TEME, г. XLV, бр. 1, јануар – март 2021, стр. 129–144

Оригинални научни рад https://doi.org/10.22190/TEME200218008M
Примљено: 18. 2. 2020. UDK 004.738.5:316.658
Ревидирана верзија: 25. 11. 2020.
Одобрено за штампу: 26. 2. 2021.

STRATEGIC COMMUNICATION AND SOCIAL NETWORK INFLUENCE: THE METHODS OF PSYCHOLOGICAL MANIPULATIONS IN CYBERSPACE AND THE SUGGESTION FOR ITS PREVENTION

Miroslav Mitrović[1]*, Dragan Vasiljević[2]

[1]Strategic Research Institute, University of Defence in Belgrade, Serbia
[2]Serbian Armed Forces, Serbia

Abstract

Strategic communication is one of the expressions of state power and the instrument for achieving political and the security of national interests. In the context of contemporary conflicts, it is an appearance of hybrid action in the fields of information, the media, the Internet and the wide spectrum of public diplomacy performances. The main goal of strategic communication (SC) is to influence public opinion. In addition, SC strives to move the focus of the public towards cultural values as well as the adjustment of the political system. The main task of strategic communication (SC) is to influence public opinion and its focus on cultural values, the possible adaptation of the political system by "reprogramming" political culture in accordance with the goals set by psychological influence. One of the main channels for influence are social networks. In the paper, we used a multi-criterion analysis to identify the method of prevention pertaining to psychological manipulations in the cyberspace. This paper suggests preventive measures against negative impacts of social networks. In the paper, we used the Analytic Hierarchical Processes for the analysis of hierarchy in the application of preventive measures. Based on the obtained results, we developed and presented the application of preventive measures, to prevent the harmful effects of psychological manipulations in the cyberspace.

Key words: strategic communication, hybrid warfare, Internet social networks, psychological manipulation, cyberspace.

* Аутор за кореспонденцију: Мирослав Митровић, Институт за стратегијска истраживања, Универзитет одбране Београд, Незнаног јунака 38, 11000 Београд, Србија, mitrovicmm@gmail.com

СТРАТЕШКА КОМУНИКАЦИЈА И УТИЦАЈ ДРУШТВЕНИХ МРЕЖА: МЕТОДЕ ПСИХОЛОШКИХ МАНИПУЛАЦИЈА У САЈБЕР ПРОСТОРУ И ПРЕДЛОГ ЊИХОВОГ СПРЕЧАВАЊА

Апстракт

Стратешка комуникација је један од израза државне моћи и представља инструмент у политичком и безбедносном остваривању националних интереса. У контексту савремених сукоба, представља израз хибридног деловања у областима информисања, медија, интернета и широког спектра деловања јавне дипломатије. Главни задатак стратешке комуникације (СК) јесте утицај на јавно мњење и њено усредсређивање на културне вредности, могућем прилагођавању политичког система „репрограмирањем" политичке културе у складу са постављеним циљевима психолошког утицаја. Један од главних канала за утицај је интернет, конкретније, друштвене мреже и активности у сајбер простору. У раду је коришћена мултикритеријумска анализа са циљем идентификације метода превенције од психолошких манипулација у сајбер простору. Поред тога, овај рад предлаже превентивне мере против негативних утицаја на друштвеним мрежама, како на појединца тако и на друштвену заједницу. У раду су помоћу аналитичких хијерархијских процеса извршене анализе приоритета у примени превентивних мера. На основу добијених резултата, развили смо и представили превентивне мере, у циљу спречавања штетних ефеката психолошких манипулација у сајбер простору.

Кључне речи: стратешка комуникација, хибридно ратовање, друштвене мреже на интернету, психолошке манипулације, сајбер простор.

INTRODUCTION

In contemporary society, Strategic communication (SC) is a part of social activities in the phase of strong development and growth, based on effective and accurate usage of information. However, not all communication is strategic, nor is all strategic communication conducted against positive goals (Holtzhausen & Zerfass, 2015, p. 3-17). The existing understanding of SC is mostly based on the definition suggested by Hallahan as "communicating purposefully to advance (the organization's) mission" and "implies that people will be engaged in deliberate communication practice on behalf of organizations, causes, and social movements" (Hallahan, et al. 2007, p. 4). Also, SC is a modern management concept of permanent adjustment of multidisciplinary interactive communication between different levels and forms of entities, with a goal to achieve the desired relationships between subjects in the process (Mitrović, 2017). In the sense of understanding of SC as a tool for presenting the organization as a social actor in creating a public culture (Mitrović, 2019a), strategic communication could be observed through:

- National (state) institutional level: public diplomacy, psychological operations, public affairs, propaganda, interest communication (lobbying, representation of interests, strategic negotiation) (Mitrović, 2019b).

- Corporate level: public relations, integrated marketing communication, socially responsible practices, corporate political activities (Mitrović, 2019c).

At the national level, to be successful, strategic communication must include the communication content and broadcast of activities, "images" and politics (Christopher, 2011a, p. 5) which will inform, influence or convince the audience in the nature of the message of national objectives (Christopher, 2011b, p. 4).

CYBERSPACE AS AN INFLUENTIAL SPACE FOR SC PERTAINING TO DEFENSE ISSUES

Besides the fact that cyberspace has no overall, unique definition, contemporary research and works indicate that cyberspace is an environment in which, a cognitive world is created by intellectual activities through the interface of information and communication systems. (Vasiljević, Vasiljević & Djurić, 2018, p. 225).

Developed technical solutions, which are the base for the implementation of channels for communication, make actual societies dependable on informational and communicational technologies. Moreover, contemporary civilization is linked with digitalized communication, which makes all national (state) systems potentially fragile and vulnerable to all sorts of attacks in cyberspace (Mitrović & Miljković, 2018).

The indicated characteristics of cyberspace are core for information operations whose goal is to influence attitudes and the public opinion and thinking. Effects are influential on the motivation for defense, the trust in political and army leadership, but also aspects of mobilization and recruitment. Influence on personality in cyberspace can affect the predictable behavior through personality change attitudes, depending on their basic psychological characteristics. The influence on the predictable behavior of the personality is the goal of contemporary psychological operations performed in cyberspace, which are referred to as "impact operations".

In the contemporary information age, the application of information technology in contemporary psychological operations is widespread and almost unavoidable. The Internet, as the prevailing part of cyberspace, is used as the main medium for the distribution of psychological content. The specialized software tools are used to analyze the target group with purpose of a more accurately and efficiently distribution of the psychological content. Therefore, the material of psychological “impact operations” must be particularly attractive for the target group. More precisely, a message must be adapted to the psychological characteristics of the target audience.

The personality characteristics determine the behavior on the Internet and this is the basis for the selection of target groups of psychological operations in cyberspace. Therefore, one of the models of psychological operations implies influencing the predictable behavior of a person through the change of beliefs and attitudes, depending on their psychological characteristics and ways of behavior in cyberspace. Concerning Hansen (Hansen, 2013), influence on the attitudes and behaviors could be exposed in the following ways: 1) critical resources controlling, 2) fraud and 3) social influence. Pratkanis (Pratkanis, 2007) defines social influence as any non-coercive technique, procedure or manipulation that relies on the socio-psychological nature of human beings as a means of creating or changing the belief or behavior of the goal.

The societal influence on the predictable behavior of a person through the change of beliefs and attitudes can significantly emerge in the cyberspace. Due to the low cost of access, the wide variety of users, the global distribution and the high speed of information flow, social networks have a major impact on the behavior of their users.

The activities of individuals or organizations consciously focused on the attempts to change attitudes and behaviors of individuals, a smaller or larger group of people, are called an "operation of influence". The goal of operation of influence is to achieve an impact on the target group audience, which consequently implies the power position of a side which leads the operation. One way of influencing toward a change of attitudes and forming the opinion of the target group, which is applied in the operations of influence, is the dissemination of information and data, messaging and knowledge exchange (Gupta & Dhami, 2015).

Research on the relationship between the cyberspace and social psychology suggest that cyberspace offers numerous possibilities for "knowledge sharing" and "coercive operations designed to influence the target group change, compromising, destruction or theft of information access to information systems and networks" (Pissanidis, Rõigas & Veenendaal, 2016). Research conducted by Deng and Liu (Deng & Liu, 2017) approved the existence of a relationship between personality traits and behavior on social networks based on the theory of the “Big Five”. The Big Fife theory considers *openness*, *conscientiousness*, *extraversion*, *agreeableness*, and *neuroticism* as main personality traits (Power & Pluess, 2015). Closely, in the scope of the psychological influence on personal cognition in cyberspace, Kosinski (Kosinski, et al. 2014) suggests that there are significant psychological links between the users' personalities, and their profile at the most famous social network, Facebook. The behavior of users in cyberspace is a cyber-personality (Sartonen, Huhtinen & Rhizomatic, 2016), the "digital image" of a real personality. It offers opportunities for precise impact operations that can be directed to a target group.

The theory of planned behavior (TPB) explains that attitudes play an important role in explaining human behavior and that they are formed from prominent beliefs about this behavior (Ajzen, 1985). The TPB suggests that the impact on behavior (and its change) can be made through changes in attitudes, subjective norms, and the perceived behavioral control. According to Ajzen (Ajzen, 2019), the consequence of the exposure of the subject's entity to new information and experiences that can lead to changes in their beliefs, is to influence their intent, which consequently, influences their behavior.

Internet users, by changing their status on social networks, making public comments, etc., can behave under the "expectations", for them some important persons, and in this way express intentions about future behavior in real life. Also, real-life behavior toward expectations is expressed by mimicking and supporting the views and activities of significant individuals. Overall conclusions of contemporary projecting of SC as an "operation of influence" in cyberspace are: 1) The behavior on the Internet shortens the selection of the target group of psychological operations (PO) in cyberspace; 2) The application of modern information technology shortens the time of the selection of the target group for PO; 3) The means of mass communication have gained a new role in a modern society based on the influence of the media influence and political power, concentrated in certain social structures (Mitrovic & Vulic, 2019).

PSYCHOLOGICAL IMPACT IN CYBERSPACE

Achieving psychological impact in cyberspace, as a form of social influence, has the aim to change the perception or behavior of people through concealment, deception or abuse. This topic was elaborated by Braiker (Braiker, 2004) and we intend to assess it through multi-criteria testing.

Manipulation is the term that describes the usage of various data or information for the "seduction of the public", in psychology it is also used in the meaning of a special manipulative, versus verbal ability (Vidanović, 2006). Potential victims of manipulators on social networks are aware that they set content to their profile on social networks, and the psychological characteristics can be detected from that content without the intention of the social network user. For a manipulator, an analysis of the content of a social network profile offers a personality draft profile of a potential victim.

Methods of Psychological Manipulation

The most commonly used methods of psychological manipulation are: 1) manipulation of fear, 2) manipulating the sense of guilt, 3) the method of small and larger demands, 4) encouraging projection, 5) provoking narcissism, 6) violation of privacy and 7) relativizing the truth.

1) Manipulating with fear – "fear – then – relief"; Fear is the primary emotion that arises from the perception or expectation of real or imaginary danger, or a serious threat. One of the most expressive fears especially occurs during adolescence, and it is the fear of social rejection (Bernstein & Borchardt, 1991). This method can be reasonably considered the most insidious of all, and psychologists call it the "fear-then-relief" method that relies on the manipulation of human emotions.

2) Manipulating the sense of guilt – "social exchange"; It is described as the interpersonal strategy of influencing where person A awards B (psychological or material), and in return, when A asks B for some favor in return, B feels the (inner) pressure to obey in favor of A's request (Benoit & Benoit, 2007).

3) Provocation of sensitivity - the method of small and higher requirements – "Foot-in-the-door" technique; This technique of manipulation is very perfidious, and at the same time imperceptible and simple. Using the "Foot-in-the-door" (Rot, 2006) method, the abuser at the beginning asks the victim for a small and simple service, followed by a new, significant requirement.

4) Encourage projection; The technique improves compliance with the interviewer by monitoring his behavior or gesture and using it in the communication process. Generally, people have positive affection toward similar gestures (mirror projection) and communication-based on projection results with a positive outcome. However, if the interlocutor consciously notes that someone copies it, it can completely break down the compliance (Pineda, 2007).

5) Provoking narcissism - setting-specific issues; The Meta model (Schwarz, Knäuper, & Oyserman, 2008), could prevent the loss of information in communication. The Meta model helps to ask specific questions (*How exactly? What exactly?*). That will provide more information and preventive conflict avoidance.

6) Violation of privacy - Milton's model; The Milton model (Laguerre, 2017) is built around the idea that using a deliberately vague and general language allows your interlocutor to open up his thoughts more easily. Unspecified language refers to words and expressions like somehow, everyone, always, the opinion is valid, people say, is generally known, etc. Using the Milton model increases the chance that the spoken sentence will be in line with the experience of the interviewer.

7) Relativizing the truth – "Yes – set"; This set is a series of statements or questions that the interlocutor answers or thinks, ''yes, yes, yes...''. This repetitive self-obedience opens the stage when an on key question interlocutor will also respond with "yes" (Gravetter & Forzano, 2015).

Applying the Process of Psychological Manipulation

The application of the manipulation method depends on the goal that has to be achieved. The application of methods of psychological manipulation in this paper is illustrated by the example of recruiting people for acts of terrorism based on the abuse of religion on the social network *Facebook*. Steps in the process consider *the definition of the target group* (based on the preview of the social network profile) and *mobilization*. The target group is usually in a pool of young people with problems such as poverty, poor relationships with their families, marginalized groups, from conflict regions, areas with extensive religious conflicts or in societies with significant deviation regarding traditional values. The process of mobilization considers three main process phases – the search, rapprochement and offer.

1) Search is the first step on websites of religious communities, self-taught teachers - interpreters of religion, religious schools and universities or on illegal websites known as "Dark Web". Recruiters (also referred to as "predators") are, most usually, people with excellent "communication" skills. On their social network's posts, they establish content about quite common things, such as devotion to faith, religious morality, avoiding any extremist intentions. The evaluation of the potential candidates' is realized through manipulative methods such as encouraging projection, perceiving inertia attitudes, adaptable non-verbal communication, experience, activities and the degree of socialization.

On Facebook, searching for "friends" is commonly possible by application suggestion, based on the network of existing or possible "friends" ("people you may know"), or by expressed and similar interest ("you may be also interested"). The profile Timeline on Facebook is the "pool" of your current "friends" and this is the best place to look for new friends based on similar interests. Favorite sites and groups on Facebook are also "good" places to search for victims because people who visit those sites have at least one thing in common with the predator. On his profile, the predator creates a "mirror" using previous knowledge about the interviewee (target) attitudes and activities. The implementation considers the following activities:

- Predator access to the *Timeline* of one of the Facebook profiles who has similar interests or interests as the predator. They found a post that the target (victim) particularly likes. Accessing the person who likes or comments on this post, the predator comes to the Timeline of that (targeted) person.
- On the selected Facebook profile, while scrolling through the Timelines, the victim (target) reads the predator's post. By choosing the link "More" below the photo on the cover page of the profile, you can see what types of movies, books, TV shows or music likes, and sees all other interests of the victim.
- By activating the "follow" menu in a photo or set profile image, the future public postings of the victim will appear in the news on the predator pro-

file. The predator marks public posts with "liking" and commented on how to create "mirrors" to start a friendship with the victim. When the predator finds it appropriate, they send a message asking for friendship.

2) Rapprochement starts after choosing the victim, when the predator aims to get closer to them. The predator does their own research, analyzing and learning everything about the family, the past, the interests, and weaknesses of its victim. The manipulative methods used in this step are provoking narcissism - setting up specific questions, manipulating the sense of guilt or social exchange and the methods of deterring privacy using Milton's patterns. This friendly help can be psychological or material. After assisting, the victim feels the pressure to rebound against the demand of the predator, then the predator goes to the next step.

3) The predator offers sacrifices in the form of faith and joins the group or organization that “fights for the right goal”. The victim finally feels accepted and purposeful. Relationships with the organization are growing, and with them, a range of crimes that the newcomers are willing to do in return. The manipulative methods applied here are relativization of the truth - "Yes - set", provocation of sensitivity - the method of small and higher demands - the technique of "foot in the door" and the manipulation of fear - frightening and scattering.

METHODOLOGY AND INTERPRETATION OF RESULTS

To determine the degree of awareness of exposure, and the categorical determination of possible vulnerability to psychological manipulations, as well as preparing preventive measures on social network behavior, we conduct an online survey. The online survey involved 250 people from the Republic of Serbia (75), The Republic of North Macedonia (50), the Republic of Croatia (50), Bosnia and Herzegovina (25), the Russian Federation (25) and the United States (25). The surveyed group consisted of 150 males and 100 females. The educational structure of the respondents is as follows: high school degree - 50 persons, bachelor degree - 100 persons and a master's degree - 100 people. For the survey of 250 respondents, an on-line questionnaire was prepared using the Likert scale of attitudes with the task of expressing the degree of agreement or disagreement on a five-step scale for each claim: "I do not agree at all," "I do not agree," "I do not have an opinion," "I agree" and "I totally agree".

The data processing of the survey was realized in the software tool for statistical data processing "Statistical Package for the Social Sciences". The results are shown in Table 1.

The results of the research indicate that although 79.6% of the respondents are knowingly aware of the possible danger of being manipulated on social networks, they do not check the profile of someone who

wants to be their "friend", but respond to the unknown without previously checking the news on social networks.

Table 1. The data processing of the realized survey

Attitude	Strongly disagree	I do not agree	No opinion	I agree	Strongly agree	Total
Through social networks getting messages that scare me	-	-	-	79%	19,9%	99,6%
				99,6%		
Sometimes I do not agree to do something I do not want	19,9%	59,8%	19,9%	-	-	99,6%
	79,7%					
When I have a problem, I always turn to my first family for help	10%	69,7%	10%	10%	-	99,6%
	79,7%		10%	10%		
I agree to help a friend	-	10%	10%	69,7%	10%	99,6%
	10%			79,7%		
I have a feeling of guilt after accepting a friend's help	-	-	10%	69,7%	19,9%	99,6%
				89,6%		
I put my own images and members of my family on my profile	-	10%	10%	59,8%	19,8%	99,6%
	10%			79,6%		
I often comment on events	-	10%	10%	69,6%	10%	99,6%
	10%			79,6%		
I explicitly respond to explicit scenes of violence	-	-	10%	79,6%	10%	99,6%
				89,6%		
I never answer unknown people	49,8%	39,8%	10%	-	-	99,6%
	89,6%					
I do not share my status on the profile publicly	-	10%	10%	69,6%	10%	99,6%
	10%			79,6%		
Always check the profile of someone who wants to be my friend	10%	79,6%	10%	-	-	99,6%
	89,6%					
I am aware of the danger of being manipulated	-	10%	10%	59,8%	19,8%	99,6%
	10%			79,6%		
I'm always looking for newspapers on social networks before activating an option	10%	79,6%	10%	-	-	99,6%
	89,6%		10%			

PREVENTION OF PSYCHOLOGICAL MANIPULATIONS IN CYBERSPACE

To define preventive measures from psychological manipulations in cyberspace, we use the methods of analytical hierarchical processes (AHP method). The aim was to convert non-material factors into numerical values and systematically evaluate the weights of selected variables in couples through a series of pairing (Saaty, 2008). In research, we used the software "Super Decision 2.6.0 – RC1". AHP method is processed through three phases: 1) data collection, 2) valuation of relative value weights and 3) determining the solution to the problem.

Data collection was conducted "on-line" by interviewing ten experts in the domain field, who were asked to fill in Satie's attitude scale of nine points to rank the importance of the criteria in pairs comparison. The results in Table 2 express Satie's rock attitudes of nine points.

Table 2. Satie's attitude scale of nine points regarding importance criteria.

Scale	Explanation / Ranking
9	Absolutely most important / most preferably
8	Very strongly to the absolutely most important / most desirable
7	Very strong to very important / desirable
6	Strong to very strong
5	Stronger more important / desirable
4	Less to more stronger
3	Less relevant / more desirable
2	Equally to the weaker more
1	Equally important / desirable
0,50	Equally to the weaker ones
0,33	Less significantly less / preferably
0,25	Less strongly towards smaller
0,20	Strongly significantly less / preferably
0,17	Strong to very strong / small
0,14	Extremely vigorously less significant / desirable
0,13	Very strongly towards smaller absolute
0,11	Absolutely the least significant / desirable

The logic diagram of a possible solution for preventive measures, which could contribute to protection against psychological manipulation activities through social networks, is in Figure 1.

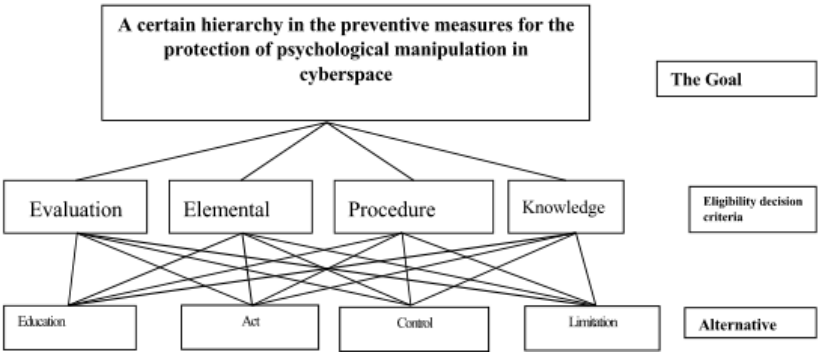

Figure 1. Hierarchy logical network of acts and measures in cyberspace manipulation prevention

As of mid-conclusion, alternatives for psychological manipulation are *education*, *method* and *control limitations*.

Determining the Solution to the Problem

Determining the solution to the problem is the last phase of the AHP method, which means finding a positive normalized vector. After determining the sequence vector of the activity criteria in the model, in the next circle, it is necessary to determine the order of importance of the alternative in the model. Finally, the overall synthesis of the problem is the participation of each alternative multiplied by the weight of the observed criterion. The obtained data represents the influence weight of the observed alternative in the model. The results of the survey for ten experts from the domain area are in Table 3.

Table 3. Experts' survey results regarding preventive alternatives

	Alternatives	**Total**	**Normal**	**Ideal**	**Ranking**
Expert 1	education	0.3393	0.6786	1.0000	**1**
	control	0.0404	0.0809	0.1192	3
	limitations	0.0198	0.0395	0.0583	4
	act	0.1005	0.2010	0.2962	**2**
Expert2	education	0.3482	0.6963	1.0000	**1**
	control	0.0366	0.0732	0.1051	3
	limitations	0.0162	0.0323	0.0465	4
	act	0.0991	0.1982	0.2846	**2**
Expert 3	education	0.3461	0.6922	1.0000	**1**
	control	0.0359	0.0718	0.1038	3
	limitation	0.0146	0.0291	0.0421	4
	act	0.1034	0.2068	0.2988	**2**

Summarizing the results obtained by using the AHP method that determines hierarchy in the application of preventive measures to protect against psychological manipulations in cyberspace is of significance ranked according to the following:

1) First – "education",100% confidence,
2) Second - "procedure", 90% confidence,
3) Third – "controlling", 90% confidence and
4) Fourth – "limits", 100% confidence.

PROPOSED MODEL IN THE APPLICATION OF PREVENTIVE MEASURES

The prevention of harmful effects in cyberspace caused by psychological manipulations based on previous research implies the application of measures in the following domains: *education, procedures, control,* and *limitations.*

In the domain of education, it is necessary to take measures in the constant education of young people on all levels of education about the dangers that they could be exposed to social networks. Besides, an important segment is the education of both the teaching staff and parents.

Prevention considers procedures, which are needed to be taken to protect privacy on social networks. Useful recommendations consider to avoid blind trust regarding "default" settings on sites, but try to evaluate the "settings" to choose the appropriate level of protection. Also, it is better not to share close information about yourself, family, or anyone else in the "online" area, even personal contact information, in open form, as well as carefully use social networking based on locating ("geotagging", "FourSquare", "checking"). These services make your daily habits available to the broad public, even to those with malicious intent. Furthermore, the suggestion is that one should not "blindly accept" friend suggestions, nor allow access to people they do not know and do not trust. Regularly review your friends and delete those with whom you are not close. If you choose to add your professions or contacts from your profession to your network, consider the option of adding them to a separate list or group and limiting/protecting what you share with that list/group. Furthermore, everything that is published on the Internet can easily be split, drawn out of context, or abused. For sure, strong passwords to protect the login to a personal account are advised.

Control as a preventive measure is a set of procedures to gain insight into the degree of disruption of privacy and functionality on the one hand, and control of the validity of the sites we visit.

Restricting access to certain sites on the Internet, in particular social networks, is an alternative that is the lowest-ranked as a preventive measure and represents the ultimate measure, which is also a measure affecting the freedoms and rights of citizens. This measure is applied when the previous measures were not applied or when they did not yield results.

CONCLUSION

Successful strategic communication (SC) has to be a planned activity where the key for success lies in the solid analyses of the environment, stakeholders and objects. The environment of communication has various dimensions and in the contemporary world, cyberspace has a unique significance, with strong influence in almost all physical dimensions. Supported by technology and globalization of media and broadband Internet contexts, especially through social networks, cyberspace is a strong tool for shaping the public opinion, behavior predictions, as well as attitudes and mass motivation management.

In this paper, methods of psychological manipulation are analyzed as a kind of social impact that aims to change the perception or behavior of other people by concealing, deceiving or abusing. Research consequently aims to examine the relation of SC and abusing of Internet social networks, from point of national defense and security, in the form of mobilization for extremism and terrorism. An online survey of 250 respondents determined the level of awareness about exposure to psychological manipulations, categorical determination, and preventive measures against their influence.

The research results indicate a low level of social network abuse knowledge, insufficient motivation for education, without the knowledge of procedures that can reduce the negative effect of psychological manipulations, and lack of control of truthfulness and evaluation of Internet content. Social networks, because of their popularity and "easy and quick" access, represent unique favorable polygons for aching malicious psychological manipulation and influence.

The application of the AHP method in this work identifies measures of prevention against harmful effects in cyberspace caused by psychological manipulations, and these are ranked by significance to the following: education, procedures, control, and limitations. Based on the identified measures and their significance as ranked preventive measures, the proposal of modeling contents for preventive measures against psychological manipulations in cyberspace is elaborated.

The results of the researches shown in this paper point to the danger of predators acting on the belief of potential victims, which, in the end, can have great negative consequences for both the individual and the wider social community in form of rising extremism beliefs and terrorists acting.

REFERENCES

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior (11-39). In Kuhl J. and Beckmann J. (Eds.). *Action Control*. SSSP Springer Series in Social Psychology. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I. (May 27, 2019). Summary of Theory of Planned Behavior - Abstract. Retrieved from http://www.valuebasedmanagement.net/methods_ajzen_theory_planned_behaviour.html.

Benoit, W., & Benoit, P. (2008). *Persuasive Messages: The Process of Influence*. Hoboken, New Jersey: Wiley-Blackwell.

Bernstein, G.A., & Borchardt, C.M. (1991). Anxiety disorders of childhood and adolescence: a critical review. *Journal of American Academy of Child and Adolescent Psychiatry,* 4, 519-532. https://doi.org/10.1097/00004583-199107000-00001

Braiker, H., (2004). *Whos Pulling Your Strings? How to Break The Cycle of Manipulation*. New York City: McGraw-Hill.

Christopher, P., (2011a). *Getting Better at Strategic Communication*. Santa Monica: RAND Corporation.

Christopher, P., (2011b). *Strategic Communication Origins, Concepts, and Current Debates*. Santa Barbara: Praeger.

Deng, Z., & Liu, S. (2017). Understanding consumer health information-seeking behavior from the perspective of the risk perception attitude framework and social support in mobile social media websites. *International Journal of Medical Informatics,* 105, 98-109. https://doi.org/10.1016/j.ijmedinf.2017.05.014

Gravetter, F., & Forzano, L.A. (2015). *Research Methods for the Behavioral Sciences*. Mason, OH, United States: CENGAGE Learning.

Gupta, A., & Dhami, A. (2015). Measuring the impact of security, trust, and privacy in information sharing: A study on social networking sites. *Journal of Direct, Data and Digital Marketing Practice*, 17(1), 43-53. https://doi.org/10.1057/dddmp.2015.32

Hallahan, K., Holtzhausen, D. R., Van Ruler, B., Verčič, D., & Sriramesh, K. (2007). Defining strategic communication. *International Journal of Strategic Communication,* 1(1), 3–35. https://doi.org/10.1080/15531180701285244

Hansen, W. (2013). *Influence: theory and practice* (Master of Science thesis). Monterey California: Naval postgraduate school.

Holtzhausen, D., & Zerfass, A. (2015). Strategic Communication: Opportunities and Challenges of the Research Area (3-17). In the Holtzhausen, D. & Zerfass, A. (Ed.). *The Routledge Handbook of Strategic Communication, Routledge*. New York: Routledge.https://doi.org/10.4324/9780203094440

Kosinski, M., Bachrach, Y., Kohli, P., Stillwell, D. & Graepel, T. (2014). Manifestations of user personality in website choice and behavior on online social networks. *Machine Learning,* 95, 357-380. https://doi.org/10.1007/s10994-013-5415-y

Laguerre, J. (May 4, 2017). The Milton Model: 27 Powerful Language Patterns. *Power Creativity Institute*. Retrieved from https://www.pciinstitute.net/nlp/milton-model/

Mitrović, M. (2017). Lobbying-Managing with Strategy Orientated Communication. *Political behavior: Cognition, Psychology, & Behavior eJournal.* https://doi.org/10.2139/ssrn.2942002

Mitrović, M. (2019a). Strategic communication in the function of national security. *Vojno delo*, 1(19), 41-54. DOI: 10.5937/vojdelo1901041M.

Mitrović, M. (2019b). Determinants of Strategic Communication Significant for National Defense and Security. *Matica Srpska Social Sciences Quarterly, LXX, 170*, 179-194. https://doi.org/10.2298/ZMSDN1970179M

Mitrović, M. (2019c). Strategic communication concept implemented through the corporate political activities – suggested strategy modeling. *Strategic management,* 24(4), 13-20. DOI: 10.5937/StraMan1904013M

Mitrović, M., & Miljković, M. (2018). Hybrid genesis of information operations in cyberspace. *TEME,* XLII, 1359-1372. https://doi.org/10.22190/TEME1804359M

Mitrović, M., & Vulić, A. (2019). Project Management of Strategic Communication in Digital Era. *Advances in Economics, Business and Management Research*, 108, 76-82. https://doi.org/10.2991/senet-19.2019.13

Pineda, J. (2007). *Mirror neuron systems: The role of mirroring processes in social cognition*. Atlanta, GA: Emory University.

Pissanidis, N., Rõigas H. & Veenendaal, M. (2016). Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. *Proceeding from 8th International Conference on Cyber Conflict Cyber Power*. Tallinn: NATO CCD COE Publications.

Power, R.A. & Pluess, M. (2015). Heritability estimates of the Big Five personality traits based on common genetic variant. *Translational Psychiatry*, 5(7), *e604*. doi: 10.1038/tp.2015.96

Pratkanis, A. (2007). Winning Hearts and Minds: A Social Influence Analysis (pp. 56-85). In Arquilla, J. & Borer, D. (Ed.). *Information Strategy and Warfare*. New York: Routledge, 2007. https://doi.org/10.4324/9780203945636.ch3

Rot, N. (2006). *Osnovi socijalne psihologije*. [Basics of social psychology]. Beograd: Zavod za udžbenike i nastavna sredstva.

Saaty, T.L. (2008). Decision Making with Analytic Hierarchy Process. *International Journal of Services Science*, 1, 82. http://doi.org/10.1504/IJSSCI.2008.017590

Sartonen, M., Huhtinen, A.M. & Rhizomatic, M. L. (2016). Target Audiences of the Cyber Domain. *Journal of Information Warfare,* 15(4), 1-14.

Schwarz, N., Knäuper, B. & Oyserman, D. (2008). The Psychology of Asking Questions. In Leeuw, Joop Hox, Don Dillman (Ed.). *International handbook of survey methodology*. Abingdon-on-Thames, Oxfordshire United Kingdom: Taylor & Francis.

Vasiljević, D., Vasiljević, J. & Djurić, A. (2018). Cyber space - definition and classification (pp. 214 – 227). In Nikolić, N. (Ed.). *Hybrid Warfare - contemporary conflict dilemma*. Belgrade: Strategic Research Institute.

Vidanović, I. (2006). *Rečnik socijalnog rada*. Beograd: Tiro-erc.

СТРАТЕШКА КОМУНИКАЦИЈА И УТИЦАЈ ДРУШТВЕНИХ МРЕЖА: МЕТОДЕ ПСИХОЛОШКИХ МАНИПУЛАЦИЈА У САЈБЕР ПРОСТОРУ И ПРЕДЛОГ ЊИХОВОГ СПРЕЧАВАЊА

Мирослав Митровић[1], Драган Васиљевић[2]
[1]Институт за стратегијска истраживања, Универзитет одбране Београд, Србија
[2]Генералштаб Војске Србије, Србија

Резиме

Стратешка комуникација представља једну од резултанти друштвених интеракција у глобалном свету. Кроз њу се очитава широк спектар комуникацијских форми које су од одлучујућег утицаја на остваривање мисије организације. Државе спровођењем стратешке комуникације остварују циљеве који су од највишег националног значаја, а налазе се у дискурсу јавне и класичне дипломатије, пропаганде, лобирања итд. Стратешка комуникација се спроводи у свим сферама деловања људске размене иформација, па тако и у сајбер простору. У овом виртуелном простору су услед готово непрекидне технолошке револуције у актуелном тренутку интензивне све, па и манипулативне, комуникацијске праксе. Са становишта стратешке комуникације, од значаја за националну одбрану и безбедност, посебно су битне мотивишуће форме утицаја на когнитивне и психолошке карактеристике популације.

Осим мотивишућих утицаја, који позитивно опредељују популацију према питањима од значаја за одбрану и безбедност, са становишта истраживања у области одбране, од великог значаја су комуникацијске форме које неповољно и деструктивно утичу на друштво. Овакве појаве су у савременој теорији конфликата препознате као један од садржаја неконвеционалних, хибридних форми угрожавања безбедности.

У остваривању циљева, које се у овом раду односи на потенцијално врбовање за ектремистичко и тероритичко деловање на основу злоупотребе садржаја на друштвеној мрежи Фејсбук, субјекти манипулације према жртвама користе све до сада од науке и праксе препознате методе управљања вољом, предвидивог понашања и психолошких манипулација.

У раду се, на основу анализе психолошких модела управљања понашањем и психолошких манипулација, приступило емпиријском истраживању, спроведном преко интернета, у коме је анализирана свест корисника о опасностима и могућим манипулативним садржајима на друштвеној мрежи Фејсбук. Даљом применом AHP методе, извршено је рангирање потенцијалних форми превенције и одбране од зло-

употреба на друштвеним мрежама. Истраживање у форми закључка сведено нуди садржаје и активности којима је могуће обезебедити превенцију, одбијање и одбрану од злоупотребе личних садржаја на друштвеним мрежама, а који могу послужити као основа за примену манипулативних психолошких форми. На овај начин, превенција у домену комуникације на интернету омогућава далекосежне ефекте на стратешку комуникацију од значаја за државу, омогућавањем потенцијалног спречавања малициозног продора у свест појединца, који се спроводи са циљем његове мобилизације за деловање опасно по националну одбрану и безбедност.