Overall, the results confirm the relevance of resilience-oriented psychological support as a key factor in sustainable educational development and justify its broader implementation within institutional frameworks of teacher training, professional development, and organizational support in education.

References

1. Bonanno, G. A. (2004). Loss, trauma, and human resilience. American Psychologist, 59(1), 20–28. https://doi.org/10.1037/0003-066X.59.1.20

2. Hobfoll, S. E. (2001). The influence of culture, community, and the stress process. Applied Psychology, 50(3), 337–421. https://doi.org/10.1111/1464-0597.00062

3. Maslach, C., Schaufeli, W. B., & Leiter, M. P. (2001). Job burnout. Annual Review of Psychology, 52, 397–422. https://doi.org/10.1146/annurev.psych.52.1.397

UDC 004.056:316.774:355.01

Social Engineering in Wartime: Manipulation of Human Behavior in the Information Domain

Olha Haborets
Donetsk State University of Internal Affairs, Kropyvnytskyi
https://orcid.org/0000-0001-7791-6795

Abstract. *The article examines social engineering as a critical instrument of influence in contemporary armed conflicts, where human cognition becomes a primary target within the information domain. Wartime conditions intensify psychological vulnerabilities and facilitate manipulation through digital communication platforms. Social engineering is analyzed as a systemic component of information warfare and a significant challenge to information and national security.*
Keywords: *social engineering, information warfare, psychological manipulation, information security, human factor.*

Social engineering in wartime constitutes a complex socio-technical phenomenon in which human cognition becomes a primary battlefield within the broader information domain. Modern armed conflicts increasingly unfold in environments where digital communication, social media platforms, and instant messaging services mediate not only personal interaction but also military coordination, humanitarian logistics, governance, and public communication. Under such conditions, the human factor emerges as both an enabler of resilience and a point of systemic vulnerability. Social engineering exploits this duality by deliberately manipulating perception,

decision-making, and behavior, thereby enabling adversaries to achieve strategic objectives without necessarily breaching technical defenses.

From a theoretical perspective, wartime social engineering is grounded in cognitive psychology and behavioral economics, particularly in the study of heuristics and biases that govern human judgment under stress. Fear, time pressure, ambiguity, and perceived authority significantly reduce analytical processing and increase reliance on intuitive decision-making. In wartime, these factors are not incidental but structural: populations operate under constant threat, institutions function in crisis mode, and individuals are compelled to act rapidly with incomplete information. Adversaries systematically leverage these conditions through carefully constructed narratives, impersonation tactics, and emotionally charged messages designed to trigger compliance, disclosure, or inaction. Consequently, social engineering becomes a force multiplier that allows limited resources to generate disproportionate operational effects.

Unlike peacetime cybercrime, wartime social engineering is rarely confined to financial gain. Its objectives are multidimensional and strategically aligned with the logic of hybrid warfare. These objectives include unauthorized access to sensitive information, disruption of command-and-control processes, manipulation of public opinion, demoralization of civilian populations, and erosion of trust in state institutions. By compromising individual accounts or persuading individuals to disseminate false or sensitive information, adversaries can indirectly influence military operations, humanitarian response, and political decision-making. The manipulation of human behavior thus operates at the intersection of cybersecurity, psychological operations, and strategic communications.

A defining characteristic of wartime social engineering is its adaptive integration with digital infrastructures. As communication rapidly shifts toward encrypted messengers, cloud-based collaboration tools, and decentralized platforms, attackers adjust their techniques accordingly. Rather than attempting to defeat cryptographic protections, they exploit legitimate platform functionalities and social norms of cooperation. Device pairing requests, document-sharing invitations, emergency coordination messages, and verification prompts are repurposed as vectors of deception. These tactics are particularly effective in environments where rapid onboarding of volunteers, ad hoc teams, and interorganizational cooperation is necessary, as formal verification procedures are often relaxed in favor of operational speed.

The informational context of war further amplifies the effectiveness of social engineering through the convergence of cyber manipulation and disinformation. Compromised accounts and impersonated identities serve as credible sources for spreading false narratives, operational rumors, or panic-inducing messages. This blurring of boundaries between technical compromise and psychological influence undermines epistemic security—the ability of individuals and societies to distinguish reliable information from deception. Over time, such manipulation degrades collective trust, fosters decision paralysis, and weakens societal cohesion, all of which align with strategic objectives aimed at destabilization rather than immediate destruction.

Technological developments, particularly in artificial intelligence, have introduced additional layers of complexity. Automated text generation, voice synthesis, and synthetic media significantly reduce the cost and expertise required to produce convincing deceptive content. In wartime, where verification windows are narrow and emotional stakes are high, even moderately realistic synthetic artifacts can be sufficient to induce compliance. Importantly, the success of such manipulation does not depend on perfect deception but on plausibility within a constrained temporal and cognitive context. This reinforces the need to conceptualize social engineering not merely as deception but as behavioral steering under pressure.

Addressing social engineering in wartime therefore requires a paradigm shift in security thinking. Traditional awareness campaigns focused on individual vigilance are insufficient in isolation. Effective countermeasures must be systemic, combining technical controls, organizational procedures, and cognitive resilience. Identity-centric security architectures, phishing-resistant authentication mechanisms, and strict access controls reduce the operational impact of successful manipulation. At the organizational level, formalized verification protocols, separation of duties, and authenticated communication channels mitigate the risks associated with urgency-driven decision-making. At the societal level, transparent official communication, media literacy, and trust calibration mechanisms strengthen collective resistance to manipulation without fostering generalized skepticism.

In scientific terms, social engineering in wartime should be analyzed as an emergent property of stressed socio-technical systems rather than as a series of isolated incidents. Its persistence and effectiveness are rooted in structural wartime conditions that cannot be eliminated but can be managed through informed design and governance. Recognizing human behavior as a critical component of the information domain allows for more accurate threat modeling and more resilient security strategies.

Social engineering during wartime represents a strategically significant form of information-domain manipulation that exploits cognitive vulnerabilities intensified by armed conflict and digital dependence. Its effectiveness derives not from technical sophistication alone but from the systematic alignment of psychological influence with operational objectives in hybrid warfare. A comprehensive response requires an integrated socio-technical approach that combines identity security, procedural safeguards, and cognitive resilience at individual, organizational, and societal levels. Only by treating human behavior as a core element of information security can states and institutions reduce the strategic advantages gained through wartime social engineering and enhance overall resilience in the face of contemporary conflicts.

References

1. Габорець, О. А., Лунгол, О. М. Соціальна інженерія як феномен інформаційного впливу в цифровому середовищі. *Національні інтереси України*. 2025. № 11(16). С. 95–104. DOI: https://doi.org/10.52058/3041-1793-11(16).