

## Counterforces and detection to disinformation

T. Sederholm, S. Sommarberg, M. Kaarkoski, P. Koistinen, A-M. Huhtinen

Department of Leadership and Military Pedagogy, National Defence University, Helsinki, Finland

[teija.sederholm@mil.fi](mailto:teija.sederholm@mil.fi)

[silvia.sommarberg@mil.fi](mailto:silvia.sommarberg@mil.fi)

[miina.kaarkoski@mil.fi](mailto:miina.kaarkoski@mil.fi)

[pekka.koistinen@mil.fi](mailto:pekka.koistinen@mil.fi)

[aki.huhtinen@mil.fi](mailto:aki.huhtinen@mil.fi)

### ABSTRACT

Cognitive warfare uses our minds as a battle-space. The operations are behaviour-centric targeting to change people's and decision-makers' mindset. Ukrainian war has demonstrated the importance of information space as one of the domains at the war. This leads us to the fact that a vital part of modern national security is the capability of public authorities to detect and to counter disinformation and other intentional efforts of malicious information influencing. A vital part of modern day national and information security is the capacity of public authorities to detect and counter disinformation, and other intentional efforts of malicious information influencing. In order to succeed at detecting and countering disinformation, public authorities need to improve their situational awareness at the information battlefield. Furthermore, countering disinformation and other malicious information influencing usually includes communicating fact-based information to citizens. It is essential that both military and other public authorities can communicate clearly, on time, and in constructed manner when a possible crisis occurs. Information resilience is a relatively new, but an extremely important element of the national preparedness system. It refers to the notion that in a crisis situation, it is essential that citizens receive and understand the government's official information quickly and accurately. And then reconsider their behaviour accordingly.

As a part of the IRWIN-project (Information Resilience in A Wicked Environment) we have studied the challenges public authorities face when communicating on disinformative and complex spaces such as social media. In addition, we have analysed public authorities' own experiences as targets of disinformation. These studies show that public authorities face major challenges in detecting and countering malicious information influencing as well as in communicating effectively on social media. The results show that the authorities felt open decision-making processes, as well as the transparency and openness of their organizations, factors that render them vulnerable to disinformation. More coordinated and top-down organised strategies on how to detect and counter disinformation are essential while developing improved situational awareness. Our aim is to present both some internationally used methods of counterforces and our findings during the project.

### KEYWORDS

communications; disinformation; national security; public authorities; social media

### Acknowledgements

This study is part of a research project funded by the Academy of Finland.