Abstract

The aim of this thesis is to examine the risk of the Czech Army not being properly secure on social networks, the behaviour of its uniformed members and their positive identification of social networking sites. The Russian aggression in the Ukraine and the hacking of Czech medical facilities have once again brought up the importance of cybersecurity and the role that it plays in the modern world, with the human factor being positively identified as the weakest link in security.

This case study seeks to define the ideal types of soldier behaviour on social media and to analyse the potential risks that each type poses. To this end, this thesis first presents information necessary to fully understand the vast topic of cybersecurity on social media. Next, it defines several ideal types and their building blocks, in order to categorize the social media accounts of soldiers it later analyses. The author concludes that each defined ideal type has inherently problematic behaviours associated with it and carries with it a level of risk for the Army of the Czech Republic. However, the present user and family member ideal types were found to be the riskiest.

Key words

OSINT, SOCMINT, NATO, Czech Armed Forces, Cybersecurity, Security, Social media, Ideal type analysis, Social engineering

Title

The insecurity of members of the army of the Czech Republic on social networks