ACTA UNIVERSITATIS WRATISLAVIENSIS
No 3824

Studia nad Autorytaryzmem i Totalitaryzmem 39, nr 4
Wrocław 2017

DOI: 10.19195/2300-7249.39.4.5

PETR KOVANDA
The University of Defence in Brno, Czech Republic

Possibilities of social media in information operations

Introduction

The current century is full of conflicts whose nature is fundamentally different from the wars that occurred in the first half of the last century. The classic concept of war, when states were fighting against each other, and conflict resolution was in the hands of nations, has become a thing of the past. Conflicts in which armed forces are employed require their solution to include the civilian aspects of the environment. Civilian actors increasingly influence the course of the operation and their failure can completely change the balance of forces on the battlefield if the actors in this environment take the side of the enemy and our armed forces will lose the benefits arising from this environment. Gaining the trust and influence of the civilian environment and fostering a positive image is used by a variety of forms and methods of soft operations. While the fulfilment of the operation's objectives can be achieved using lethal or non-lethal means, it is quite likely that currently and in the future there will be an increased emphasis on the management of Information Operations (INFOOPS). Increased attention to INFOOPS in the planning and conduct of military operations comes from the recognition that we live in an information environment that provides great possibilities to influence certain groups to achieve our goals. Thanks to the growing use of new technologies, the broad masses of people can be to disseminate information and use social media. On the other hand, thanks to the accessibility of these technologies, arise possible threats to be faced.

1. Operating environment

The operating environment can be divided into allied and enemy environments. Between these two environments, there are many players that we can include in the civilian environment. For influencing the civilian environment using social media, you should first define the individual elements. Its individual elements have their own interests that contradict each other and the operating environment creates additional disagreements that considerably affect the operation of the armed forces. The civilian environment can be classified into the following categories. The basic element of the civilian environment is the local population, influenced by their local and religious leaders. Another element that affects by their activities the first group — civilians — are humanitarian organizations. These organizations are divided into governmental and non-governmental organizations, which is further divided into international and local. The interests of humanitarian organizations are determined by their statutes and by entering the individual governments. Here it is necessary to remark that in many cases their status directly excludes cooperation with the armed parties to the conflict. Moreover, other future important elements of the civilian environment are civilian agencies. Workers in civilian agencies will defend the main interests of their employer and it is expected that they will be armed with the basic types of weapons. Any operation in the environment of their interests will have to be discussed and coordinated. All the actors interact with each other and interact, for themselves and get the most benefit from mutual cooperation.

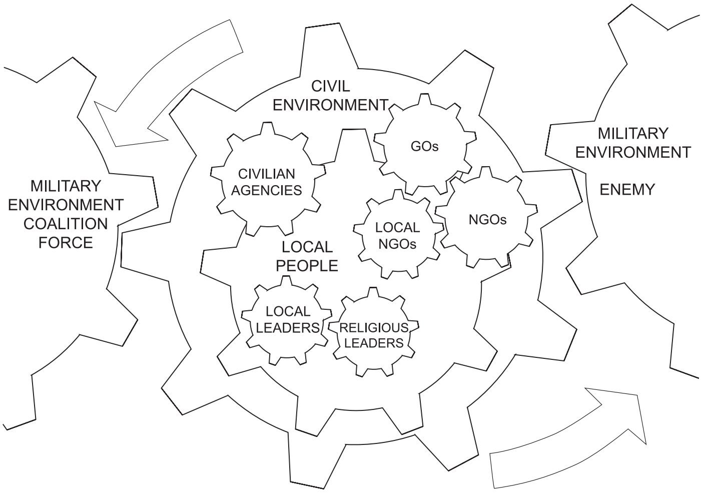

Figure 1. Civil environments

Source: own work.

2. Social media

The social network is a virtual community or profile site, a social network is a website that brings people together to talk, share ideas and interests, or make new friends. This type of collaboration and sharing of data is often referred to as social media.[1] The first step to social networks as we know them today, or Internet-based social networks were sending messages between institutions within the project “ARPANET” (Advanced Research Projects Agency Network), created by the United States Defence Department for communication with research projects between universities UCLA (University of California Los Angeles), SCRI (Stanford Central Research Institute), UCSB (University of California Santa Barbara) and University of Utah.[2] The next step for the emergence of social media as we know it today was the launch of the most famous product “Facebook” on 4 February 2004. Social media is a service that concentrates certain groups of people and keeping in touch with your friends online. Communication that takes place there, can be realized between two completely separate individuals or within the interest group. There is a certain interaction between users — e.g., chats, messages, e-mails, newsgroups. While sharing individual messages, whether in written, visual or audio-visual form, here is to share information that affects the target groups.

Between the basic features of social networking sites, we rank the association of people. This means that people are associating in various social networks for communicating, sharing, presentations of themselves, familiarization with new people, contact with loved ones, etc. Another feature is communication, which mostly takes place in two main ways — private newsgroup messages — public communication.

3. Information operations

The most natural way of integrating social media into military operations is their use in the context of Information Operations (INFOOPS). The definition of Info Ops and information activities is as follows:[3]

— Info Ops is a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding

[1] *Social network*, http://www.computerhope.com/jargon/s/socinetw.htm (access: 31.10.2016.).

[2] The Computer History Museum, SRI International, and BBN Celebrate the 40th Anniversary of First ARPANET Transmission, Precursor to Today’s Internet. Available from: https://www.sri.com/newsroom/press-releases/computer-history-museum-sri-international-and-bbn-celebrate-40th-anniversary (access: 1.10.2016).

[3] *AJP-3.10*: *ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS*, 2009, https://info.publicintelligence.net/NATO-IO.pdf, pp. 1–3 (access: 5.04.2018).

and capability of adversaries, potential adversaries and other NAC approved parties[4] in support of Alliance mission objectives;

— Information activities are actions designed to affect information and/or information systems. They can be performed by any actor and include protective measures.

The INFOOPS aim is to achieve information dominance over the enemy. INFOOPS are thus an umbrella overarching military capabilities, using soft methods to influence the target groups using the information. Between tools INFOOPS according to AJP-3.10. belong:

— Psychological Operation — PSYOPS;
— Presence Posture Profile — PPP;
— Operational Security — OPSEC;
— Information Security — INFOSEC;
— Military Deception — MD;
— Electronic Warfare — EW;
— Physical Destruction — PD;
— Key Leader Engagement — KLE;
— Computer Network Operations — CNO;

Among other military capabilities for which it is appropriate to coordinate are:

— Civil Military Cooperation — CIMIC;
— Public Activities — PA.

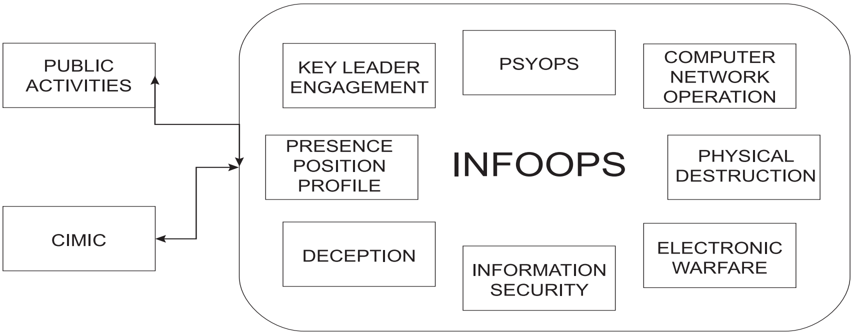

Figure 2. Tools of INFOOPS

Source: own work according to AJP-3.10.

But not all forms of INFOOPS can use social networks. Furthermore, there will be discussed military capabilities that could, within the social media, develop their activities.

[4] NAC-approved parties are those identified in top-level political guidance on NATO information activities. These may include adversaries, potential adversaries, decision-makers, cultural groups, elements of the international community and others who may be informed by NATO information activities.

3.1. Psychological operations

PSYOPS is in many cases mistaken for INFOOPS. This commutation appears to stem from a lack of knowledge of terminology and the fact that PSYOPS is the largest component INFOOPS and many activities are conducted by its tools. The primary purpose of PSYOPS is to influence the attitudes and behaviour of target groups to achieve political and military objectives. For planning and purposeful psychological impact on target groups, PSYOPS is used to the dissemination of information products that are divided into the following groups:[5]

— Audio-visual products;
— Audio products;
— Press products;
— Software products;

If we disregard the traditional dissemination of these products through television and radio broadcasting and distribution of printed media, the era of the Internet opens up a completely new path of distribution. Social media in this area will be in prime position. Their great advantage is fast dissemination. Another reason to use social networking for PSYOPS could be to find target groups. Target groups in social media create spontaneously. It is sufficient just to identify, characterize, and eventually influence the audience/social media users with appropriate PSYOPS products.

3.2. Military deception

Deception is among the oldest military operations that use dissemination of misleading information. Here, the use of social media directly offers. Social networks are often used directly for the coordination and management of the enemy's armed forces. Inserting false orders into this communication gives us the opportunity to influence the enemy's behaviour. Other use of misleading information can be directed against enemy troops with the aim to demoralize them and thereby contribute to the overall victory. In terms of influencing the civilian environment, however, we noted that these activities will be more focused on the elements of the enemy's civilian environment and thus their linking with PSYOPS or CIMIC activities are counterproductive.

[5] *AJP-3.10.1*: *ALLIED JOINT DOCTRINE FOR PSYCHOLOGICAL OPERATION*, 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf (access: 5.04.2018).

3.3. Computer network operation

The aim of the operations in computer networks (CNO) is finding a way to enter the computer network, attack it and extract data. Activities in computer networks are conducted to undermine confidentiality and consistency, the disruption in the availability of computer data and systems. CNO consists of three basic elements.

— CNA (*Computer Network Attack*) — an attack on computers, computer networks and data storage devices or malicious virus code. The goal is disruption, disablement, or performance degradation;

— CNE (*Computer Network Exploitation*) — extraction data from computers and computer networks. The aim is to gain the ability to access, view, copy, or otherwise manipulate data that is stored in the system;

— CND (*Computer Network Defence*) — protection of computer networks are measures to prevent distortion, disclosure, or destruction of its own information located on computers or computer networks.

Although it seems that the CNO only deals with computer networking hardware, with proper coordination of INFOOPS activities, we have a tool that enables using social networking to influence a wide range of target groups. CNO can be used in the distribution of PSYOPS products insertion into the communications of specific target groups of social networks and thus enable their self-dissemination. Of course, this can be done by even inserting a false report under military deception and thereby disorient the enemy group.

3.4. Public activities

Even though public information is not a direct instrument of INFOOPS, it is closely associated with them. Their mutual coordination is necessary to prevent violation of INFOOPS activities and thereby breaking the concept of influencing target groups. Because it is not appropriate to combine Public Activities with activities such as military deception, it is appropriate to create their own profile on social media and put news that will enhance the legitimacy of military operations. The advantage of social networks is the ability to distribute instant messages, which then disseminate by themselves. Here you would use the adage “Speed message — true message.”

4. Use of social media

The possibilities of using social media are extensive for contemporary information operations. We are in possession of an instrument by which both individuals and target groups can be influenced by a military operation. An advantage is the enormous speed with which we can disseminate individual messages, in the form of video and audio. Social media is replacing classic broadcasting channels such as radio and newspapers. The basic possibilities of using social media include:

— Spread rate of the message;
— Focus the message on certain target groups within PSYOPS;
— Using EW smuggling targeted messages into enemy communications;
— For coalition soldiers the opportunity to communicate with family.

5. The threats of social media

On the other hand, social media brings, in addition to benefits, risks that we must not forget. The ability to monitor social networking is also in the hands of a potential enemy. The enemy's intelligence activity is primarily focused on the flow of information and especially on a keyword search. With trained members of the armed forces, information about the beginning of the operation can be found in communication with family members. For example, on March 3, 2010, a military operation to be conducted by the Israeli Defence Forces (IDF) in the Palestinian Territory had to be abandoned. Details of this operation were revealed by an Israeli soldier on his Facebook profile.[6] Opportunities to avoid this is often done by blocking the internet network. However, if the enemy monitors communication on an open social network and reduces it significantly or stops it, we send him clear information that a military operation will take place in the near future.

Another threat to social networks is the direct targeting of members of the armed forces. Members of the armed forces may be attacked by targeted messages that contain personal information about family members. The result is that their morale and willingness to fight will drop significantly. Another group to which the enemy may be affected is the general public — taxpayers whose armed forces are participating in the mission. We have recently witnessed the distribution of videos from individual executions performed by ISIL members.

Other threats to social networks are directly related to the technologies of devices that are used to access the social network. Many members of the armed forces on social networks access their smartphones. These modern devices already include a GPS module, making it easier to locate the device and move its owner. In addition, the phone continually transmits its IMEI — International Mobile Equipment Identity code, which detects it on the network. IMEI information

[6] https://www.novinky.cz/zahranicni/blizky-a-stredni-vychod/193778-izrael-odvolal-vojenskou-operaci-protoze-byla-vyzrazena-na-facebooku.html (access: 5.04.2018).

is stored in the so-called Equipment Identity Register (EIR). If you connect an IMEI to a particular phone, then that is only one step away from observing people.

Conclusion

Social networking has become a phenomenon, not only for young people, but increasingly these mediums are used by all age groups. Social networks are used in marketing to influence the broad masses of the population. Military use of social networks for influencing target groups are still of marginal interest for military officials, as well as on the outskirts of interest for use of information operations that would be mutually coordinated. Social networking brings many benefits on the one hand, and disadvantages on the other. It depends only on the knowledge of commanders and relevant specialists that we use the advantages that using social networks as a part of INFOOPS brings.

Bibliography

AJP-3.4.9 — ALLIED JOINT DOCTRINE FOR CIVIL-MILITARY COOPERATION. 2013. Edition A Version 1. NSA. Available from: http://www.cimic-coe.org/wp-content/uploads/2014/06/AJP-3.4.9-EDA-V1-E1.pdf.

AJP-3.10 — ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS. 2009. Available from: https://info.publicintelligence.net/NATO-IO.pdf.

AJP-3.10.1 — ALLIED JOINT DOCTRINE FOR PSYCHOLOGICAL OPERATION. 2014. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf.

Kovanda, P. 2015. "The relation between military and civilian actors in military operations". In: *The 21st International Scientific Conference Knowledge-Based Organization. Management and Military Sciences*. Sibiu: "Nicolae Balcescu". Land Force Academy Publishing House, pp. 62–65.

Pikner, I., Galatík, V. 2010. "Future operational environment and military concepts". In: *The 16th International Conference The Knowledge-Based Organization management and military sciences*. Sibiu: "Nicolae Balcescu". Land Force Academy Publishing House, pp. 157–162.

POSSIBILITIES OF SOCIAL MEDIA IN INFORMATION OPERATIONS

Summary

Current conflicts are characterized by the changing environment having a considerable influence on military operations. The armed forces must calculate with civilian factors that are increasingly coming to the forefront in conducting operations. It is no longer enough to defeat the enemy using military power, but necessary to stabilize the area of responsibility and incline the local population to be on our side. Influencing the civilian population is conducted mainly by providing information that is disseminated by traditional methods such as radio, television, and print. Dissemination of information is no longer just the domain of the media but comes to the fore via internet communication. Thanks to the development of technologies and especially the availability of Smartphones, social networks are becoming the new phenomena.

Keywords: social media, information operations, psychological operations, influence.

Petr Kovanda
petr.kovanda@unob.cz