Róza Számadó: Analysing cybersecurity and online capabilities of local governments, considering questions of developing the human factor.

Summary

Nowadays ICT tools, the internet are intertwined with the modern world and all aspects of life. This change has taken place abruptly, almost unnoticed. Security studies, in general information security as a discipline has undergone dynamic progress. Organisations of the public sphere - especially local governments - are slow to react to technological and citizens' expectations; organisational operation and organisational culture are slow to react by nature. The vulnerability of central and local governments to information security events and incidents has increased significantly in the past decades.

The research focus of my doctoral dissertation is the analysis of online presence and cybersecurity capabilities of local governments, taking into special consideration the significance of the human factor. In information society, changes in citizens' expectations and meeting information security challenges pose a significant challenge to local governments - in addition to accomplishing their extensive tasks. The complex security approach of information society originates from the interpretation of the people-technology-environment system as a whole. From these three elements, in my paper, I put the emphasis on the human factor. In my research I investigated whether a system of awareness-raising, education and cooperation can be formed that could help local governments meet citizens' and cyber security expectations.

In order to fulfil desired research ambitions, beyond cybersecurity questions, I also examined issues related to regulation, and consequently the character of municipal operation and the structure of local governance. In my research I aimed at achieving the complexity of theoretical correlations and practical application. The main purpose of reviewing literature and documents describing regulatory practices was to support empirical research and to place the results in the system. The attitudes, capabilities and practices of local governments regarding cyber security - based on the known theoretical and regulatory framework - were assessed through an online survey, whose results were also subjected to mathematical statistical analysis. I used factor and cluster analysis to explore the characteristics of online capabilities of local governments using data from the Ministry of Interior's nation-wide municipal data collection. Interpretation of the results and explanation of the main issues took place in a focus group interview.

Research results indicate that information security awareness of local governments is very low, which carries great risk considering cybersecurity trends, directions and this technological progress. The quick development of technology constantly increases vulnerability, making complete security impossible. As a result, prevention and improving resilience should be in focus, in which the individual is a key element. Critical attention should be given to the training, awareness-raising and motivation of officials, especially of executives by using a wide range of supporting toolsets. In order to use resources optimally, the possible benefits of horizontal and vertical cooperation and coordination between stakeholders should be reaped. Moreover, government organisations in cybersecurity need to regularly prepare short, comprehensible, online accessible guides for local governments about cyber threat incidents; learning materials improving cyber defence, cybersecurity awareness that can be processed through the method of e-learning and self-learning.