 DOI: 10.3849/2336-2995. 28. 2019.03.083-096

Peer-reviewed

Information and Psychological Operations as a Challenge to Security and Defence

Informační a psychologické operace jako výzva pro bezpečnost a obranu

Petra Vejvodová

Abstract: The article focuses on information and psychological operations as a challenge for the security and defence establishments of NATO member states. A conceptualisation of the terms 'information operations' and 'psychological operations' is discussed in the contexts of reshaping the war-and-peace dichotomy, and of resilience and deterrence. It is suggested that these terms suffer from a normative approach to the paradigm of war and peace, and to the use of non-military means. This may lead to the greater vulnerability of security and defence systems in confrontation with an adversary. Also, special attention is paid to the vulnerabilities of security and armed forces, being overlooked in concepts of resilience.

Abstrakt: Článek se věnuje informačním a psychologickým operacím jako výzvě pro bezpečnostní a obranné systémy zemí NATO. Nejprve jsou jednotlivé termíny diskutovány v souvislosti s pojímáním dichotomie válka a mír, a také v kontextu odolnosti a odstrašování. Text upozorňuje na to, že definice pojmů jsou ovlivněny normativním přístupem vůči paradigmatům války a míru a užití nevojenských prostředků. Tato situace vede k vyšší zranitelnosti bezpečnostních a obranných systémů při jejich konfrontaci s protivníkem. Zvláštní pozornost je také věnována zranitelnostem bezpečnostních a ozbrojených složek, které jsou v rámci formulací strategií na zvýšení odolnosti přehlíženy.

Key words: Information Environment; Information Operations; Psychological Operations; Resilience; Security Forces; Vulnerability.

Klíčová slova: Informační prostředí; informační operace; psychologické operace; odolnost; bezpečnostní složky; zranitelnost.

INTRODUCTION

Information operations, psychological operations: two terms very often articulated in the context of hybrid warfare, irregular warfare, information warfare etc. Western democracies and NATO try to define carefully what these terms mean to promote as much transparency as possible. Nevertheless, we suggest that current definitions do not reflect the reality, probably because the Western approach differs from that of the West's adversaries, the ones who actively develop and deploy such operations in the modern age. Therefore, this article discusses and highlights the main issues and weaknesses related to the Western understanding of information and psychological operations, and also reflects on the gap in civil-military affairs. We witness intense discussions about the protection of society against the influence of information and psychological operations, but these reflect only civil society. Military and security representation is missing from this discussion.[1]

1 DIFFICULTIES IN UNDERSTANDING INFORMATION AND PSYCHOLOGICAL OPERATIONS

According to NATO and the US Department of Defense, information operations are defined as '*the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own*.'[2] Information operations are coordinated military activities in an information environment having specifically defined goals. They represent offensive and defensive measures focused on influencing an adversary's decisions, manipulating information and information systems. They also include measures protecting a country's own decision-making processes, information and information systems.

Information operations may affect all three dimensions of the information environment. In the psychological dimension they have potential to influence command and control systems, key decision makers and supporting infrastructure. The physical dimension covers human beings, but also command and control facilities and ICT. What is important is that the physical dimension is not connected only to military or nation-based systems and processes. In the psychological dimension, information operations target the ways information is collected, processed, stored, disseminated and protected.

1 This paper was written under the project Optimisation of Intelligence Activities and Intelligence Institutions in the Changing Environment (OPTIZ9070204510), funded by the Ministry of Defence of the Czech Republic as part of the 'Development of the Armed Forces of the Czech Republic! (907 020) defence research programme.

2 Joint Chief of Staff. *Joint Publication 3-13. Information operations*. [online] 2014 [cit. 2019-04-30]. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

Operations in these dimensions affect the content and flow of information. Last but not least, in the cognitive dimension, information operations influence the minds of those who transmit, receive, respond to or act on information. The cognitive dimension means individuals and groups, their individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, education, mental health, identities and ideologies[3]. Understanding these factors is crucial for developing best operations in order to influence decision makers and produce the desired effect.

Information operations are not only a collection of single information activities. They are a process of integrating the effects of single information activities, together leading to influencing an adversary. Information operations integrate psychological operations (psyops), operations security, information security, deception, electronic warfare, kinetic actions, key leader engagement and computer network operations. All together they target the will of adversaries to fight, their understanding of the situation, and their capabilities.

Information activities aimed at influencing the adversary mainly focus on decision-makers who have the ability to influence the situation. Activities in this case include questioning the legitimacy of political leaders, undermining the morals of the population or the military, polarising society and so on. Information activities to affect the understanding of the situation seek to influence the information available to the enemy for their decision-making processes. They include disseminating disinformation, using military-scale mock-ups to fool the enemy's radar systems, deliberately leaking distorted information, destroying or manipulating information in the opponent's information systems, and so on. The third kind of information activities is to act on the enemy's abilities and try to disrupt his ability to understand information and promote his will. These include disruptions to internet connections, the physical destruction of infrastructure, cyber attacks and so on.

Information operations are sometimes mistakenly referred to as strategic communication. Although these two terms may seem very similar, there are differences between them. Strategic communication is driven from a political, strategic level; its reach and audience are global and it operates only in the cognitive dimension of the information environment. By contrast, information operations are managed from an operational, military level, have a well-defined scope of action and audience, and operate in all three dimensions of the information environment.[4] Strategic communication is thus a broader term to which information operations are subordinate.

In this approach, information operations concentrate information-technical and information-psychological activities during military operations. In this article, we are interested in information-psychological activities, which are often understood as psyops. As was mentioned, psychological operations are defined as one type of activity belonging

---

3 Joint Chief of Staff. *Joint Publication 3-13. Information operations*. [online] 2014 [cit. 2019-04-30]. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

4 DIVIŠOVÁ, Vendula. Strategická komunikace v protipovstaleckých operacích NATO. *Obrana a strategie* [online]. 24(2), 105-118 [cit. 2019-04-30]. ISSN 12146463. Available at: https://www.obranaastrategie.cz/cs/archiv/rocnik-2014/2-2014/clanky/strategicka-komunikace-v-protipovstaleckych-operacich-nato.html.; ŘEHKA, Karel. *Informační válka*. Praha: Academia, 2017. ISBN 978-80-200-2770-2.

to information operations. Allied Joint Doctrine AJP 3-10.1 for psychological operations from 2014 defines psyops as '*planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievements of political and military objectives.*'[5] It is also understood that all actions in the area of operations undertaken by NATO are highly probable to have a psychological impact.

Psychological operations are pre-planned activities using communication methods and other resources aimed at selected target audiences to influence their moods, attitudes, behaviour, perception and interpretation of reality. Thus, by using special methods, it is possible to induce desirable responses in the target population, which in the broader context contributes to the fulfilment of specific political and/or military objectives. Every psychological operation is based on a certain psychological theme (the main, carefully prepared narrative, or ideas). The greater the target audience receptivity, i.e. sensitivity to specific psyops tools, the greater the probability of success of the whole psychological operation[6].

The importance of psyops is based on the belief that the psychological nature of the conflict is as important as the physical. People's attitudes and behaviour affect the course and outcome of the conflict and the nature of the environment in which the conflict takes place. For a well-conducted psychological operation, it is important to know the target audience, its will and motivation. The psyops work with these elements and aim to influence them, weakening the adversary's will, strengthening the target group's commitment, and gaining the support and cooperation of undecided groups.

The poorly defined relationship between information operations and psychological operations is a problem for the definition of psyops themselves. From the logic of provided definitions, psyops help to fulfil the aims of information operations at the information-psychological level of military operations. Aiming at the cognitive dimension of the information environment, psyops influence the perceptions, attitudes and behaviour of the target audience, which should lead to an effect on decision makers. So they are a sub-category of information operations, coordinated through information operations processes. Allied Joint Doctrine AJP 3-10.1 states that psyops are conducted across the

5 NATO Standardization Office. *Allied Joint Doctrine for Psychological Operations AJP 3-10.1.* [online] Brussels: North Atlantic Treaty Organization, NATO Standardization Office, 2014 [cit. 2019-04-30]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf.

6 NATO Standardization Office. *Slovník NATO s termíny* a *definicemi. AAP-06(2016)*. [online] Praha: Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti, Odbor obranné standardizace, 2016 [cit. 2019-04-30]. Available at: http://oos.army.cz/terminologicky-slovnik-aap-6; NATO Standardization Office. *NATO Glossary of Terms and Definitions. AAP-06.* [online] Brussels: North Atlantic Treaty Organization, NATO Standardization Office, 2018 [cit. 2019-04-30]. Available at: http://oos.army.cz/terminologicky-slovnik-aap-6; NATO Standardization Office. *Allied Joint Doctrine for Psychological Operations. Allied Joint Publication – 3.10.1.* Brussels: North Atlantic Treaty Organization, NATO Standardization Office, 2014.

full spectrum of military operations[7]. Here, a first contradiction arises, when we compare the NATO understanding of psyops with the understanding of the Czech army, which sees psyops as „planned and purposeful psychological influence on target groups, carried out in peacetime under a state of external threat to the country, and in wartime"[8]. Based on this, psyops can be conducted both in times of peace and war. In this understanding, psyops erase the dichotomy between peace and war and imply a shift in the understanding of the tasks of the armed forces to the effect that even during peacetime the security and defence establishments needs to be active and conduct operations. But as a sub-category of information operations, psyops should be connected only with military operations – normally undertaken during war. Support for a redefinition of terms comes from e.g. Brangetto and Veenendaal from NATO Cooperative Cyber Defence in their paper, in which they introduce psychological operations as an activity also undertaken during peacetime. They talk about a category of operations they describe as „strategic communication and propaganda[9]" (see Figure 1).

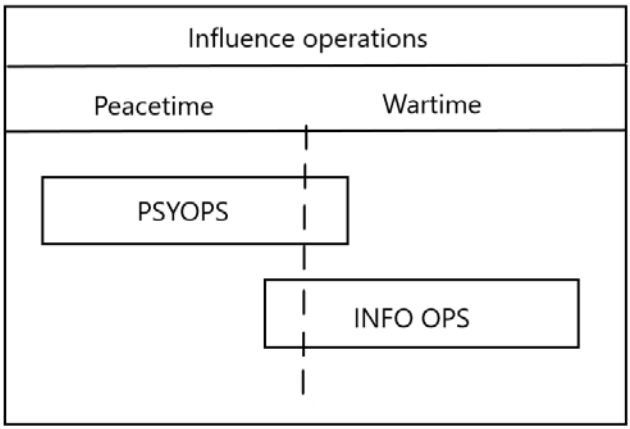

Figure 1: Psyops vs Info ops (modified according to Brangetto and Veenendal)

The intention is clear here, but it causes another terminological confusion when mixing strategic communication and psychological operations that comes from that fact that in NATO terminology psyops are replaced by strategic communication (stratcom). It

7 NATO Standardization Office. *Allied Joint Doctrine for Psychological Operations AJP 3-10.1.* [online] Brussels: North Atlantic Treaty Organization, NATO Standardization Office, 2014 [cit. 2019-04-30]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf.

8 103rd Centre of Civil-military cooperation and psychological operations of the Czech Army. [online] Official website [cit. 2019-04-30]. Available at: http://www.103cp.army.cz/.

9 BRANGETTO, Pascal, VEENDENDAAL, Matthijs, A. Influence Cyber Operations: the Use of Cyberattacks in Support of Influence Operations. *8th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2016.

may be better to say that the definitions of both are the same in principle. On one hand, Allied Joint Doctrine AJP 3-10.1 defines psyops as subordinated to stratcom and fulfilling the goal of supporting the Alliance's aims, policies, operations and activities, including the strategic narrative. On the other hand, psyops are defined by the same principles as stratcom, especially in terms of attribution, credibility, consistency and truthfulness. It is said that psyops have to be based on true information and preserving Alliance credibility, so they are generally attributable to NATO, a partner nation or organisation. Psyops are also nested within the strategic narrative and overall information strategy.[10] This understanding might be problematic. Respectively, psychological operations overlap with strategic communication with an emphasis on the narrative. Nevertheless, in contrast to strategic communication, psychological operations may in theory use disinformation and propaganda and may try to manipulate target audiences with false or misleading information. Like propaganda, psychological operations can be divided into white, grey and black psyops based on the source and accuracy of information, and the methods used. White psyops activities are openly acknowledged by the sponsor. Grey ones do not specifically reveal their sources. Black ones deceive about the source, pretending that it is other than the true one. In these terms, psyops are subordinate to the concept of strategic communication (especially with white psyops), but psyops may go well beyond the frame of principles of stratcom and use dirty measures in order to influence a target audience.

Let's come back to understanding information operations and psychological operations in practical terms and consider what consequences might follow. The contradiction in terms of when to apply such operations (peacetime vs. wartime) has already been mentioned. Western democracies believe that such operations should be associated with military operations only. They also believe that deception, disinformation and propaganda should be avoided as tools to be used during operations. The Western approach builds on the belief that carefully developed narratives can only be effective if the messages are reliable and consistent. The approach also counts on the critical thinking of audiences so that the truthful narrative will win[11]. What is more, using disinformation and deception do not theoretically belong in a democracy's peace-time toolbox at all. As a side effect, this approach prevents us from building a comprehensive, complex and functional approach to psyops, which is needed based on our experience with the Eastern approach to this issue.

As we have seen, Russia and China have adopted integrated and holistic approaches, which include information and psychological operations as tools that can be used both in peacetime and during an armed conflict. This approach stands on the belief that strategic advantage can be reached by using non-military means. Non-military means can

10 NATO Standardization Office. *Allied Joint Doctrine for Psychological Operations AJP 3-10.1.* [online] Brussels: North Atlantic Treaty Organization, NATO Standardization Office, 2014 [cit. 2019-04-30]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf.

11 BRANGETTO, Pascal, VEENDENDAAL, Matthijs, A. Influence Cyber Operations: the Use of Cyberattacks in Support of Influence Operations. *8th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2016.

allow political or strategic goals to be reached without the conflict being escalated into an armed one and officially recognised as such, thus activating an armed response. Eligible non-military means used might be economic manipulation, disinformation and propaganda, and fostering civil disobedience. Influencing the consciousness of the masses is an aspect of the rivalry between different countries.[12] Such an approach then exploits the weaknesses of the Western approach.

Another weakness of the current understanding of information and psychological operations is that it overlooks one important target audience – the security and armed forces, i.e. those responsible for protection and defence and for deploying such operations. The current understanding of operations and preparedness for action focuses on four levels according to who is influenced by whom:

1. Own security/armed forces influencing adversary's general public (both information-technical and information-psychological level);
2. Own security/armed forces influencing adversary's security/armed forces (both information-technical and information-psychological level);
3. Own general public being affected by the adversary (both information-technical and information-psychological level);
4. Own security/armed forces being affected by the adversary (only information-technical level).

What is missing here is a notion of the vulnerability of own security/armed forces being the target audience of information and psychological operations at the information-psychological level (i.e. targeting their hearts and minds). That this is the case is demonstrated in the next section.

2 INFORMATION AND PSYCHOLOGICAL OPERATIONS AGAINST SECURITY/ARMED FORCES

One well-known example are the psychological and information operations undertaken by ISIS against the security forces of their enemy nations. Examples include a 2015 video recording of the brutal burning of a Royal Jordanian Air Force pilot, Moaz al-Kasasbeh, whose F-16 fighter jet was shot down near the city of Raqqa in Syria. The 22-minute video was published on a Twitter account used by ISIS. The pilot died in flames, locked in a cage. The video was used for propaganda, to send out the threatening message that any soldier fighting against ISIS would die a remorseless death. The video was professionally shot, using multiple cameras and following a script, and complemented

12 MONAGHAN, Andrew. The 'War' in Russia's 'Hybrid Warfare'. *Parameters* [online]. 45 (4) (inter 2015-2016), 65-75 [cit. 2019-04-30]. ISSN 0031-1723. Available at: https://ssi.armywarcollege.edu/pubs/parameters/issues/winter_2015-16/9_monaghan.pdf; RING, A. Teylur. *Russian Information Operations and the Rise of the Global Internet*. Master Thesis. Washington DC: University of Washington, 2015.

with sound effects intended to engender fear. Before murdering the pilot, ISIS published an 'interview' with him in its English-language propaganda magazine.

ISIS, or more precisely the 'ISIS Hacking Division', a group linked with it, published personal information of 100 current and past members of the US armed forces. The information included the names, home addresses and photographs of people who fought against ISIS. In its original online appeal, the 'Hacking Division' incited its followers to attack these military personnel, and indeed some people from the list or their family members became targets of verbal attacks on Facebook. But ISIS also called on its sympathisers to track these people to their homes and kill them. Personal information was collected from the internet – specifically, social networks. In response to this incident, the US government appealed to members of its security forces to limit their activities on social networks. The US Marine Corps instructed its members and their families to check their footprint on the internet, to verify the settings of their social networking accounts and to limit the amount of personal information they shared online. So far, the authorities have not sought to ban the use of social networks entirely. The US armed forces have issued instructions on how to use social networks as safely as possible, including advice on blocking access to the user's position, and advised armed forces personnel not to accept friend requests from people they do not know. On the opposite side, ISIS takes an essentially similar position, banning its fighters from using social networks to avoid surveillance from intelligence agencies. In May 2017, ISIS issued an official ban to all its fighters.

Of course, there have been multiple instances of ISIS intimidation on social networks. For instance, the Twitter account of US Command was hacked and the following message posted: 'American soldiers, we are coming, watch your back!'[13] The group Gasper CyberCaliphate Sadz hacked the Twitter account of Military Spouses of Strength and sent threats to partners of US soldiers via Twitter and Facebook. The following message was posted on Twitter: 'You think you're safe but IS is already here. #CyberCaliphate got into your PC and smartphone.' The messages sent to soldiers' wives contained death threats: 'We know everything about you, your husband and your children and we're much closer than you can ever imagine. You'll see no mercy, infidel!'; 'While your president and your husband are killing our brothers in Syria, Iraq and Afghanistan we're coming for you.'[14]

ISIS (also known as Daesh) has used mobile phones for intimidation, sending text messages to enemy soldiers. For instance, it nearly paralysed the Iraqi army units which were supposed to fight near Mosul in 2014. The message sent to soldiers was, 'Daesh is here'. They were also sent information that ISIS controlled Mosul and had released thousands of extremists from prison. The soldiers were so affected by the campaign that

13 COOPER, Helen. ISIS Is Cited in Hacking of Central Command's Twitter and YouTube Accounts. *New York Times* [online]. 12 January, 2015 [cit. 2019-04-30]. Available at: https://www.nytimes.com/2015/01/13/us/isis-is-cited-in-hacking-of-central-commands-twitter-feed.html.

14 MARTINEZ, Michael. Cyberwar: CyberCaliphate targets U.S. military spouses; Anonymous hits ISIS. *CNN* [online]. 11 February 2015 [cit. 2019-04-30]. Available at: https://edition-m.cnn.com/2015/02/10/us/isis-cybercaliphate-attacks-cyber-battles/index.html?r=https%3A%2F%2Fedition.cnn.com%2F2015%2F02%2F10%2Fus%2Fisis-cybercaliphate-attacks-cyber-battles%2Findex.html.

they refused to go further or to obey orders. They literally threw away their uniforms and weapons and deserted.

Psychological and information operations are also known from the ongoing Russo-Ukrainian conflict. As part of its information war, Russia conducts psychological operations against the Ukrainian armed forces, the aim of which is to undermine the morale of Ukrainian soldiers and to spread panic and fear among them. Mobile phones are used for this purpose to send intimidating text messages to Ukrainian armed forces fighting the pro-Russian separatists. This method of conducting psychological operations has been called 'pinpoint propaganda', and can be seen as an updated version of leaflets dropped from aircraft on to enemy territory. The sending of messages has been ascribed to the Russian armed forces, which have an IMSI catcher device at their disposal[15]. Normally, the police and intelligence services use such devices legitimately for the surveillance and apprehension of criminals, but according to Ukraine's cybernetic police, they are employed there for the purposes of psychological warfare. In eastern Ukraine, since 2014 propaganda messages have been sent through the largest Ukrainian mobile services provider, Kyivstar, owned by a Russian company. Examples of such messages include: 'Soldier, if you want to live, go home.' 'Welcome to the Donetsk People's Republic. Your generals are cowards and liars.' 'Your commanders have fled because they know the war is already lost. You're alone and no-one will help you.'[16] Messages threatening Ukrainian soldiers that they will be killed unless they leave, are not rare either. Similar messages are sent to soldiers' families and friends.

Several investigations into the origin of these messages suggest that Leer-3, a Russian system for electronic combat, is being used in Ukraine and is known to be deployed by Russia in Syria[17]. At a 2016 plenary session of the Organisation for Security and Cooperation in Europe (OSCE) Special Monitoring Mission to Ukraine, the Ukrainian delegation produced evidence of this system's presence in Donetsk[18].

Last but not least, disinformation and manipulated news can also affect members of the security forces even when they are not themselves the direct target of the disinformation. Many quasi-news websites seek to pose as alternative news sources, often claiming that – unlike mainstream or traditional media – they do not hide 'the truth'. These on-line media report on domestic and international events, and often offer what they call an 'alternative explanation of reality' or 'alternative facts' (which, of course, is

---

15 CHIRGWIN, Richard. Someone is sending propaganda texts to Ukrainian soldiers. *The Register* [online]. 2017 [cit. 2019-04-30]. Available at: https://www.theregister.co.uk/2017/05/12/someone_is_sending_propaganda_texts_to_ukranian_soldiers/.

16 KOPOTIN, Igor, SAZONOV, Vladimir. Russia's Information Warfare against Ukraine II: Influences on the Armed Forces of Ukraine [online]. Estonian National Defence College, 2015 [cit. 2019-04-30]. Available at: http://www.ksk.edu.ee/wp-content/uploads/2017/11/RUSSIA-%E2%80%99S-INFORMATION-WARFARE-AGAINST-UKRAINE-II-koolon-INFLUENCES-ON-THE-ARMED-FORCES-OF-UKRAINE.pdf.

17 DFRLab. Electronic Warfare by Drone and SMS: How Russia-backed separatists use 'pinpoint propaganda' in the Donbas. *Medium* [online]. 2017 [cit. 2019-04-30]. Available at: https://medium.com/dfrlab/electronic-warfare-by-drone-and-sms-7fec6aa7d696.

18 OSCE. *Statement by the Delegation of Ukraine at the 822nd FSC Plenary Meeting* [online]. 2016 [cit. 2019-04-30]. Available at: https://www.osce.org/fsc/252856?download=true.

a logical impossibility). Some of these media are directly state-orchestrated (for example, Russia's RT and Sputnik); others are independent of states but directed by people who support the geopolitical, security, civilisational etc. interests of other powers, or they simply prefer the worldviews of these powers to those offered by the West. Ideologically, they are closer to conservative, nationalist and authoritarian views than to liberalism and democracy. Their online disinformation works on the same principle, customising their interpretations of domestic and world events to the values of readers who tend to be anti-EU, anti-NATO and often right-wing. They also skilfully work with their readership's emotions and, through eliciting various sentiments, manipulate their opinions. Principles of cognitive dissonance and cognitive bias play an important role in this. A 2017 study by experts of the Indiana University School of Informatics and Computing shows that it does not matter whether the information given is provided by fact-checked or low-credibility articles (or even pieces of outright disinformation). Both types have the same chance of success with non-biased audiences[19]. We already have preconceived opinions on the bulk of the information we receive. Theories of cognitive dissonance and cognitive bias say that people have a natural tendency to accept information that upholds their position and keeps their behaviours in harmony, i.e. does not cause dissonance or inner tension. This leads us to false reasoning and decisions and the faulty remembering of information. We naturally tend to choose information that confirms our opinions. Members of the security/armed forces are as vulnerable as the population at large.

Besides already existing tools affecting the security/armed forces we can expect in the near future threats connected with artificial intelligence and machine learning processes. These might newly affect not only security/armed forces, but the general public as well. One of them might be madcom (machine-driven communication). Madcom refers to a state where artificial intelligence offers a multitude of tools and ways to manipulate the human mind, integrating artificial intelligence systems into robotic propaganda tools. This propaganda is then spread by an automated profile on social networks. By using sophisticated algorithms, this profile may produce its own content.[20] The development of madcom is expected to improve so-called chatbots. A chatbot (or also a chat robot) is a computer program designed for automated communication that asks people questions based on a predefined scenario. Chatbots have already been used in e-shops, and in communication applications such as Messenger and Skype. They communicate with clients in order to process online order returns or they help in choosing a product. With a set of questions, the chatbot finds out what the customer is interested in and redirects him or her to the product/manual. It is also expected that in the near future chatbots will learn to produce dynamic content based on psychological user profiling.

Above all, the security threats associated with madcom are that it is a tool that has the potential to spread highly personalised propaganda and disinformation

19 SHAO, Chengcheng et al. The spread of low-credibility content by social bots. *Nature communications* [online], 2018 [cit. 2019-04-30]. ISSN 2041-1723. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6246561/.

20 CHESSEN, Matt. *The Madcom Future*. Washington: Atlantic Council, 2017.

campaigns - based on information about the recipient. These will be personalised based on information about our activities in the virtual space, and on information we might share in the virtual space about family and friends, political preferences, demographic data and hobbies. Madcom tools will be able to come up with a very convincing and manipulative form of communication, able to target our vulnerabilities and detect our emotions in real time.

A newly discussed threat is also presented by deep fakes, which consist of audio or video of real people appearing to say or do things they never actually said or did. Originally, deep fake technology was used in the porn industry – faces of famous people were added into pornographic films. Replacing one person's face with another's using hyperrealist digital technology is a very accomplished illusion, based on deep machine learning. Beyond learning a person's movements and expressions, the machine also clones their voice and can make them appear to say anything – even words that the artificial intelligence had not learned directly. This technology has been marketed by companies such as Baidu, iSpeech and Lyrebird, which offered it for commercial purposes (for example, for human-machine interfaces). The Siri and Alexa digital assistants provide a generally known example of cloning a voice using machine learning.

There are a number of threats implied by the abuse of deep fake technology and the security risks are very high. Deep fakes exploit the same cognitive processes (and their weaknesses) as disinformation. They rely on the same processes of receiving information as any other communication and we can say that deep fakes are more dangerous than text, as we are more likely to believe video than text. Video seems naturally to guarantee the trustworthiness of information and are commonly used as proof that particular utterances were made. One question is: what will happen to video and audio material as evidence in judicial processes? To top it all, machine learning makes deep fake a technology that is very difficult to detect.

Bobby Chesney and Danielle Citron[21] identified several possible negative effects from deep fakes. Individuals and organisations, they say, might be abused, blackmailed or sabotaged. Nearly anyone could be blackmailed using a deep fake – whether for money, trade secrets, or any other information of a sensitive nature. Only a few hundred photographs of the person from social networks are needed to create a convincing video. Deep fake video depicting Barack Obama speaking about the dangers of disinformation needed 56 hours of recordings in order to create a plausible simulation of the ex-president's voice[22]. Deep fakes could also be used to falsely associate a person with another person, product, service or idea – an association that might not happen in the real world.

Deep fakes and other tools based on machine learning may damage not just people and legal entities; they may even have a very negative impact on society itself. Based on the analysis of Chesney and Citron, we can identify these threats, some of them very relevant in the context of vulnerability or resilience of security/armed forces:

---

21 CHESNEY, Bobby, CITRON, Danielle. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *SSRN Electronic Journal*, 2018. ISSN 1556-5068.

22 Bloomberg. How Faking Videos Became Easy – And Why That's So Scary. *Fortune* [online]. 11 September 2018 [cit. 2019-04-30]. Available at: http://fortune.com/2018/09/11/deep-fakes-obama-video/.

1) *Disruption of democratic discourse and of trust in institutions*

A substantial volume of disinformation damages democracy, aiming to undermine trust in the democratic system, consisting of political institutions and constitutional and political officials. Disinformation narratives seek to create the impression that political representatives betray their voters and misgovern, or to create an atmosphere where everyone lies and nobody can be trusted. Deep fakes will only make matters worse. Let us imagine, for instance, deep fake video or audio capturing law enforcement officials discussing possible ways of abusing their powers.

2) *Manipulating elections*

Disinformation plays a very conspicuous role at times of elections, entering the public discourse with increased frequency and aiming to influence the voters and outcome of the elections.

3) *Artificial increase of conflict in society*

It can be expected that this technology will be abused to increase or escalate tensions between various groups in the population, be they social, ethnic or religious. False information about the migration crisis, terrorist attacks in Europe (or Czechia) or support for radical Islam, are some obvious examples. For instance, let us imagine a deep fake video of a Muslim who in a Czech mosque openly supports ISIS or another terrorist organisation, and the possible consequences of such a video going viral.

4) *Dangers to public security*

Conflicts in society are only a small step away from dangers to public security. It is very easy to create panic with a gunshot, and a deep fake can work similarly in the virtual word (and from there, of course, such panic may be transferred into the real world). In the least harmful scenario, the panic creates financial damage; in the worse case, damage to property, accidents or deaths. Chesney and Citron[23] cite an example of intentional disinformation issued by a Russian research agency, which claimed that there had been a chemical disaster in Louisiana and an Ebola outbreak in Atlanta. The real damage caused by this disinformation was ultimately minimal, as both stories lacked proof and the facts were easy to verify. However, deep fake video and audio materials can potentially substantially improve the plausibility of disinformation.

5) *Undermining diplomacy*

Deep fakes could also seriously disrupt diplomatic relations. Words could be put in the mouths of political representatives that have never been uttered. Pressure could then be created to respond rapidly, causing damage in international relations and increasing the likelihood of a conflict breaking out. International relations could be disrupted by

23 CHESNEY, Bobby, CITRON, Danielle. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *SSRN Electronic Journal*, 2018. ISSN 1556-5068.

the publication of a video on the internet of army officers committing war crimes during their mission abroad.

6) *Dangers to national security*

The use of deep fakes to create danger to public security and to disrupt international relations can be thought of as threats to national security. We have encountered well developed propaganda from Daesh and the successor to Daesh might use deep fakes to create an 'alternative reality' in which their own fighters are strong and invincible. By contrast, armies or intelligence services might come under political or public pressure demanding the curtailing of their powers and greater control over them. This might happen when audio or video materials are published purporting to show that army or intelligence agency had abused their powers.

CONCLUSIONS AND RECOMMENDATIONS

Information and psychological operations are powerful instruments of warfare. Nevertheless, as has been demonstrated information and psychological operations have also become important instruments during peacetime and they have become a crucial part of what is called hybrid warfare, irregular warfare or asymmetric conflict (as the reader wishes). However, the Western /NATO military think about information and psychological operations in their own way in contrast to their Eastern equivalents, which have a more holistic and complex view. The Western thinking is more military-operations-focused, associating information operations exclusively with military operations. With psychological operations it is even more complicated. Psyops are here to support the aims of military operations, i.e. they are related to military affairs. Nevertheless, it is also said that psyops mean purposeful psychological influencing of target groups, carried out in peace and in wartime. Psyops play the role of a sub-category, but they also overlap with information operations. Based on this less-than-exact definition of mutual relations, and also due to the realities of conducting hybrid warfare (under the threshold of what is officially recognised as armed conflict, and preferring non-military tools) by a variety of state and non-state actors, the redefinition of information operations should be discussed in terms of expanding the definition in peacetime.

Also psyops deserve terminological redefinition so that they do not overlap with strategic communication, or are not narrowed down to white psyops only. The current definition reflects the democratic approach, which says that covert actions, deception and propaganda do not belong in the toolbox of democracies. Such an approach prevents us from being able to react to the toolbox of our adversaries, who do not apply the same approach. We do not need to be afraid that the redefinition means a green light for democracies to use such tools. It just creates space for better understanding our adversaries and for developing counter-measures.

Last but not least, as was demonstrated in the article, defence and security establishments should also react to the existing vulnerability of our own security/armed forces at the information-psychological level. In military affairs, a lot of attention is paid

to the information-technical level, but not necessarily enough is paid to the information--psychological level. We should be aware that it is not only the general public, but also military and security staff who are vulnerable and recognised as potential targets to be psychologically influenced by adversaries. Since psyops exploit fear, play with emotions and the cognitive dimension, it is necessary to build resilience also in this area.

Author: ***Petra Vejvodová, PhD.,*** *born 1984, works as assistant professor at the Department of Political Science of the Faculty of Social Studies, Masaryk University, and since 2016 has been the head of Security and Strategic Studies. She graduated in political science and international affairs at the Faculty of Social Studies. Her doctoral studies were successfully finished in 2014 with her PhD thesis on international cooperation of European neo-Nazis. In her research, she focuses on political extremism and radicalism in Europe, security policy, information warfare, propaganda and disinformation campaigns. Petra is author and co-author of multiple research papers. She is also a member of the Radicalisation Awareness Network and the European Expert Network on Terrorism Issues.*

How to cite: VEJVODOVÁ Petra. Information and Psychological Operations as a Challenge to Security and Defence. *Vojenské rozhledy*. 2019, 28 (3), 083-096. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz