Information warfare in the 21st century: soldiers' resistance to information threats

S. Bekesiene

General Jonas Zemaitis Military Academy of Lithuania, Silo 5a, LT-10322 Vilnius, Lithuania;
svajone.bekesiene@lka.lt

ABSTRACT

During the last decade, not only NATO and the European Union are increasingly faced with the manifestations of information warfare. Therefore, researchers paid a lot of attention to the analysis of phenomena related to resistance to informational threats, the concept of emerging threats. The scholars investigated informational balance of power to provide a description of the concept of informational threats (Theohary, 2018). These investigations helped to presented information warfare tools applied in the information environment (Fridman, 2019; Libicki, 1995), to describe influence operations (Zachary et al., 2021) and present a model of resilience principles (Gibson 2010). Moreover, after studying the informational confrontations of the Russian Federation, and the tools of hybrid warfare, the researchers rightly named these informational threats as informational warfare carried out by Russia (Kitsa et al., 2019; Pocheptsov 2018; Firinci 2020).

Informational threats are not a new challenge for the Lithuanian state, because during the period of independence, after the collapse of the Soviet Union, the Russian propaganda and disinformation machine was operating at full capacity in order to denigrate the Republic of Lithuania, Lithuanian history, resistance and state identity. Based on the assessment of threats to national security (available at https://www.vsd.lt/wp-content/uploads/2021/03/2021-LT-el_.pdf), the Russia purpose was to discredit the name of Lithuania in the international community due to the history of the Republic of Lithuania, NATO and EU membership. Russia seeks to use diplomatic missions, news agencies, international companies, diasporas and student organizations to spread its propaganda. Although information threats are more focused on society, but considering the tools used by information warfare, it can be said that the tools used by information warfare are methods of military doctrine. In addition, informational effects can be directed at friendly, neutral, and hostile country audiences in order to publicize beneficial reforms and programs with the goal of influencing society (Zachary et al., 2021).

Due to the transfer of Russia's double information war to the information space and information psychological areas, it is necessary to take into account the existing technical and psychological factors of the Russian information war spreading in Lithuania, which influence not only the society but also for the militaries who are serving in the army. According to researchers (Franke, 2015), the use of Russian information warfare is aimed at:

- disinformation and deception of the enemy (informational – psychological attack);
- the psyche of the enemy using special means (psychotropic attack);
- computers of the enemy's command and control system (computer attack).

Taking into account the goals and concept of Russian information warfare, it can be seen that the methods of Russian information warfare do not differ much from NATO's doctrine of information warfare. Also, must be mention that Russia is the most aggressive and hostile towards the NATO alliance bloc and Lithuania, which, by the way, is geographically closest to Russia. Therefore, it is obvious that the Lithuanian Army is constantly surrounded by an informational threat field, and informational threats against Lithuania can be formed on a specific basis, that is, geopolitical, historical, and Russian-speaking people living in Lithuania. Notable, the public opinion formation is reflected in the Lithuanian army, the attitude and sentiments about geographical and domestic politics, and it is also transferred to the soldiers' mindset and general informational perception of the situation, which creates an unwanted threat to national security. Today, the Lithuanian army is faced with various forms of information warfare, and in its environment, another concept of information threats is undoubtedly evident - the recognition of the spread of positive, neutral and negative information that can be broadcast from a state position and carry a good attitude.

Despite the fact, that Lithuanian scientists have studied the resilience of the army (Žilinskas, 2017) and distinguished the elements of hybrid threats (Bajarūnas et al., 2018), the novelty of this work is based on the fact that in the 21st – century hybrid threats are a daily occurrence and their dynamics are constantly changing, so it is important to constantly monitor this phenomenon. Moreover, considering Lithuania's geographical situation, in order to increase the army's resistance to hybrid threats, it is necessary to constantly educate not only the public, but also the soldiers. There is still a great lack of more detailed research that would reveal the impact of information threats on soldiers serving in the Lithuanian army, and would help to answer whether the soldiers' resilience is sufficiently developed. Therefore, taking into account all of the above, the purpose of this study is to determine the critical impact of information threats on soldiers serving in the Lithuanian army and to assess the resistance of soldiers to information threats.

KEYWORDS
Information warfare; electronic warfare; psychological warfare; cyberwarfare; information threats; soldiers' resistance.

REFERENCES

Bajarūnas, E., Keršanskas, V. (2018). Hibridinės grėsmės: turinio, keliamų iššūkių ir priemonių. p. 127–172. Retrieved from https://etalpykla.lituanistikadb.lt/object/LT–LDB–0001:J.04~2018~1546411321557/
Fridman, O. (2018). Russian "Hybrid Warfare." Russian "Hybrid Warfare," September. p. – 16. https://doi.org/10.1093/oso/9780190877378.001.0001
Firinci, Y.(2020). "Countering Psychological Operations and Deceptions That Indoctrinate AntiIslam Hate and Violence". International Journal of Politics and Security, p.94-126
Franke, U. (2015). War by non-military means. Understanding Russian information warfare. p. 23 – 25. Retrieved from http://johnhelmer.org/wpcontent/uploads/2015/09/Sweden-FOI-Mar-2015-War-by-non-military-means.pdf.
Assessment of Threats to National Security. – Vilnius: VSD, 2021, p. 11. Retrieved from https://www.vsd.lt/wp-content/uploads/2021/03/2021-LT-el_.pdf
Gibson, C. A., Tarrant, M. (2010). A conceptual Models approach to organisational resilience. The Australian journal of Emergency Management, 25(02)
Kitsa, M., & Mudra, I. (2019). Інформаційний Захист: Історіографія, Визначення, Механізми Впровадження. p. 5-9. Retrieved from http://publications.lnu.edu.ua/bulletins/index.php/journalism/article/view/9973
Libicki M. (1995) What is Information Warfare? Washington: National Defense University. Institute for National Strategic Studies. Center for Advanced Concepts and Technology, DC, p. 1 – 85.
Pocheptsov, G. (2018). Cognitive Attacks in Russian Hybrid Warfare. Information & Security: An International Journal, 41, 37–43. https://doi.org/10.11610/isij.4103
Theohary, C. A. (2018). Information Warfare: Issues for Congress. Information Warfare, p. 2–19. Retrieved from http://files/218/Theohary
Zachary, D., Gac, F., Rager, C., Reiner, P., & Snow, J. (2021). Strategic Latency Unleashed - The role of technology in a revisionist global order and the implications for special operations forces. Center for Global Security Research Lawrence Livermore National Laboratory, p. 101. Retrieved from https://www.osti.gov/servlets/purl/1782516
Žilinskas, R. (2017).Valstybės atsparumas išorinėms hibridinio pobūdžio grėsmėms: hipotetinis modelis. Politologija, Nr. 3 (87), Vilnius. p. 45.