MEDIA – (DIS)INFORMATION – SECURITY

What is information warfare?

Information warfare is an operation conducted in order to gain an information advantage over the opponent. It consists in controlling one's own information space, protecting access to one's own information, while acquiring and using the opponent's information, destroying their information systems and disrupting the information flow. Information warfare is not a new phenomenon, yet it contains innovative elements as the effect of technological development, which results in information being disseminated faster and on a larger scale.

Defence Education Enhancement Programme (DEEP)

deepportal.hq.nato.int

Awareness of information warfare

At present, interest in information warfare has significantly increased in connection with the Russian-Ukrainian conflict and the annexation of Crimea by Russia in 2014. Russia has been influencing the Ukrainians and the international community in order to promote its own version of events. This was achieved using both traditional media controlled by the Russian authorities and social media, which were a field of operation of the troll factories.

Cyberwarfare

Cyberspace and the related area of new technologies provide an important field for information warfare. Cyberwar activities may consist of cyber attacks, destroying information systems of the opponent, but these may also involve so-called social cyber-attacks, by creating in people's minds a specific image of the world, consistent with the goals of the information warfare conducted by a given country.

Information war over the Internet

The Internet enhances and expands the possibilities of data acquisition, information defence and information disruption, and makes it easy to reach both the citizens of a given country and the international community. Given the speed of communication, wide coverage and low cost of (dis)information campaigns, social media play a crucial role. Social networking sites are also a valuable source of information on the target groups to which (dis)information activities are to be addressed. Information warfare over the Internet uses, among others:

- Troll factories – entities employing people who post comments on the Internet in line with the goal of the ordering party, using fake profiles in social media.
- Bots – programs sending out messages automatically, e.g. in response to the appearance of a keyword.
- Fake news – messages intended to mislead media users.

The journalists' perspective

Media not only report on war conflicts, but they also become the targets of attacks involving, for example, disinformation through the dissemination of fake news. Journalists must be extremely careful in verifying information related to international relations, as the messages they receive may be part of disinformation activities. Another problem is often related to the hacking of websites whose profile is in opposition to the activities of the state conducting information warfare.

The perspective of media users

Media users become victims of information warfare conducted using both the so-called traditional media and the Internet. The signs of propaganda and disinformation are present in numerous media messages, including traditional media as well as social media. Media users are becoming increasingly aware that they are the objects of (dis)information activities aimed at affecting their perception of reality. With growing distrust towards information appearing in official circulation, Internet users are turning to alternative sources of information, including civil media. An important element of individual resistance to propaganda and disinformation is to escape the "information bubble" ("echo chamber", a situation of a restricted access to information other than that those provided by algorithms based on the user's previous activity) by diversifying the sources of information and acquiring information other than that suggested by algorithms regulating social media.

Bibliography

Aro, J. (2016), *The Cyberspace War: Propaganda and Trolling as Warfare Tools*, European View, (15), 121–132.

Ohlin, J.D., Govern, K., Finkelstein, C.O. (Eds.) (2015), *Cyberwar: Law and Ethics for Virtual Conflicts*, Oxford University Press, Oxford.

Macdonald, S. (2006), *Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations*, Routledge, London – New York.

Thomas, T. (2014), *Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?*, The Journal of Slavic Military Studies, (1), 101–130.

Thornton, R. (2015), *The Changing Nature of Modern Warfare. Responding to Russian Information Warfare*, The RUSI Journal, (4), 40–48.