Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P084-cd

Assessment of Soldiers' Resilience to Cognitive Attacks of Russian Hybrid Warfare

SVAJONE BEKESIENE[1]and DARIUS LELIŪNAS[1]

[1]Research Group on Logistics and Defence Technology Management,
General Jonas Žemaitis Military Academy of Lithuania, Silo 5a, Vilnius, 10322, Lithuania.
E-mail:svajone.bekesiene@lka.lt
E-mail: darius.leliunas@edu.lka.lt

Aspects of modern warfare are moved into the information technology space before kinetic military operations to affect, disrupt, mess up, or influence an adversary's decision-makers. According to researchers, the concept of information threats can be based on the concept of information confrontation – a war without declared front lines, where it is practically difficult or impossible to detect ongoing information operations, but informational and technical, as well as informational and psychological components of informational threats can be distinguished (M. Kitsa et al., 2019).

According to Y. Firinci (2020), as technological progress increases, the impact on the military also increases. Thus, based on the identified means and methods of information warfare, it can be assumed that one of the most effective methods of information warfare is to influence human psychological and cognitive behavior by means of INO and PSO (Z. Modrozejewski. 2018; T. Thomas, 2014).

The goal of this research is to assess the response of a military unit to information threats and the ability of soldiers to identify information threat attacks. The study hypotheses are tested on a sample of 152 soldiers of the military unit. To evaluate the resistance of the military unit to informational threats and to identify the best ways to strengthen the resistance of the soldiers, this study examined: (1) the ability of military unit soldiers to identify information threat attacks; (2) factors that determine whether a military unit is resilient to information threats; (3) informational threats that have the greatest impact on soldiers. The SPSS v29.0 statistical software package was used and the data collected were analyzed by structural equation modeling.

The results of the study showed that respondents react differently to information threats depending on their experience and education. The simulation results allow us to assume that properly prepared soldiers of a military unit are able to identify information threats and take countermeasures, that is, manage the effects of the information environment. The ability to purposefully train personnel and apply preventive measures would increase the resistance of a military unit to informational threats.

Keywords:Hybrid warfare,resilience,military preparedness,reliability,multidimensional database.

References

1. Y. Firinci, International Journal of Politics and Security, 94-126 (2020).
2. M. Kitsa and I. Mudra, Вісник Львівського університету. Серія журналістика, (45) (2019).
3. Z. Modrozejewski, Obrana a strategie, 18(1), 113-130 (2018).
4. T. Thomas, *Journal of Slavic Military Studies*, 27(1), 101-130 (2014).