of this work lies in the architectural design that shifts computational logic and geospatial processing to the client side, allowing the system to operate autonomously in DIL environments. In addition, the proposed dual-channel data integration model enables interoperability with external systems by separating high-frequency positional updates from structured tactical graphics exchange in accordance with established standards [6], [7].

The evaluation results confirm that the system achieves real-time responsiveness for local operations and maintains high geometric accuracy in formation control, with deviations remaining below 0.1% during dynamic maneuvers. These findings indicate that modern browser-based environments can support the level of precision required for tactical planning tasks [3].

Furthermore, the implementation demonstrates that standard web technologies can be effectively used to generate and manage structured tactical data, including military symbology and complex graphical elements, in accordance with relevant interoperability standards [5], [7].

The presented approach is particularly suitable for scenarios requiring lightweight and rapidly deployable tools, such as training environments or mission preparation at lower command levels. By reducing dependence on dedicated hardware and persistent network connectivity, the system increases operational flexibility while maintaining compatibility with standardized data exchange mechanisms.

Future work will focus on extending the system with advanced capabilities, including autonomous behavior modeling for simulated entities and improved security mechanisms for data exchange and local storage. Further validation in large-scale operational scenarios may also provide additional insights into system scalability and robustness.

Acknowledgement

The paper has been supported by the outputs of the research project "NI4200642 – Complex scientific research and testing laboratory for command and control systems (hC2)" funded by the Ministry of Defence of the Slovak Republic through the inter – ministerial sub – program 06E0I – Research and development in support of state defence.

References

[1] ALBERTS, David S. et al. 2001. *Understanding Information Age Warfare*. Washington, DC: CCRP Publication Series. ISBN 1-893723-04-6. Available at: https://doi.org/10.21236/ADA386374

[2] ALBERTS, David S.; GARSTKA, John J. and STEIN, Frederick P. 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, DC: CCRP Publication Series. Available at: https://doi.org/10.21236/ADA406255

[3] NATO STANDARDIZATION OFFICE. 2020. *NATO Glossary of Terms and Definitions (English and French)*. AAP-06. Edition 2020. Brussels: NATO.

[4] NATO STANDARDIZATION OFFICE. 2011. *NATO STANDARD APP-6(C): NATO JOINT MILITARY SYMBOLOGY*. Edition C, Version 1. Brussels: NATO.

[5] DEPARTMENT OF DEFENSE. 2008. *MIL-STD-2525C: Department of Defense Interface Standard - Joint Military Symbology*. Washington, D.C.: DoD.

[6] NATO STANDARDIZATION OFFICE. 2021. *NATO STANDARD ADatP-36: FRIENDLY FORCE TRACKING SYSTEMS (FFTS) INTEROPERABILITY*. Edition A, Version 2. Brussels: NATO.

[7] NATO STANDARDIZATION OFFICE. 2017. ADatP-4733: NATO Vector Graphics (NVG). Edition A, Version 1. Brussels: NATO.

[8] NATO STANDARDIZATION OFFICE. 2021. NATO STANDARD APP-11: NATO MESSAGE CATALOGUE. Brussels: NATO.

[9] TOLK, A. 2013. *Engineering Principles of Combat Modeling and Distributed Simulation.* Wiley. Available at: https://doi.org/10.1002/9781118180310

[10] PETERSON, Michael P. 2020. *Mapping in the Cloud*. Guilford Press.

[11] HRŮZA, P.; DUMIŠINEC, I.; ČERNÝ, J. and GALLUS, P. 2024. Use of Information Technology by the Army of the Czech Republic for Command and Control in Operations. In *Science & Military*, 1/2024. pp. 5-14. Available at: https://doi.org/10.52651/sam.a.2024.1.5-14

[12] ENDSLEY, Mica R. 1995. Toward a Theory of Situation Awareness in Dynamic Systems. In *Human Factors*, 37(1), 32–64. Available at: https://doi.org/10.1518/001872095779049543

[13] NOHEL, J.; FLASAR, Z. and STODOLA, P. 2019. Possibilities of Implementation of Friendly Units' Maneuver in the Common Operational Picture. In *Science & Military,* 2/2019. pp. 18-23. ISSN 1336-8885.

[14] PILARSKI, G. 2017. ICT Support of Decision Making Process in the Network of Tactical Command Post. In *Science & Military,* 2/2017. pp. 16-24. ISSN 1336-8885. Available at: https://doi.org/10.1515/9781620973707-030

Maj Dipl. Eng. Marek **BENČÍK**, PhD.
Armed Forces Academy of General M. R. Štefánik
Department of Informatics
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: marek.bencik@aos.sk

Pte 1st class Bc. Dominika **DUDÁŠIKOVÁ**
Armed Forces Academy of General M. R. Štefánik
Department of Informatics
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: dominika.dudasikova@aos.sk

Maj Dipl. Eng. Martin **RÉVAY**, PhD.
Armed Forces Academy of General M. R. Štefánik
Department of Informatics
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: martin.revay@aos.sk

Marek BENČÍK was born in Dolný Kubín, Slovakia in 1988. He received his Eng. (MSc.) at the Armed Forces Academy in Liptovský Mikuláš in 2014. He received his PhD. Degree in Military communication and information systems in 2022. He specializes in programming languages and their applications in command and control systems, as well as in modeling and simulation systems. He also focuses on the transfer and processing of sensor data into command and control systems and their proper representation within these systems. He is currently working as an assistant professor at the Department of Informatics, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš.

Dominika DUDÁŠIKOVÁ was born in Trenčín, Slovakia in 2001. She received her Bc. at the Armed Forces Academy in Liptovský Mikuláš in 2024. She is currently a student at the Department of Informatics at the Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš.

Martin RÉVAY was born in Močenok, Slovakia in 1987. He received his Eng. (MSc.) at the Armed Forces Academy in Liptovský Mikuláš in 2014. He received his PhD. Degree in Military communication and information systems in 2023. His research interests are focused on command and control systems, virtual and augmented reality. He is currently working as an assistant professor at the Department of Informatics, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš.

DOI: https://doi.org/10.52651/sam.a.2026.1.33-41

INTERIOR NAVIGATION USING AUGMENTED REALITY: DESIGN AND IMPLEMENTATION OF A VPS-BASED PROTOTYPE

Martin RÉVAY, Ivo KUĽHA, Marek BENČÍK

Abstract: Indoor navigation in large, visually repetitive buildings is challenging without GPS or wayfinding infrastructure. This paper presents an infrastructure free- augmented reality navigation prototype for complex military interiors, combining ARCore tracking, a Visual Positioning System (VPS), and a navigation mesh from a 3D scan to deliver real-time, first person guidance. Tested in a real scanned facility, the system showed stable localization, smooth AR route visualization, and intuitive use. The results indicate the practical applicability of the prototype in unfamiliar and monotonous environments, as well as its potential applications in military, evacuation, and crisis scenarios. The prototype also establishes a foundation for multi-floor navigation and dynamic rerouting.

Keywords: Augmented Reality (AR); Indoor Navigation; Visual Positioning System (VPS); Visual-Inertial Tracking; Military Facilities; Evacuation Guidance.

1 INTRODUCTION

Navigation within large and complex indoor environments has long been recognized as a challenging problem, particularly in spaces characterized by low visual diversity or architectural monotony. Cognitive studies of spatial orientation show that users tend to lose their sense of direction in corridor networks with repeated structural patterns, which increases cognitive load and complicates decision-making, especially for individuals without prior familiarity with the building [1], [2]. This challenge arises in various types of facilities, such as administrative complexes, hospitals, and university campuses, but it is especially prevalent in buildings where the use of explicit wayfinding signage is limited for operational or security reasons. These conditions are typical for military environments such as operational headquarters, command buildings, accommodation facilities, technical infrastructure, logistics warehouses, and specialized training structures often rely on intentionally uniform architectural layouts, minimal public signage, restricted movement zones, and interior organization that may be unknown to personnel from outside the local unit. As a result, indoor navigation becomes difficult not only for newcomers, external visitors, or maintenance teams, but also for military personnel entering unfamiliar facilities during inter-unit cooperation, inspections, or rapid-response tasks [3].

The need for precise and intuitive indoor navigation is even more critical during time-sensitive or stress-inducing situations, such as building incidents, security breaches, or emergency evacuations. Research in human factors and crisis ergonomics shows that users' ability to interpret static signs and evacuation maps deteriorates significantly under stress. This often results in disorientation, repeated traversal of the same areas, or reliance on heuristic shortcuts rather than spatial reasoning [4], [5]. In such scenarios, an augmented reality (AR) navigation system capable of presenting real-time guidance directly within the user's field of view can reduce ambiguity, shorten reaction time, and support safer movement through unfamiliar environments.

Augmented reality enables navigation cues to be superimposed directly onto the physical scene, eliminating the need to interpret abstract 2D floor plans or search for signage. Combined with VPS, it becomes possible to establish a consistent spatial reference frame derived solely from camera imagery, without requiring additional infrastructure such as radio beacons or sensors. Recent studies suggest that this approach is promising not only for public facilities but also for security sensitive or infrastructure restricted environments where conventional indoor navigation systems cannot be easily deployed [6], [7].

The aim of this paper is to present the design and implementation of an AR-based indoor navigation prototype developed and experimentally tested within the premises of the Armed Forces Academy of General Milan Rastislav Štefánik. Although the academic environment represents a controlled and well-defined testbed, it also exhibits characteristics typical of larger military buildings: extensive corridor networks, limited wayfinding cues, repetitive architecture, and a high turnover of users unfamiliar with the interior layout (students, course participants, visitors). In this sense, the selected use-case serves as a demonstration platform, while the proposed solution is applicable to a broader spectrum of military facilities, including scenarios such as rapid unit movement in unknown buildings, technical inspections, supported evacuation of personnel, and navigation for emergency response teams.

The main contribution of this work lies in demonstrating that the combination of ARCore, VPS, and a navigation mesh can support stable navigation in architecturally uniform military spaces.

The resulting system highlights the potential of AR-based indoor guidance to support both routine movement in unfamiliar buildings and more demanding safety-critical scenarios requiring rapid orientation and reliable route guidance.

2 THEORETICAL BACKGROUND

Indoor navigation is an interdisciplinary research area that connects computer science, psychology, architecture, and spatial planning. In contrast to outdoor environments-where satellite-based positioning systems provide reliable global localization-indoor spaces lack such signals, forcing users to rely on visual cues and mental spatial representations. These mechanisms, however, often fail in environments that are architecturally uniform, monotonous, or entirely unfamiliar.

2.1 Cognitive Aspects of Navigation in Unknown Indoor Environments

Research in spatial cognition confirms that humans rely primarily on visual landmarks, boundary cues, and prominent spatial features when navigating indoors. In environments with low visual diversity, the formation of accurate mental maps becomes significantly impaired, resulting in increased cognitive load and a higher likelihood of navigational errors [8].

Experimental virtual-reality studies further show that even small variations in the number or clarity of visual cues can substantially affect cognitive load and spatial performance. As task complexity increases, users exhibit higher mental effort and reduced navigation accuracy [9].

These insights support approaches that provide egocentric navigation cues directly within the user's field of view, such as augmented reality. This reduces the cognitive demands associated with interpreting abstract maps or static signage.

2.2 Specifics of Military Buildings from a Navigation Perspective

The following architectural and operational characteristics of military facilities make navigating their interior spaces particularly challenging:

- uniform and modular layouts,
- limited or intentionally absent wayfinding signage,
- extensive multi-level spatial structures,
- frequent operational reconfiguration,
- strict security constraints limiting physical navigation aids.

Research on multi-level building navigation demonstrates that strategic visibility, the ability to see key architectural decision points, has a significant influence on navigation success. A lack of such visibility increases route choice errors and reduces wayfinding efficiency [10].

Similarly, comprehensive behavioral models of indoor wayfinding suggest that the complex, highly connected interiors typical of military facilities result in increased uncertainty in decision-making, especially when visual reference points are limited or inconsistent [11].

The importance of spatial visualization in military training and operational environments has been emphasized in prior research, where advanced visualization services were shown to improve spatial awareness and interpretation of complex indoor spaces during joint training activities [24].

2.3 Navigation in Emergency and Evacuation Scenarios

Evacuation scenarios present a distinct set of navigation challenges. Stress, time pressure, reduced visibility, and crowd dynamics impair the user's ability to process static signage or interpret complex spatial layouts.

Studies show that users form more accurate mental representations of escape routes when these are learned through visually rich environments, such as virtual walkthroughs, rather than traditional 2D floor plans [12]. This finding directly supports the use of AR for evacuation guidance, where visual elements are anchored within the real environment.

Modern AR-based evacuation systems demonstrate that combining AR visualization, building models, and dynamic path computation can significantly improve decision-making and evacuation speed, even under conditions of limited visibility or spatial confusion [13]. Other studies confirm that AR-enhanced emergency applications provide effective real-time routing, improved situational awareness, and clearer escape cues in complex multi-story buildings [14].

2.4 Technological Approaches to Indoor Localization

Current indoor localization technologies generally fall into three categories:

a) Radio-based methods – Wi-Fi fingerprinting, bluetooth low energy (BLE) beacons, and hybrid radio systems. These approaches often suffer from signal interference, multipath effects, and environmental instability, leading to inconsistent accuracy, especially in complex buildings, and require dedicated infrastructure [15].
b) Inertial methods – based on inertial measurement unit (IMU) sensors and step-based dead reckoning. While infrastructure-independent, these methods accumulate drift over time.
c) Visual and visual-inertial methods – simultaneous localization and mapping (SLAM), visual-inertial odometry (VIO), VPS. These methods provide precise spatial anchoring without additional

hardware and are naturally compatible with AR visualizations.

Modern AR navigation systems built on ARCore, NavMesh, and real-time mapping have shown high usability and accuracy across varied building types, confirming the suitability of visual-inertial approaches for large indoor structures [16]. Their advantages become particularly evident in emergency scenarios and in environments where infrastructure deployment is limited or undesirable, such as military facilities.

3 METHODOLOGICAL BACKGROUND AND DESIGN DECISIONS

The design of the AR-based indoor navigation system required a series of methodological decisions that considered the technical limitations of mobile devices, the need for infrastructure-independent localization, and the requirement for stable and intuitive spatial guidance in architecturally complex indoor environments. This chapter outlines the key methodological choices that informed the final system architecture, building upon the workflow illustrated in Fig. 1.

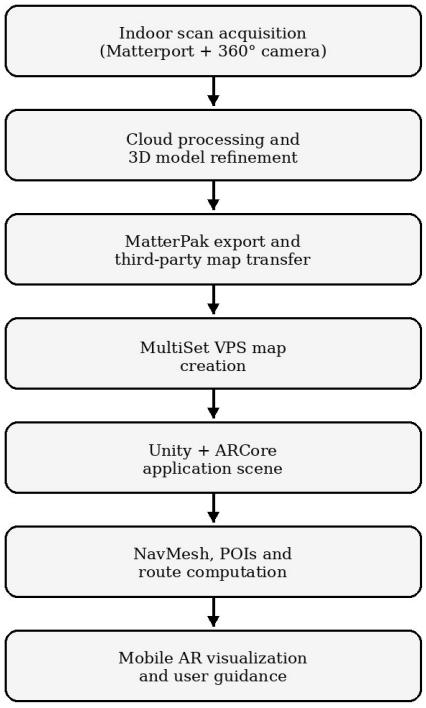

Fig. 1 Proposed workflow of the AR interior navigation system
Source: author.

3.1 Selection of the Localization Approach

Three main categories of indoor localization technologies were evaluated during system design:

a) Radio-based methods (Wi-Fi, BLE, ultra-wideband (UWB)) – radio-based positioning typically requires extensive infrastructure. These methods are sensitive to interference, multipath effects, and spatial configuration changes. Comparative research confirms that their accuracy is strongly affected by building complexity and temporal instability of radio signals, making them less suitable for large institutional and security-restricted environments [14].
b) Inertial methods (IMU, pedestrian dead reckoning (PDR)) – although infrastructure-free, these methods accumulate drift over time, making them unreliable for long-distance indoor navigation without periodic recalibration.
Visual-inertial methods (SLAM, VIO, VPS) – visual-inertial approaches provide high-precision localization without additional infrastructure and are inherently compatible with AR environments. Recent studies show that ARCore combined with VPS delivers reliable relocalization and stable virtual object anchoring in known interiors [16].

Based on these findings, ARCore + VPS was selected as the primary localization method due to its robustness, accuracy, and independence from building infrastructure.

3.2 Design of the Data Processing Workflow

The complete data workflow consisted of four primary stages:

a) Indoor scanning – the interior was captured using the Matterport mobile application and 360° camera. Achieving sufficient scan density and overlap is essential for maintaining visual localization stability, as confirmed by building information modeling – augmented reality (BIM-AR) evacuation research [14].
b) VPS map generation – the MatterPak export was processed in the MultiSet platform to generate a VPS-compatible visual reference model. This map provided the global coordinate frame for subsequent localization.
c) Model alignment in Unity – the VPS model was imported into Unity as the fixed spatial reference for all AR navigation components. This practice is consistent with recommendations for scalable AR navigation systems in large buildings [19].
d) Preparation of the navigational substrate (NavMesh) – the scanned geometry was corrected (closing holes, adding auxiliary surfaces, simplifying irregular areas) to enable generation of a continuous NavMesh. Research demonstrates that NavMesh-based navigation performs particularly well in orthogonal indoor environments typical of administrative and military buildings [17].

3.3 Design of the Navigation Model

The navigation model consisted of three principal components:

- NavMesh Surface – defining walkable indoor areas,
- A* – computing the optimal route,
- trajectory densification – ensuring smooth AR rendering of the navigation line.

A* (pronounced "A-star") is a heuristic search algorithm used to compute the shortest and most efficient path between two points in a graph or mesh.

Thus, A* always chooses the next step that is both closest to the goal and least costly so far. It is widely used in AR and robotics because it is:

- fast,
- optimal,
- computationally efficient for mobile devices.

The system also employed logical destinations to group multiple physical points (e.g., several offices) under a unified semantic destination.

3.4 System Software Architecture

The system architecture was designed as a four-layer model to ensure modularity, scalability, and clear separation of concerns:

a) Sensor Layer – camera, inertial sensors, ARCore motion tracking.
b) Localization Layer – ARCore VIO, VPS relocalization, transformation into a unified coordinate system.
c) Navigation Layer – destination management, NavMesh route computation, dynamic route updates.
d) Presentation Layer – AR rendering of navigation elements, UI components and direction indicators.

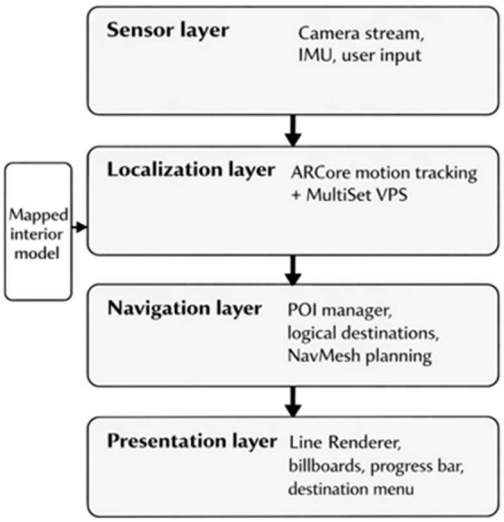

Fig. 2 Layered software architecture of the implemented prototype.
Source: author.

As shown in Fig. 2, this layered structure is important because it allows the system to separate localization from navigation logic and visual rendering. This approach is consistent with modern augmented reality navigation designs. [16].

4 IMPLEMENTATION OF THE PROTOTYPE

This section presents the practical implementation of the proposed AR-based indoor navigation system. The implementation follows the methodological framework introduced in Section III and integrates VPS-based localization, preparation of navigation geometry, NavMesh generation, and the visualization of AR navigation cues in real indoor environments.

4.1 Spatial Data Acquisition and Pre-Processing

We used the Matterport mobile application and a 360° camera to capture the indoor environment. Ensuring sufficient scan density and visual diversity was critical for achieving stable visual localization. Studies on AR and BIM-driven evacuation systems confirm that visually rich 3D models significantly enhance localization performance in complex interiors [14].

After cloud processing, the Matterport pipeline exported the dataset as a MatterPak bundle, which included:

- a textured 3D mesh,
- a point cloud,
- auxiliary spatial metadata.

This dataset was imported into the MultiSet environment, where it was converted into a VPS-compatible visual reference map, enabling ARCore to localize the device within the scanned indoor space.

4.2 VPS Integration in Unity

The VPS model generated in MultiSet was integrated into the Unity engine using the MultiSet Unity SDK. This created a unified global coordinate system, which is essential for stable AR content anchoring. Prior research highlights that spatial coherence between physical and virtual coordinates is a key requirement for reliable AR navigation in large buildings [18].

The imported VPS mesh is depicted in Fig. 3, where it serves as the foundational spatial reference for all virtual navigation elements.

Once localization is initialized, ARCore provides the device's 6-Degrees of Freedom (6-DoF) pose within the VPS coordinate frame. This enables accurate placement of directional arrows, labels, and UI elements directly into the user's live camera feed.

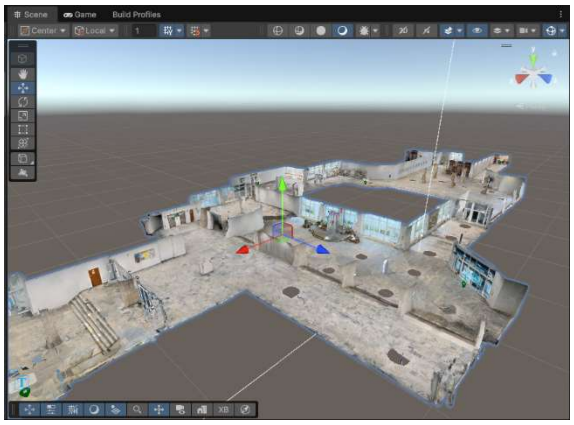

Fig. 3 Imported VPS mesh in the Unity development environment
Source: author.

4.2 Navigation Geometry Preparation and NavMesh Generation

The raw scan included several reconstruction artefacts, such as tripod-induced holes and discontinuous stair surfaces. These imperfections were corrected by adding invisible planar patches and simplifying problematic regions. Similar geometric refinement approaches are described in NavMesh-based indoor navigation studies, where raw 3D scans commonly require structural adjustments prior to path computation [17].

Unity's NavMesh Surface component was employed to generate walkable regions for navigation. The corrected geometry and the resulting NavMesh are shown in Fig. 4.

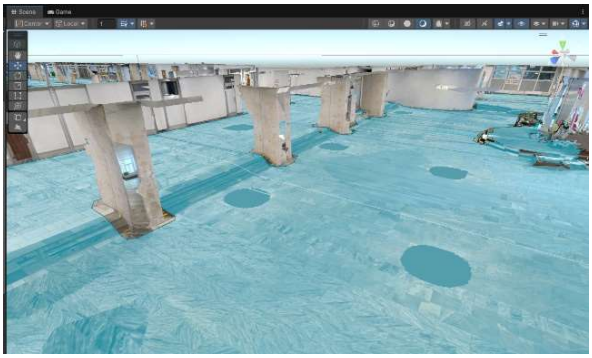

Fig. 4 Correction of the imported mesh and generation of the walkable navitation surgace
Source: author.

NavMesh laid the groundwork for real-time pathfinding using the A* algorithm. This algorithm has proven to be an optimal, computationally efficient solution for route planning in mobile and augmented reality navigation applications [16].

4.3 Navigation Logic and AR Route Visualization

The navigation subsystem comprised:

- management of logical and physical destinations,
- A*-based shortest-path computation over the NavMesh,
- densification of the computed polyline for smooth AR visualization,
- dynamic updates in response to changes in localization confidence.

a) Logical Destinations – a single physical anchor could correspond to multiple semantically meaningful destinations (e.g., multiple offices accessed through a common corridor), minimizing redundant path nodes and simplifying destination management.
b) AR Visualization – the route was visualized using Unity's Line Renderer paired with animated directional textures, generating a clear flow of movement toward the goal. Points of interest were displayed through billboarded labels to maintain readability regardless of viewing angle.

The resulting AR route visualization is shown in Fig. 5.

The interface also includes:

- a searchable list of destinations,
- localization status indicators,
- real-time distance-to-target information,
- route cancellation controls.

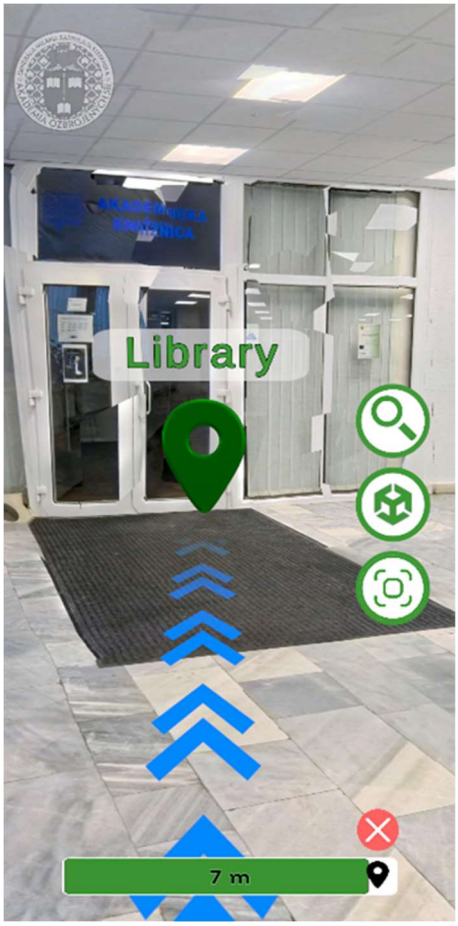

Fig. 5 Route visualization in the Unity environment
Source: author.

5 RESULTS, DISCUSSION, AND OVERALL CONTRIBUTION

This section summarizes the key results obtained during prototype testing, discusses identified limitations, and highlights the practical significance of the proposed AR-based indoor navigation system. The findings demonstrate that the implemented approach is technically feasible, functionally reliable, and well-suited for complex military buildings where conventional navigation support is insufficient.

5.1 Prototype Testing Results

The prototype was evaluated in a real indoor environment modeled from a detailed 3D scan. Testing showed that the system is capable of:

- stable initialization and maintenance of visual localization in visually distinctive areas,
- stable anchoring of AR navigation elements during user movement,
- smooth and intuitive rendering of navigation paths in AR,
- providing clear directional cues to users unfamiliar with the environment.

The system performed best in zones with richer visual features, such as corridor intersections and entrance areas. In contrast, long and monotonous corridors occasionally led to reduced localization stability. This behavior is consistent with the expected limitations of visual positioning systems. However, localization consistently improved when entering visually richer segments.

In addition to qualitative evaluation, basic quantitative metrics were collected to provide an indicative assessment of system performance. Localization stability was observed during navigation along predefined routes, and route completion time was compared against navigation without AR assistance.

Although the evaluation was not designed as a controlled user study, these measurements provide an initial quantitative insight into system behavior and operational feasibility.

Tab. 1 Indicative quantitative evaluation of the prototype

Metric	Observed value
Localization initialization success	approx. 90-95 %
Average localization drift	< 0.4 m
Route completion improvement vs. no AR	approx. 30-40 %
Observed navigation errors	Occasional in monotone corridors

Source: author.

5.2 Identified Limitations and Improvement Opportunities

Testing revealed several practical limitations:

- Monotonous architectural segments: Long, visually repetitive corridors had insufficient feature density for stable VPS operation,
- differences in lighting conditions: Significant deviations between lighting during scanning and testing affected localization confidence,
- limited multi-floor navigation support: Although vertical transitions were technically supported, a more explicit user interface for multi-level guidance is needed.

These limitations can be addressed by expanding visual coverage during scanning, introducing recommended initialization zones, and combining VPS with auxiliary techniques (e.g., markers at critical points). Future development may also include enhanced multi-floor routing and dynamic path recalculation.

5.3 Practical Value in Military Environments

The prototype demonstrated strong potential for deployment in military buildings, which typically exhibit:

- repetitive spatial modules,
- minimal or restricted signage,
- frequent movement of personnel unfamiliar with the layout.

The system can assist new cadets, visitors, technical staff, and operational units in efficiently navigating large and orientation-challenging facilities. The absence of required physical infrastructure makes the approach especially suitable for secure or classified environments.

5.4 Potential for Evacuation and Crisis Scenarios

Even though the prototype was not designed as an emergency solution, its properties indicate high relevance for crisis situations:

- clear egocentric navigation cues displayed directly in the user's field of view,
- reduced cognitive load under stress,
- support for navigation in low-visibility conditions,
- ability to dynamically adjust instructions when route segments are blocked.

These characteristics suggest that AR-based navigation could substantially improve evacuation efficiency and decision-making in high-risk conditions.

5.5 Summary of Contribution

The evaluation demonstrates that the proposed prototype:

- the feasibility and practical relevance of infrastructure-free AR-based indoor navigation,
- provides reliable and intuitive guidance in real architectural spaces,
- addresses a practical operational need in large, complex military facilities,
- offers meaningful value for safety-critical scenarios, including evacuations,
- forms a robust foundation for future development of a fully deployable navigation system.

Overall, the work clearly shows that integrating AR and VPS for indoor navigation is a meaningful and practical direction. It has tangible benefits for military, security, and emergency-response contexts and demonstrates strong potential for real-world deployment.

6 CONCLUSION

This work presented the design and implementation of an augmented reality indoor navigation prototype integrating ARCore, a visual positioning system, and NavMesh-based route planning. The system was developed and experimentally evaluated in a real military-academic environment, demonstrating its ability to deliver intuitive route guidance through direct spatial visualization anchored to the physical interior.

The results indicate that a VPS-based approach can enable accurate localization without requiring additional infrastructure, making it suitable for GPS-denied environments commonly found in military facilities. Although visually repetitive corridors, low-texture walls, and uniform architectural patterns reduce the robustness of visual localization, these characteristics also represent exactly the environments in which users experience the greatest disorientation and where AR guidance provides the highest operational benefit. The prototype therefore illustrates not that monotony improves system performance, but that AR-based navigation remains viable and useful even where environmental conditions challenge visual algorithms.

Testing showed that reliable localization can be achieved when the system is initialized in visually distinctive areas, after which ARCore tracking maintains stable pose estimation throughout the navigation task. The approach proved functional and practical for guiding unfamiliar users, such as cadets, visitors, and personnel entering new operational zones, toward selected destinations in a complex indoor layout. The system's design also suggests broader applicability in military logistics facilities, command buildings, and emergency response scenarios, where rapid orientation is critical and static signage may be insufficient or intentionally minimized.

The main limitations identified include sensitivity to lighting variation, dependence on high-quality mapping data, and reduced localization confidence in visually homogeneous corridors. Future work should therefore explore multi-floor integration, dynamic rerouting under obstructions, hybrid localization combining VPS with inertial or radio-based cues, and enhanced feedback mechanisms for re-localization during emergency movement. Additional evaluation in stress-inducing or evacuation-specific scenarios may further validate the system's usability and situational robustness.

Overall, the findings indicate that AR-based indoor navigation represents a promising capability for military and safety-critical environments, offering improved spatial awareness, reduced cognitive load, and infrastructure-independent guidance in complex interior spaces.

Future work will focus on controlled user studies and structured experiments to further quantify localization accuracy and navigation efficiency.

Acknowledgement

The paper has been supported by the outputs of the research project " NI4200642 – Complex scientific research and testing laboratory for command and control systems (hC2)" funded by the Ministry of Defence of the Slovak Republic through the inter – ministerial sub – program 06E0I – Research and development in support of state defence.

References

[1] ZAFARI, F.; GKELIAS, A. and LEUNG, Kin K. 2019. A survey of indoor localization systems and technologies. In *IEEE Communications Surveys & Tutorials.* (Online). Vol. 21, no. 3, pp. 2568–2599. Available at: https://doi.org/10.1109/COMST.2019.2911558

[2] LIU, H.; DARABI, H.; BANERJEE, P. and LIU, J.. 2007. Survey of wireless indoor positioning techniques and systems. In *IEEE Transactions on Systems, Man, and Cybernetics C.* (Online). Vol. 37, no. 6, pp. 1067–1080. Available at: https://doi.org/10.1109/TSMCC.2007.905750

[3] FARAGHER, R. and HARLE, R.. 2015. Location fingerprinting with Bluetooth Low Energy beacons. In *IEEE Journal on Selected Areas in Communications.* (Online). Vol. 33, no.

11, pp. 2418–2428. Available at: https://doi.org/10.1109/JSAC.2015.2430281

[4] CADENA, C.; CARLONE, L. and CARRILLO, H. et al. 2016. Past, present, and future of simultaneous localization and mapping: Toward the robust-perception age. In *IEEE Transactions on Robotics.* (Online). Vol. 32, no. 6, pp. 1309–1332. Available at: https://doi.org/10.1109/TRO.2016.2624754

[5] GOOGLE. 2025. *ARCore Documentation.* (Online). Available at: https://developers.google.com/ar/develop

[6] MATTERPORT. 2025. *Download the MatterPak™ Bundle.* (Online). Available at: https://support.matterport.com/s/article/Download-the-MatterPak-Bundle

[7] MULTISET. 2026. *MultiSet Developer Documentation.* (Online). Available at: https://docs.multiset.ai/

[8] XU, J.; WANG, S. and FANG, F. 2026. Boundary strategies enhance spatial cognitive efficiency in indoor navigation: A VR-based investigation. In *Buildings.* (Online). Vol. 16, no. 5, article 1001. Available at: https://doi.org/10.3390/buildings16051001

[9] AN, J.; CHENG, B.; RUDYKA, D.; DONATI, E. and FABRIKANT, S.. 2025. EEG-based cognitive load classification during landmark-based VR navigation. In *arXiv.* (Online). Available at: https://doi.org/10.48550/arXiv.2509.14056

[10] GATH-MORAD, M.; GRÜBEL, J.; STEEMERS, K. et al. 2024. The role of strategic visibility in shaping wayfinding behavior in multilevel buildings. In *Scientific Reports.* (Online). Vol. 14, article 3735. Available at: https://doi.org/10.1038/s41598-024-53420-6

[11] FENG, Y. and DUIVES, D.. 2023. Pedestrian wayfinding behavior in a multi-story building: A comprehensive modeling study. In *arXiv.* (Online). Available at: https://doi.org/10.48550/arXiv.2304.11167

[12] SNOPKOVÁ, D.; ŠVĚDOVÁ, H.; KUBÍČEK, P. and STACHOŇ, Z.. 2019. Navigation in indoor environments: Does the type of visual learning stimulus matter? In *ISPRS International Journal of Geo-Information.* (Online). Vol. 8, no. 6, article 251. Available at: https://doi.org/10.3390/ijgi8060251

[13] SHARMA, S. and SUMMITT, A.. 2025. A mobile augmented reality application for indoor emergency evacuation and navigation. In *Electronic Imaging.* (Online). Vol. 37, article ERVR-170. Available at: https://doi.org/10.2352/EI.2025.37.13.ERVR-170

[14] VALIZADEH, M.; RANJGAR, B. and NICCOLAI, A. et al. 2024. Indoor augmented reality pedestrian navigation for emergency evacuation based on BIM and GIS. In *Heliyon.* (Online). Vol. 10, no. 12, e32852. Available at: https://doi.org/10.1016/j.heliyon. 2024.e32852

[15] BEKTESHI, E. and PASCARELLI, C. 2026. Indoor navigation: A comparative study of traditional and machine learning algorithms. In *CEUR Workshop Proceedings.* (Online). Vol. 4044. Available at: https://ceur-ws.org/Vol-4044/short03.pdf

[16] PUTRA, B. S. Ch.; SENAPARTHA, I.K.D.; WANG, J. Ch. et al. 2025. Adaptive AR navigation: Real-time mapping for indoor environment using node placement and marker localization. In *Information.* (Online). Vol. 16, no. 6, article 478. Available at: https://doi.org/10.3390/ info16060478

[17] CALLICO, M.; GIROUDEAU, R.; DARTIES, B. and CARRIÈRE, J. 2025. Indoor navigation: Navmesh applied to indoor graph creation. In *Proceedings of ICORES 2025.* (Online). pp. 221–228. Available at: https://doi.org/10.5220/0013109800003893

[18] AHN, Y.; CHOI, H.; CHOI, R. H. et al. 2024. BIM-based augmented reality navigation for indoor emergency evacuation. In *Expert Systems with Applications.* (Online). Vol. 255, 124469. Available at: https://doi.org/10.1016/j.eswa.2024.124469

[19] LOVREGLIO, R. and KINATEDER, M. 2020. Augmented reality for pedestrian evacuation research. In *Safety Science*. (Online). Vol. 124, 104605. Available at: https://doi.org/10.1016/j.ssci.2020.104605

[20] XU, F. et al. 2024. Improving indoor wayfinding with AR-enabled egocentric cues. In *Applied Ergonomics.* (Online). Article ID. Available at: https://doi.org/10.1016/j.apergo. 2023. 104002

[21] TOMA, M. V.; TURCU, C.O. and PASCU, P. 2025. Evaluating user acceptance and usability of AR-based indoor navigation in a university setting: An empirical study. In *International Journal of Advanced Computer Science and Applications.* (Online). Vol. 16, no. 4. Available at: https://doi.org/10.14569/IJACSA.2025.0160406

[22] UNITY TECHNOLOGIES. 2025. NavMesh Surface Component Reference. (Online). Available at: https://docs.unity3d.com/Packages/com.unity.ai.navigation@2.0/manual/NavMeshSurface.html

[23] HAILU, T. G.; GUO, X. and SI, H.. 2025. Indoor positioning systems as critical infrastructure: An assessment for enhanced location-based services. In *Sensors.* (Online). Vol. 25, no. 16,

4914. Available at: https://doi.org/10.3390/s25164914

[24] HODICKÝ, J. and FRANTIŠ, P. 2010. Visualization services for joint training facility. In *Science & Military*. (Online). 2010, vol. 5, no. 2. Available at: https://www.aos.sk/www/data/uploads/files/Science-Military/sm-2010-2.pdf

Maj Dipl. Eng. Martin **RÉVAY**, PhD.
Armed Forces Academy of General M. R. Štefánik
Department of Informatics
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: martin.revay@aos.sk

Maj Dipl. Eng. Marek **BENČÍK**, PhD.
Armed Forces Academy of General M. R. Štefánik
Department of Informatics
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: marek.bencik@aos.sk

Pte 1st class Bc. Ivo **KUĽHA**
Armed Forces Academy of General M. R. Štefánik
Department of Informatics
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: ivo.kulha@aos.sk

Martin RÉVAY was born in Močenok, Slovakia in 1987. He received his Eng. (MSc.) at the Armed Forces Academy in Liptovský Mikuláš in 2014. He received his PhD. Degree in Military communication and information systems in 2023. His research interests are focused on command and control systems, virtual and augmented reality. He is currently working as an assistant professor at the Department od Informatics, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš.

Marek BENČÍK was born in Dolný Kubín, Slovakia in 1988. He received his Eng. (MSc.) at the Armed Forces Academy in Liptovský Mikuláš in 2014. He received his PhD. Degree in Military communication and information systems in 2022. He specializes in programming languages and their applications in command and control systems, as well as in modeling and simulation systems. He also focuses on the transfer and processing of sensor data into command and control systems and their proper representation within these systems. He is currently working as an assistant professor at the Department od Informatics, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš.

Ivo KUĽHA was born in Michalovce, Slovakia in 2002. He received his Bc. At the Armed Forces Academy in Liptovský Mikuláš in 2024. He is student in Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš. His focus of study is virtual and augmented reality at Department of Informatics.

SCIENCE & MILITARY - WRITER´S GUIDELINES

1. Scientific articles submitted for publishing have to be original, topical and never been published before.

2. Articles have to be written in English language and in accordance with ethical standards. For more details, please visit the website of the Science & Military Journal (https://www.aos.sk/en/article/science-military-ethical-standards).

3. Length of the article should not exceed 6 pages in defined format. Microsoft Word text editor must be used for writing. Articles must be written using Times New Roman, single line spacing and follow the following form: Title -12 point bold capital letters aligned to the center. Full author´s (co-author´s) name – 10 point normal letters aligned to the center. Abstract – 9 point normal letters, extent 3-5 lines. Keywords – 9 point normal letters. The article text – 10 point normal letters. Contact - full author´s (co-author´s) name, affiliation, e-mail – 9 point normal letters at the end of the article. The article text will be written in 2 columns format with a 75 mm column width and 10 mm empty space separating the columns. The first line of each paragraph must be shifted 5 mm to the right.

4. Upper and lower margins must be set to 25 mm, left and right margins to 20 mm. Select mirror margins and set binding margins to 10 mm. The distance between the header/footer and the page margin must be 12,5 mm, while different odd and even pages must be selected.

5. Photographs for publication must be in black-white (not in color) of excelent quality with good contrast.

6. Equations in the text are also to be written using the equation editor. (Equation must be typed in Microsoft Equation, which is an integral part of Microsoft text editor.) They must be numbered. Numbers are to be enclosed in parentheses and aligned to the right margin of a column.

7. Figures, graphs and tables must be included in the text and numbered and must contain description. Figures must be identified as Fig. 1 followed gradually by the figure description. Graphs must be identified as Graph 1 followed by the graph description. Tables must be identified as Tab. 1, followed by the table description.

8. References must be fully and accurately documented (according to ISO 690). References should be quoted in the text in square brackets and listed in the order they have appear in the text.

9. The specimen article that can be found on the web-site: https://www.aos.sk/en/article/science-military-for-authors can be used as an example of the correct format.

10. The editorial board will consider submitted articles in the next scheduled meeting. If it decides to include the article in the next issue it submits the manuscript to the editors for the peer review. The final version (before printing) will be sent to the author for the final revision. The authors are fully responsible for the level of language.

11. Contributions in A4 format edited according to the specimen article should be submitted in electronic form to the Editorial board.

12. The deadlines for the delivery of the articles in calendar year are: March 1 and September 1.

SCIENCE & MILITARY

No 1 | Volume 21 | 2026

Content

ISSN 1336 – 8885 (print)
ISSN 2453 – 7632 (online)