 DOI: 10.3849/2336-2995. 31. 2022.01.038-050

Peer-reviewed

Issues of Resilience to Cyber-Enabled Psychological and Information Operations

Problematika resilience vůči psychologickým a informačním operacím vedených v kybernetickém prostoru

Petra Mlejnková

Abstract: This article discusses the transformation of the information environment, which allows an adversary to exploit cyber-enabled psychological and information operations. It presents the options currently available to an adversary to exploit the vulnerability of the information environment, chiefly the cognitive vulnerabilities of target groups. Thus, hostile interests are often pursued through manipulation, using disinformation, propaganda, algorithms and artificial intelligence. In the light of these developments, the article defines a society-centric approach, in which societal and human resilience are emphasised.

Abstrakt: Tento článek diskutuje transformaci informačního prostředí, která umožňuje protivníkovi využívat kybernetické psychologické a informační operace. Text představuje možnosti, které v současné době má protivník k dispozici za účelem exploatace zranitelností informačního prostředí, zejména kognitivních zranitelností cílových skupin. Nepřátelské zájmy jsou tak často prosazovány manipulací, použitím dezinformací, propagandy, algoritmů a umělé inteligence. Ve světle tohoto vývoje článek definuje přístup, který staví společnost do svého centra a který zdůrazňuje societální a lidskou odolnost.

Keywords: Information Operations; Psychological Operations; Information Environment; Resilience; Cognitive Resilience; Society-centric Approach.

Klíčová slova: informační operace; psychologické operace; Informační prostředí; odolnost; kognitivní odolnost; societální přístup.

INTRODUCTION

Among other things, the 21st century is characterised by major developments of cyberspace, information and communication technologies, new media and ways of distributing information to users online and influencing them in general. These developments have tremendous impacts on the contemporary information environment – an environment that integrates systems, information and people, both those who collect information and those who make decisions on its basis. The information environment is thus defined as having three dimensions: physical, informational and cognitive. In the physical dimension, we think about information infrastructure, collection, transmission, processing and delivery systems and devices that can be affected, as well as command and control facilities, ICT and supporting infrastructure. This dimension also covers people. It is not connected exclusively to military or nation-based systems and processes. Even though we consider here the military arena, civilians and civil infrastructure are also included. In the informational dimension, we think of information itself – its content and flow. This dimension covers the collection, processing, storage, dissemination and protection of information. Lastly, the cognitive dimension relates to the minds of those who transmit, receive, respond to or act upon information. The cognitive dimension covers individuals and groups, their personal and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, education, mental health, identities and ideologies[1].

Technological developments have transformed the character of the information environment to such an extent that it has become a new battlefield. Obviously, information warfare is nothing new and was around even before the emergence of cyberspace (consider, for example, electronic warfare and deception), but as cyberspace develops, the thinking about information warfare changes too and much emphasis is currently put on cyber-enabled information operations and particularly on psychological operations (psyops), which allow hostile actors to exert influence on their targets remotely. Thus states and their security actors face new challenges from hacking and operations to influence target populations through social hostile manipulation, which is defined by[2] as 'the purposeful, systematic generation and dissemination of information to produce harmful social, political, and economic outcomes in a target country by affecting beliefs, attitudes, and behavior.' This category integrates activities such as the exploitation of disinformation, propaganda or manipulation with algorithms and the use of artificial intelligence (AI)[3] – all of which helps to manipulate cognitive abilities and change the perception of reality.

1 UNITED STATES – JOINT CHIEFS OF STAFF. Joint Publication 3-13: Information operations. 2014; MILJKOVIC, Milan – PEŠIC, Anita. Informational and Psychological Aspects of Security Threats in Contemporary Environment. TEME, 2019, vol. 43, no. 4, pp. 1079-1094; VEJVODOVÁ, Petra. Information and Psychological Operations as a Challenge to Security and Defence. Vojenské rozhledy, 2019, vol. 28, no. 3.

2 MAZARR, J. Michael - BAUER, M. Ryan - CASEY, Abigail - HEINTZ, A. Sarah – MATTHEWS, J. Luke. 2019. The Emerging Risk of Virtual Societal Warfare. Social Manipulation in a Changing Information Environment. RAND Corporation, 2019, p. 1.

3 MAZARR – BAUER - CASEY - HEINTZ – MATTHEWS, ref. 2.

These new challenges of information warfare transcend the limits of the armies and security actors involved in providing security to the state; and society itself becomes involved in information warfare. Its vulnerability or resilience becomes a major factor in our ability to counter information and psychological operations. This article is about developing a holistic society-centric approach, which aims to put the society at the focal point and to decrease the population's vulnerability in the context of information warfare (with emphasis on the effects of cognitive operations).

First, the usual vectors of cognitive operations in cyberspace are identified together with cognitive vulnerabilities they exploit. These vectors are derived from the definition of tools of social hostile manipulation mentioned above, which integrates activities such as the exploitation of disinformation, propaganda or manipulation with algorithms and the use of artificial intelligence. Second, the article proposes a change to the way we think about resilience to psychological and information operations in cyberspace, and defines and conceptualises a society-centric approach together with human/societal resilience. Third, the society-centric approach and human/societal resilience are analysed on the case of the Czech Republic. The relevant actual national security strategic documents (defence and military related) are qualitatively analysed and evaluated in terms of the proposed approach and human/societal resilience. The analysis looks at whether the approach is present and in what way. These documents include the Long Term Perspective for Defence 2030 (issued 2015), the Concept of Construction of the Czech Army 2025 (2015), the Defence Strategy of the Czech Republic (2017), the National Cyber Defence Strategy of the Czech Republic (2018), the Concept of Preparing Citizens to Defend the State 2019-2024 (2019), the Long Term Perspective for Defence 2035 (2019), the Concept of Construction of the Czech Army 2030 (2019), the National Cyber Security Strategy of the Czech Republic for the Period 2021-2025 (2020), and the National Strategy for Countering Hybrid Interference (2021)[4].

1 PSYCHOLOGICAL AND INFORMATION OPERATIONS

Psychological operations, or psyops, can be defined as planned activities that use communication methods and other resources to select target audiences and influence and shape their emotions, attitudes, behaviour, perception and interpretation of reality. By using such methods, it is possible to induce particular responses in the target population, which, in the broader context, contribute to the fulfilment of specific objectives. Every psychological operation is based on a particular theme: the main, carefully prepared narrative or idea. The greater the target audience's receptivity – in other words,

4 MINISTRY OF DEFENCE OF THE CZECH REPUBLIC. Czech strategic documents. Available from: https://www.mocr.army.cz/dokumenty-a-legislativa/ceske-dokumenty-46088/. NATIONAL CENTRE OF CYBER OPERATIONS (NÁRODNÍ CENTRUM KYBERNETICKÝCH OPERACÍ). 2018. Strategie kybernetické obrany ČR 2018-2022. NATIONAL CYBER AND INFORMATION SECURITY AGENCY (NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST). 2020. The National Cyber Security Strategy of the Czech Republic for the Period 2021-2025.

their sensitivity to specific psyops tools – the greater the probability of the psychological operation's success[5]. The use of psychological operations increases the effectiveness of other actions and one's chances of success in a conflict, which, contemporarily, often takes place in an asymmetric environment. The importance of psyops is based on the belief that the psychological nature of a conflict is as important as the physical[6]. People's attitudes and behaviour affect the course and outcome of a conflict and the nature of an environment in which a conflict takes place. Psychological operations are perceived as a specific part of information operations.

Information operations can be defined as activities undertaken to counter hostile information and information systems while protecting one's own. They involve the coordinated and integrated employment of information-related capabilities to influence, disrupt, corrupt or usurp an adversary's decision-making[7]. They represent offensive and defensive measures to influence an adversary's decisions, manipulating information and information systems. They also include measures to protect one's decision-making processes, information and information systems. Information operations must have specifically defined goals and targets; therefore, careful planning is part of the process. Information operations are conducted within an information environment in which they affect all three of its dimensions: physical, informational and cognitive.

Information operations are complex processes that integrate information activities (collection, creation, transmission and protection), leading to influence over an adversary and the attainment of goals. They include psychological operations, operations security, information security, deception, electronic warfare, kinetic actions, key leader engagement and computer network operations. All together, they target the will of adversaries, their understanding of the situation and their capabilities.

5 MAREŠ, Miroslav - MLEJNKOVÁ, Petra. Propaganda and Disinformation as a Security Threat. In GREGOR, Miloš – MLEJNKOVÁ, Petra (eds.). Challenging Online Propaganda and Disinformation in the 21st Century. Palgrave Macmillan, 2021; NATO STANDARDIZATION OFFICE. Allied Joint Doctrine for Psychological Operations. Allied Joint Publication – 3.10.1. Brussels: North Atlantic Treaty Organization, NATO Standardization Office, 2014;

NATO STANDARDIZATION OFFICE. NATO Glossary of Terms and Definitions. AAP-06. Brussels: North Atlantic Treaty Organization, NATO Standardization Office, 2018; VEJVODOVÁ, ref. 1; WOJNOWSKI, Michal. Presidential elections as a state destabilization tool in the theory and practice of the Russian info-psychological operations in the 20th and 21st century. Przegląd Bezpieczeństwa Wewnętrznego, 2019, vol, 11, no. 21, pp. 311-333.

6 STILWELL, G. Richard. Political-Psychological Dimensions of Counterinsurgency. In GOLDSTEIN, L. Frank - FINDLEY, F. Benjamin (eds.). Psychological Operations. Principles and Case Studies. Alabama: Air University Press, 1996, pp. 319-332.

7 UNITED STATES – JOINT CHIEFS OF STAFF, ref. 1; MILJKOVIC – PEŠIC, ref. 1.

2 EXPLOITING COGNITIVE VULNERABILITIES

The development of the information environment permits the use of cyberspace to exploit our cognitive abilities, which directly influence our decision-making and actions. Technological development has caused the fragmentation and dynamic growth of the sources of information in the information environment, and cyberspace is overwhelmed by an enormous volume of information[8]. The options for controlling the credibility of such sources are very limited at present. Their fractionalisation encloses users in their own echo chambers[9], which facilitates the influencing of the audiences in these chambers and accelerates the formation of their attitudes. If users are not satisfied with an information source, they may very easily find an alternative that provides more satisfying information (which may be correct and verified, or unsubstantiated or even fabricated and intentionally untrue).

Social networks pose their own specific problems. This new type of media in its own way allows serious sources of information to be circumvented and, through the algorithms that control social networks, polarise society, enclosing its segments in information bubbles and contributing to the radicalisation of the positions people take. Social network algorithms confine users to social bubbles on the basis of the content they consume. They offer personalised content, prepared on the basis of the information users disclose about themselves and their behaviours in virtual space. We must therefore see social networks not only positively, as facilitating the dissemination of information, education and democratisation, but equally as instruments of cognitive radicalisation, which cause divisions in society and limit the options for discussion[10].

Algorithms are also poor masters when it comes to the dissemination of disinformation and propaganda. Here automation has two main effects: information can be distributed on a massive scale and very quickly, and it can be very well targeted to particular segments of society, who can be approached with content that is personalised and appears plausible to them. This makes psychological operations much more efficient, and – thanks to the internet and social networks – cheaper as well. Automated propaganda, or robotic propaganda, employs so-called bots and botnets – programs that automatically produce content that appears to have been created by a human[11]. Bots

8 MAZARR – BAUER - CASEY - HEINTZ – MATTHEWS, ref. 2.

9 JASNY, Lorien - WAGGLE, Joseph - FISHER, R. Dana. An empirical examination of echo chambers in US climate policy networks. Nature Climate Change, 2015, 5, pp. 782–786; LEWANDOWSKY, Stephan - ECKER, K.H. Ulrike - COOK, John. Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era. Journal of Applied Research in Memory and Cognition, 2017, vol. 6, no. 4, pp. 353-369.

10 TUFEKCI, Zeynep. YouTube, the Great Radicalizer. The New York Times. 2018. Available from: https://nyti.ms/3kQIygh. Accessed 20 February 2020.

11 THE COMPUTATIONAL PROPAGANDA PROJECT. Resource for Understanding Political Bots. 2016. Available from: http://comprop.oii.ox.ac.uk/research/public-scholarship/resource-for-understanding-political-bots/. Accessed 10 November 2019; GORWA, Robert - GUILBEAULT, Douglas. Unpacking the Social Media Bot: A Typology to Guide Research and Policy. Policy & Internet, 2018. Available from: https://doi.org/10.1002/poi3.184.

interact with people online and, if programmed well, can be difficult to identify as bots. Low price, availability and the option to segment the target audience[12] are benefits that mean bots can help their masters to manipulate the attitudes of a target audience. Robotic propaganda can also create the impression that the topic being manipulated is of mass interest and importance. This might entice users to be more active, as it makes them believe that it is a crucial issue. This phenomenon is known as astroturfing[13]. In the future, bot activities may intensify thanks to links with artificial intelligence. The Atlantic Council defines this phenomenon as MADCOM – machine-driven communication[14]. MADCOM employs the options of machine learning, deep learning and chatbots. Chessen notes that this may create a very powerful instrument for propaganda[15], which will deploy personalised content and user information and hence will be more precise and more efficient in exploiting the vulnerability of a target audience, and will be able to do so in real time.

Personalisation is becoming a generally powerful instrument for communicating and exerting influence within the virtual space. Until recently, those working in information and psychological operations knew their effects on the target audience only to a very limited extent; rather, they could only guess at these effects and hope that their efforts would be effective. Likewise, it was difficult to do any precise targeting. With the internet, mobile phone apps and social networks, we have experienced a tremendous change as far as knowledge of users is concerned. The internet allows data to be collected about groups and individuals on a mass scale. The result is that social behaviour can be observed today on various levels. It is possible to observe small communities and the responses of target groups across time and space. This development in turn changes the way information is transmitted, makes information more important and opens new options for developing information warfare.

Such developments mean that one does not have to limit oneself to the dissemination of manipulative content and defined narratives; one may take a notional step back and focus on controlling the networks of contacts, the links between people and the strength of these links online. In information warfare, achieving victory no longer means disseminating the narrative; victory means gaining control over the network in question[16]. Having taken control of the network's configuration, one may then manipulate and disseminate narratives as needed. The technological setting of the internet allows one to conduct operations whose aim is to reconfigure both the links between users and the

12 WOOLEY, C. Samuel - HOWARD, N. Philip. Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media. Oxford University Press, 2018.

13 PAVLÍKOVÁ, Miroslava - ŠENKÝŘOVÁ, Barbora -DRMOLA, Jakub. Propaganda and Disinformation Go Online. In GREGOR, Miloš – MLEJNKOVÁ, Petra (eds.). Challenging Online Propaganda and Disinformation in the 21st Century. Palgrave Macmillan, 2021.

14 CHESSEN, Matt. (2017). The MADCOM future: How artificial intelligence will enhance computational propaganda, reprogram human culture and threaten democracy and what can be done about it. Washington: Atlantic Council, 2017.

15 Ibid.

16 HWANG, Tim. *Maneuver and Manipulation: On the Military Strategy of Online Information Warfare*. Carlisle: Strategic Studies Institute, 2019.

networks of trust. One may influence with whom people communicate, with whom they become acquainted, and whom they consider a trustworthy source. The internet allows one to obtain detailed knowledge about how individual users are interconnected. It is easy, for instance, to identify individuals with anti-government feelings, and to target and directly influence them. It is also possible purposely to link various groups, and to focus on making their mutual links more intense, hence strengthening their opposition. Thus, for instance, a group of people with anti-government feelings can be intentionally enlarged. If data reveal that these users live enclosed in their social bubbles and exert no influence outside, again, one can intervene in the network and, using seemingly unconnected data, strengthen their links outside their social bubbles and bridge various groups, for instance on the basis of people's leisure-time interests. This represents a major change compared with the situation where information operations worked with very coarsely defined demographic segments and groups.

Awareness of these options, and of vulnerabilities, is important, because research shows that the structure of the social links between individuals strongly influences their attitudes and behaviours. The structure of the network influences political affiliations, health habits and shopping, as well as such matters as the likelihood of divorce[17]. By manipulating the network of connections on a micro-level, one may influence the entire structure of a society's or a target group's attitudes and behaviours. This may threaten social cohesion and the very social capital of a society, of which the network of connections constitutes a source. To individuals, social links define credible sources and legitimise standards of behaviour.

The effectiveness of all these instruments would be limited if they could not misuse the limits of human cognitive abilities. Here we talk about the tendency to avoid information that contradicts our views. This phenomenon is called selective exposure and the obverse is that we seek out information that confirms our positions. New information we are willing to accept will therefore confirm our position rather than the opposite[18]. We tend to ignore, downplay or reformulate new information that contradicts our beliefs. Going hand in hand with selective exposure is another cognitive limit – selective perception – which is what happens when we project what we want to see and hear[19].

---

17 BAPNA, Ravi - UMYAROV, Akhmed. Do Your Online Friends Make You Pay? A Randomized Field Experiment on Peer Influence in Online Social Networks. *Management Science*, vol. 61, no. 8, 2015, pp. 1902-1920; BREDECKER, Robert – ELKIND, Edith. Manipulating Opinion Diffusion in Social Networks. Proceedings of the 26th International Joint Conference on Artificial Intelligence, 2017. Available from: https://bit.ly/30gogDD. Accessed 20 December 2020; HWANG, ref. 14.

18 O'SHAUGHNESSY, Nicolas. From Disinformation to Fake News: Forward into the Past. In BAINES, Paul - O'SHAUGHNESSY, Nicolas - SNOW, Nancy (eds.). *The SAGE Handbook of Propaganda*. London, Thousand Oaks, New Dehli and Singapore: SAGE, 2020, pp. 55-70.

19 FREEDMAN, L. Jonathan – SEARS, O. David. Selective Exposure. *Advances in Experimental Social Psychology*, 1965, vol. 2, pp. 57-97. Available from: https://doi.org/10.1016/S0065-2601(08)60103-3. Accessed 14 November 2020; HART, William - ALBARRACÍN, Dolores – EAGLY, H. Alice - BRECHAN, Inge - LINDBERG, J. Matthew - MERRILL, Lisa. Feeling validated versus being correct: A meta-analysis of selective exposure to information. *Psychological Bulletin*, 2009, vol. 135, no. 4, pp. 555-588. Available from: https://doi.org/10.1037/a0015701. Accessed 12 November 2020. ZILLMANN, Dolf -JENNINNGS, Bryant. *Selective Exposure to Communication*. London: Routledge, 2011.

The selection of information is also influenced by cognitive dissonance: if we are faced with two incompatible pieces of information, we tend to decrease the importance of one of them.

The sleeper effect causes us to remember information longer than its source. If initially we remember that the message was from an untrustworthy source and is probably false, over time we tend to forget this and only the message itself remains in our brain. It has been shown that we have a tendency to disseminate negative news more readily than positive, and we remember negative information better than positive[20]. A study conducted on 2006–2010 Twitter data shows that people shared 126,000 rumours and hoaxes online, which reached users ten times faster than true information. Researchers checked the role of bots and found that these did not bias the data or conclusions[21]. The first information received stands a higher chance of success. This means that, when faced with a topic on which we do not yet have an opinion, there is a greater chance that our view of it will be influenced by the first message we receive about it, even if this information may be false. From the perspective of cognitive processes, a second message, albeit true, is greatly handicapped in its ability to convince us.

Modern operations in the information environment draw on all these technological and cognitive options, and the cognitive dimension of the information environment[22] becomes essential for the success in modern information warfare. Such a situation draws society itself, and not only the state's security forces, into the game. The centrality of the societal dimension of conflict is now more important than at any point in history[23].

3 SOCIETY-CENTRIC APPROACH AND RESILIENCE TOWARDS PSYCHOLOGICAL AND INFORMATION OPERATIONS

It is fitting to consider the importance of a society-centric approach, through which to focus on increasing the resilience of society and those parts of it that become targets of cyber-enabled information and psychological operations. We cannot exclude classical technology- and operations-driven strategies and military thinking, nevertheless the possibility of direct military to military operations decreased. Instead, West's challengers increasingly search for operations with societal impact under the threshold of war blurring classical distinction between peace and war, or warrior and non-combatant. The adversaries often target pre-identified societal groups and individuals and their cognitive

20 KENSINGER, A. Elizabeth. Negative emotion enhances memory accuracy. Behavioral and neuroimaging evidence. *Current directions in psychological science*, 2007, vol. 16, no. 4.

21 VOSOUGHI, Soroush – ROY, Deb – ARAL, Sinan. The spread of true and false news online. *Science*, 2018, vol. 359, no. 6380, pp. 1146-1151.

22 TASHEV, Blagvest – PURCELL, Michael – MCLAUGHLIN, Brian. Russia's Information Warfare. Exploring the Cognitive Dimension. *MCU Journal*, 2019, vol. 10, no. 2.

23 KELTON, Maryanne - SULLIVAN Michael – BIENVENUE, Emily, ROGERS, Zac. Australia, the utility of force and the society-centric battlespace. *International Affairs*, 2019, vol. 95, no. 4, pp. 859-876.

vulnerabilities. Therefor the society-centric approach gains higher relevance. This approach was first described by Levite and Shimshoni[24]. Then applied, albeit very generally, by Kelton, Sullivan, Bienvenue, Rogers[25] in the context of defending Australia against information warfare. It puts humans, society and the cognitive dimension to the foreground, since they are the targets of the information and psychological operations.

The approach corresponds well to the fact that in modern information warfare one person influences another. Protecting people, or increasing of their resilience, thus becomes crucial in adapting to a changing environment, and brings us to the concept of human/societal resilience. In this scheme, human resilience represents the micro-level, and societal resilience the meso-level.

Four levels are crucial in ensuring human and societal resilience in the context of information and psychological operations: (1) cognitive resilience, (2) institutional settings, (3) technological operations and (4) legal framework[26].

Of these four levels, cognitive resilience probably poses the greatest challenge. This type of resilience tends to be reflected today more in psychology and education than in security studies. It is the only level that is directly linked with people and their ability to interpret social reality. Cognitive resilience serves to prevent disinformation and propaganda from taking root and being internalised by the target audience. It relates to world views and interpretative schemata, making sense of information and affecting the process of decision-making[27]. Cognitive resilience helps people withstand the pressure of various ideas that are spread around, not least via disinformation and conspiracy theories[28]. The quality of cognitive resilience at the level of the individual influences its quality at the societal level. Building this type of resilience is largely the responsibility of those who provide the education and training of abilities in the cognitive domain. However, it is also connected with the political culture in the given society, or with such factors as the measure of trust in institutions.

The other three levels (institutional, technological and legal) are linked with a systematic and coordinated response on the part of the state, and these levels must support the effort to build up cognitive resilience (through the prism of the society-centric approach). In the case of the institutional level, this means setting up multi-agency and multidisciplinary cooperation between relevant institutions affected by the operations in the information environment. Understandably, this level is also about building an adequate institutional structure, which will be able to deal with information and psychological operations (whether that means defence, or pursuing active operations).

---

24 LEVITE, Ariel, E. – SHIMSHONI, Jonathan (Yoni). The Strategic Challenge of Socienty-centric Warfare. *Survival*, 2018, vol. 60, no. 6, pp. 91-118.

25 KELTON – SULLIVAN – BIENVENUE . ROGERS, ref. 23.

26 GREGOR, Miloš – MLEJNKOVÁ, Petra (eds.). Challenging Online Propaganda and Disinformation in the 21st Century. Palgrave Macmillan, 2021.

27 BJOLA, Corneliu – PAPADAKIS, Krysianna. Digital propaganda, counterpublics and the disruption of the public sphere: the Finnish approach to building digital resilience. *Cambridge Review of International Affairs*, 2020; HANSEN, S. Flemming. Russian hybrid warfare. A study of disinformation. Copenhagen: Danish Institute for International Studies, 2017.

28 HANSEN, ref. 24.

The importance of the legal and technological levels consists in the fact that cognitive resilience, after all, has certain natural limits. These levels are thus tasked with supporting the resilience of people and society. For instance, technological development has contributed to psychological operations assuming such characteristics that our cognitive abilities are insufficient to determine what is true and false (e.g. the ever-improving deep fake videos and other ways of manipulation using artificial intelligence). Furthermore, the information environment is increasingly complicated and overloaded, creating substantial demands – in terms of time and resources – if we are to orient ourselves in this environment. On the technological level, we face the challenge of collecting and evaluating large volumes of data. In the context of information and psychological operations this specifically means developing instruments that will help us to detect and analyse the evidence obtained about the operations of hostile actors. But even those outputs that have been facilitated by technology will ultimately have to be evaluated by humans, which takes us back to cognitive resilience. The task of the legal level is to set up a suitable legal framework to protect the state and society.

4 SOCIETY-CENTRIC APPROACH IN THE CZECH DEFENCE-RELATED STRATEGIC DOCUMENTS

Based on the qualitative analysis of the Czech defence-related strategic documents, the strategic thinking only slowly approaches the society-centric approach. Analysed documents (covering the period 2015-2021) prove the awareness of hybrid threats targeting the Czech security environment and their vectors of action. Role of media, social networks, cyberspace operations, or disinformation campaigns as adversaries' tools are mentioned already in the Long Term Perspective for Defence 2030 from 2015 and the Defence Strategy from 2017. This type of threat is elaborated more intensively in the Long Term Perspective for Defence 2035, where is stated that modern information and communication technologies, media, social networks can be used for information and psychological operations spreading disinformation and propaganda. Such awareness led to issuing the National Strategy for Countering Hybrid Interference in 2021. Here, the threat is already communicated also within the society-centric approach when the document states that the hybrid interference endangers society and political decision-making process on the first place. For the first time since 2015 it is specifically mentioned in the defence-related materials that hybrid interference might happen also through mobilization of civilian segments of the society in order to destabilize the system and endanger the security.

In terms of the threat classification, we can observe that the society-oriented view has been adopted. Nevertheless, when discussing the issue of resilience and need-to--be-taken actions, the society-oriented approach is almost missing. The resilience is dominantly connected with technology-driven operations. The Long Term Perspective for Defence 2030 from 2015 and the Long Term Perspective for Defence 2035 from 2019 briefly mention the need of protection of information systems and building the cyber defence in technology- and operations- dominant manners. The Concept of Construction of the Czech Army 2030 from 2019 does not differ when focusing on resilient

information system and defence against cyber attacks. The emphasis is put on building the institution of professional cyber forces as a military unit enabled to lead information and psychological operations. Another institutional aspect of resilience building reveals in the National Strategy for Countering Hybrid Interference from 2021, which declares establishment of official coordinator for countering hybrid interference. The general need of proper legal framework defining competencies in cyber defence is touched by the National Cyber Defence Strategy of the Czech Republic 2018-2022 and again repeated in the National Cyber Security Strategy of the Czech Republic for the Period 2021-2025.

First signals of society-oriented approach appear in the Concept of Construction of the Czech Army 2030 from 2019, in the National Cyber Security Strategy of the Czech Republic for the Period 2021-2025 (2020), and the National Strategy for Countering Hybrid Interference (2021). In the Concept of Construction of the Czech Army 2030 the importance of societal resilience is specifically mentioned, however very briefly. The National Cyber Security Strategy develops rather specific issue of need to widen the pool of motivated and well-educated experts as one of the precious sources of the state. Slightly more society-oriented remarks appear in the National Strategy for Countering Hybrid Interference. According to the document, the government defines as one of the strategic goals resilient society and whole-of-society approach to counter the hybrid interference. The societal vulnerabilities and conflicts are one of the targets of such activities of adversaries. Interestingly, nothing like that can be found in the National Cyber Defence Strategy.

As mentioned above, the key feature of society-centric approach are humans, society and cognitive dimension. Resilience towards the psychological and information operations targeting cognitive vulnerabilities leads us to the necessity of increasing the cognitive resilience to survive in the changing environment. However, this is reflected in the strategic documents in a limited way. It is only the National Cyber Security Strategy and the National Strategy for Countering Hybrid Interference (the newest documents) touching upon such issues. It is the necessity of strategic communication, development of critical thinking, and media literacy, which are mentioned as general principles of increasing the resilience. In case of capacities of security forces, the strategic documents avoid the issue of cognitive resilience. The support for this segment of society is meant to be psychological, humanitarian, and spiritual. In the context of cyber-enabled operations, the empowerment stays in line of technical skills.

The Czech strategic documents confirm what Levite and Shimshoni mention. The strategical thinking and military logic are still more technological- and operation-oriented, rather than society-oriented. Process of reflexion of challenges related to changing environment and character of hybrid threats exploiting cognitive vulnerabilities leading to shift in strategical thinking is on its very beginning. Levite and Shimshoni stress that socio-psychological understanding and definition of mission in terms of engaging the social dimension are crucial. With cyber-enabled cognitive operations society becomes strategical and the states are challenged to think more in terms of societal impact. Levite and Shimshoni suggest assessment of the societal dynamics and impacts flowing from different modes of confrontation in case of own population and adversaries' populations; the consideration of the social strengths, weaknesses, vulnerabilites, motivations,

and intents are necessary.[29] In case of armed forces the preparedness is not anymore only in combat and technical skills, and psychological resilience, but certain level of cognitive resilience is also necessary.

CONCLUSION

As the information environment changes, and modes of waging war and other aspects are modernised, as a society and state we are increasingly at risk of threats that are not military in character, and that do not cross that limit which normally impels a democratic regime to declare a state of emergency. Adversaries today have a broad palette of instruments to promote their interests, influence their target audiences and induce them to act according to their expectations. They can do this literally from the comfort of their own homes, without having to cross national borders. Adversaries are employing cyber-enabled psychological and information operations, which by their very nature are often intended to influence the cognitive abilities or vulnerabilities of the target audience. Moreover, these efforts often seek to influence the population at large, aiming to undermine its morals and its trust in its domestic regime and its representatives. Thus the common people are more than ever before drawn into the mutual contest for power, and are exposed to sophisticated methods such as personalised content. Many threats thus take a cognitive and society-centric character. This can be shown by the weaponisation of information, especially on social media. As noted in the introduction to this paper, we are facing socially hostile manipulation[30] – manipulation that uses propaganda, disinformation, algorithms and artificial intelligence to exploit cognitive vulnerabilities. In this context, this paper proposes to change our point of view of these threats, and to see them through the lens of the society-centric approach, which puts the society and its vulnerability – and hence the need to build up its resilience – at the focal point. Of course, this approach does not mean limiting the building of technological resilience. Rather, these two go hand in hand, as societal resilience will not be effective without advanced technologies, and technological processes are an important supporting element. Nonetheless, as noted in this paper, ultimately the outputs of modern technologies are, again, evaluated by people, and thus human cognitive abilities re-enter the game. Similarly, this approach does not preclude building the resilience of specific segments of society, such as the armed forces. Again, these specific segments are part of this broader concept.

On the case of the Czech Republic is demonstrated that the society-centric approach is accepted in strategic thinking only in a very limited way. It is rather its fragments which appear in the strategic documents, however the Czech Republic lacks complex approach.

29 LEVITE – SHIMSHONI, ref. 24.

30 MAZARR – BAUER - CASEY - HEINTZ – MATTHEWS, ref. 2.

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.

Author: ***Mgr. et Mgr. Petra Mlejnková, Ph.D.*** *(born 1984) is an assistant professor at the Department of Political Science, Faculty of Social Studies, Masaryk University (FSS MU) and a researcher at the International Institute of Political Science, FSS MU. She focuses on research of extremism and radicalism in Europe, propaganda, and information warfare. She is a member of the expert networks the Radicalisation Awareness Network, the European Expert Network on Terrorism Issues, and the Czech RAN CZ expert network coordinated by the Ministry of the Interior of the Czech Republic.*

How to cite: MLEJNKOVÁ, Petra. Issues of Resilience to Cyber-Enabled Psychological and Information Operations. *Vojenské rozhledy*. 2022, 31 (1), 038-050. ISSN 1210-3292 (print), 2336-2995 (online). Available at: www.vojenskerozhledy.cz