



*The 20<sup>th</sup> International Scientific Conference*  
**“DEFENSE RESOURCES MANAGEMENT  
IN THE 21<sup>st</sup> CENTURY”**  
Braşov, October 30<sup>th</sup>-31<sup>st</sup> 2025



## **ORGANIZATIONAL CULTURE AS AN ELEMENT OF INFORMATION SECURITY IN THE MILITARY**

**Dionisie CIUBOTARU**

Head of Advanced Distributed Learning Service, Center for Studies and Quality Management;  
Assistant Professor, Department of Communications and Informatics, Faculty of Military Sciences,  
“Alexandru cel Bun” Military Academy

**Abstract:**

*The article explores the essential role of organizational culture in military information security. Beyond technology and regulations, security relies on shared values, norms, and behaviors that guide personnel in handling sensitive information. A strong culture prevents leaks, strengthens resilience against hybrid and cyber threats, and promotes discipline in following security rules. The analysis covers four areas: defining organizational culture in the military, its link to information security, risks from weak cultures, and strategies to reinforce cultural foundations for better information protection.*

**Keywords:** *organizational culture; information security; military discipline; loyalty; leadership; confidentiality; NATO; resilience; ethics.*

### **Introduction**

The contemporary era is characterized by hybrid conflicts, information warfare, and the proliferation of cyberattacks. In this context, information has become a strategic weapon, and its protection represents an absolute priority for the military. However, information security cannot be reduced merely to technical measures or legislation. It is closely connected to the cultural dimension of the military organization, which shapes the level of awareness, responsibility, and discipline of its personnel. Organizational culture, understood as a set of shared values and practices, thus becomes an “invisible shield” against threats, but also a potential source of vulnerability if it is weak or incoherent.

### **1. Characteristics of military organizational culture**

Military organizational culture is characterized by specific traits that provide stability and efficiency in times of crisis. These features are not mere conventions but the result of historical evolution and adaptation to strategic and operational demands. One of the most evident characteristics of the military is the existence of a clearly defined chain of command. Authority is distributed across hierarchical levels, ensuring coherence in decision-making and coordination. In military contexts, decision-making ambiguity can have severe consequences, which is why hierarchy becomes a guarantor of order and operational efficiency.

Discipline represents a fundamental mechanism of cohesion. It implies the willingness of soldiers to execute orders, follow procedures, and assume responsibility even under extreme conditions. Through discipline, the military transforms heterogeneous groups into a unified and coordinated force. Similarly, tradition and symbolism—embodied in uniforms, flags, anthems, ceremonies, and branch-specific customs—strengthen collective identity and transmit to successive



*The 20<sup>th</sup> International Scientific Conference*  
**“DEFENSE RESOURCES MANAGEMENT  
IN THE 21<sup>st</sup> CENTURY”**  
**Braşov, October 30<sup>th</sup>-31<sup>st</sup> 2025**



generations a sense of continuity and belonging. These symbols act as moral and cultural anchors, sustaining the spirit of sacrifice and loyalty to the institution and the nation.

Solidarity among comrades, known as *esprit de corps*, is another central dimension of military culture. It generates cohesion, mutual trust, and the willingness to protect the group, even at the cost of one's life. In operational theatres and crisis situations, this collective spirit becomes decisive for morale and mission success.

A strong organizational culture constitutes a cornerstone of institutional resilience in the military. It manifests in the army's ability to withstand external pressures, hybrid threats, and psychological challenges. A military institution that possesses a well-established culture is able to sustain stability, even when confronted with significant military, political, or social crises. Shared values and norms function as an invisible shield that reduces vulnerability to external instability.

## **2. NATO, the European Union, and security culture**

Within NATO, the concept of security culture occupies a main place in strategic documents. The Alliance highlights that true security relies not just on sophisticated technology or infrastructure, but also on a strong organizational culture embraced by everyone involved. This is particularly relevant for the protection of critical infrastructures and operational data, where even a minor human error can compromise the entire security chain.

NATO has developed awareness and training programs for both military and civilian personnel, focused on the importance of individual behavior and collective responsibility. All members should treat security as a personal responsibility, not just an institutional requirement.

Similarly, the European Union, within its Common Security and Defence Policy, places strong emphasis on developing cyber resilience. Through the European Union Agency for Cybersecurity (ENISA) and initiatives such as the NIS2 Directive, member states are required to adopt security measures grounded in an initiative-taking organizational culture. Western military organizations have implemented compulsory training for all ranks, conducted simulation exercises like red team versus blue team drills, and launched internal awareness initiatives that use actual case studies to demonstrate the impact of negligence.

These NATO and EU initiatives demonstrate that information security is not merely a technical concern but an integral element of organizational culture. Armies that successfully internalize these values across all levels—from enlisted personnel to general staff—are more resilient, better prepared to counter hybrid threats, and more capable of protecting both their people and critical infrastructures.

## **3. Challenges and contemporary risks**

One of the major challenges facing modern militaries is the persistence of traditionalist mentalities that regard recent technologies with skepticism or treat them superficially. Bureaucratic rigidity and the attachment to “old ways of doing things” can delay the implementation of digital security measures, leaving institutions vulnerable to fast-evolving cyber and information threats. Another significant risk lies in underestimating the impact of social media and personal communication technologies. Numerous soldiers view online activity as innocuous, yet they may not recognize that sharing photos, remarks, or their whereabouts can inadvertently disclose vital details about current missions. This lack of awareness turns the digital sphere into fertile ground for adversaries exploiting even minor human errors.

Some military organizations may hide security incidents to avoid penalties or damage to their reputation. This “culture of silence” is extremely dangerous, as it allows vulnerabilities to persist. Conversely, a “culture of reporting,” where personnel are encouraged to promptly disclose any



*The 20<sup>th</sup> International Scientific Conference*  
**“DEFENSE RESOURCES MANAGEMENT  
IN THE 21<sup>st</sup> CENTURY”**  
**Braşov, October 30<sup>th</sup>-31<sup>st</sup> 2025**



deviation or incident—no matter how minor—fosters trust and enables swift risk mitigation. Leadership is crucial in this regard, as the way superiors respond to such reports determines whether openness or concealment prevails.

#### **4. Case studies and lessons from modern conflicts**

Contemporary conflicts offer concrete examples of how culture influences information security. Cultural and behavioral factors have played a key role in operational security during the Ukraine war (2022–present).

1. Open-source intelligence indicates that in early 2023, more than 70% of Russian artillery strikes were guided by intercepted frontline mobile phone signals. The Ukrainian Armed Forces also suffered losses when soldiers’ use of popular messaging apps such as **Telegram** and **WhatsApp** inadvertently revealed geolocation data. In **December 2022**, a single phone signal exposure in Makiyivka led to a **missile strike that killed over 80 Russian soldiers**, underscoring the fatal consequences of insufficient security culture.

2. Between 2022 and 2023, NATO monitoring centres identified **hundreds of cases** where soldiers publicly shared operational images on platforms like **TikTok** and **Instagram**, unintentionally revealing troop movements or base coordinates. The lack of awareness regarding digital footprints highlighted cultural gaps in understanding cyber risks within combat units.

3. In multiple coalition missions (2017–2021), social media posts by deployed personnel disclosed **classified locations and mission schedules**, forcing last-minute operational changes. These breaches were not the result of hacking, but of a lack of cultural adaptation to the digital environment.

4. Following these incidents, armed forces implemented structured awareness programs. For example, the **U.S. Department of Defence’s “Think. Type. Post.” campaign (2018)** reduced social media-related breaches by approximately **35%** within two years. Similarly, NATO’s **“Operational Security Culture”** initiative introduced **mandatory digital behaviour courses** for all deployed units starting in **2021**.

These examples illustrate that information security depends not only on technology but, even more so, on organizational culture. Failures in discipline, awareness, or digital responsibility can result in devastating operational consequences, as seen in real-world conflicts. When cultural values, norms, and mindsets evolve in harmony with technological advances, the military becomes more resilient, adaptive, and capable of safeguarding sensitive information. Conversely, when culture lags, even the most advanced systems remain vulnerable to human error and manipulation.

#### **5. Education, technology, and shared responsibility**

Continuous education is a vital pillar for strengthening information security. Regular training adapted to innovative technologies and adversarial tactics does not merely transmit rules—it builds behavioral reflexes. Cyberattack simulations, red team/blue team exercises, and case studies based on real incidents enhance awareness, helping soldiers understand that every action—from using a mobile device to sending a message—has direct implications for operational security.

In today’s military, security is not just the duty of IT personnel or security staff alone. All military personnel should make this practice routine. Creating a culture of shared responsibility means ensuring that all members feel personally accountable. Prompt incident reporting, procedural compliance, and diligence become expressions of active loyalty to the institution and its mission.

Technology, when used intelligently, can reinforce organizational culture. Artificial intelligence and big data analytics allow real-time monitoring of informational risks and the identification of abnormal behaviors. In addition to their technical applications, these tools may be



*The 20<sup>th</sup> International Scientific Conference*  
**“DEFENSE RESOURCES MANAGEMENT  
IN THE 21<sup>st</sup> CENTURY”**  
**Braşov, October 30<sup>th</sup>-31<sup>st</sup> 2025**



utilized within training programmers to demonstrate system vulnerabilities and highlight the potential ramifications of security breaches. In this way, technology becomes an ally of the security culture rather than a mere technical barrier.

In NATO and EU operations, cultural diversity can represent both a challenge and an opportunity. Soldiers from different nations bring distinct traditions, values, and organizational practices. To avoid cultural conflicts and security gaps, it is essential to develop common standards and a convergent organizational culture regarding information protection. Cultural interoperability is developed through collaborative exercises, shared experiences, and the establishment of a standardized organizational language that emphasizes informational discipline and collective accountability.

### **Conclusion**

Organizational culture constitutes the foundation of information security within the military. Beyond technologies, procedures, and regulations, the human factor remains both the greatest vulnerability and the strongest line of defence.

A military institution in which values such as confidentiality, loyalty, and responsibility are deeply internalized by all members will be far more resilient in the face of hybrid threats and information warfare. Organizational culture functions as the first line of defence against error, negligence, or manipulation, providing cohesion and stability even in the most challenging circumstances.

At the same time, it amplifies the effectiveness of technical instruments, transforming rules and security procedures from mere administrative constraints into institutional reflexes shared by all. Military leadership, continuous training programs, and the assumption of collective responsibility are the essential ingredients for building a solid organizational culture. Only under these conditions can the military remain protected not only through technology but through its people—making information security an organic component of military identity.

### **References:**

- [1] Spidalieri, F., and McArdle, J., Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The Role of Cybersecurity Education in U.S. Service Academies, *The Cyber Defense Review*, Vol. 1, No. 1, 2016, pp. 141–164.
- [2] Schein, E. H., *Organizational Culture and Leadership*, Vol. 2, John Wiley & Sons, 2010.
- [3] Martins, J., et al., Information Security Model to Military Organizations in Environment of Information Warfare, *The Institute Ecole Supérieure en Informatique Electronique et Automatique*, Laval, France, 5–6 July 2012, pp. 172.
- [4] Tang, M., Li, M., and Zhang, T., The Impacts of Organizational Culture on Information Security Culture: A Case Study, *Information Technology and Management*, Vol. 17, No. 2, 2016, pp. 179–186.
- [5] Leenen, L., and Jansen van Vuuren, J. C., Framework for the Cultivation of a Military Cybersecurity Culture, *Proceedings of the 14th International Conference on Cyber Warfare and Security (ICWS 2019)*, Stellenbosch, South Africa, 2019.