Dr Miroslav Mitrović

Strategic Research Institute, University of Defence in Belgrade, 1 Veljka Lukica Kurjaka str. 11000 Belgrade, Serbia

E-mail: mitrovicmm@gmail.com

DOI:

Original Research Paper

Received: September 09, 2022

Accepted: October 14, 2022

RUSSIAN STRATEGIC COMMUNICATION - ENDLESS INFORMATION WARFARE

Abstract: *Strategic communication determines the communicative aspects of national soft power, and it is an integral part of the national security structure of a modern state. Russian military thought makes a substantial deviation from the term „strategic communication", defining and applying the communicative contents of soft power by the terms „information security" and „information warfare". Russian understanding uses these forms of strategic communication in a constant struggle for supremacy and control of all information domains. Thus, Russia declares a permanent state of war in the information sphere. Based on a comprehensive analysis of the Russian scientific and operational approach to the interpretation of strategic communication, the article provides insight into Russia's basic idea and genesis of information warfare. By reviewing strategic documents and applied organisational forms, the paper contributes to understanding the vital level of strategic communication on the applied aspects of national security of the Russian Federation. The article elaborates application forms of the Russian's concepts of information security and information warfare, information operations, and psychological operations. Paper offers a case of Russia's information warfare toward Serbia. Conclusively, Russia is very active in an informative sphere in international relations, which should have in mind in the relations with that power.*

***Keywords**: strategic communication, national security, information security, information warfare, information operations, psychological operations, Russian Federation, Serbia.*

1. INTRODUCTION

There is a disagreement in using the term „strategic communication“ between Russian and Western authors, but the essence of the understanding is almost identical: strategic communication refers to one of the expressions of state power. Strategic communication reflects the state's soft power, directly related to its national security issues, and it aims to use communication means to achieve the set national interests (Mitrović, 2019a). It is an instrument in the political and security realisation of national interests. In the context of contemporary conflicts, it is an expression of hybrid action in the sphere of information, media, the Internet, and public diplomacy (Mitrović, 2018a). Globalisation has contributed to the misuse of the media for geopolitical purposes, and the production and management of media content plays a significant role in modern hybrid wars (Jakovljević and Šćekić, 2018). The most common form of media abuse is manipulation to raise political tension and mobilise the public to support military intervention (Mitrović, 2020). In general, the function of strategic communication is to use propaganda to influence one's own and foreign public opinion (Mitrović, 2018b). The main goal of the impact is to shift the focus of the public's attitude towards cultural values and the eventual adjustment of the political system through the „reprogramming“ of political culture following the set goals (Mitrović and Nikolić, 2022: 233-277).

2. RUSSIAN STRATEGIC COMMUNICATION APPROACH

Instead of „strategic communication“, Russian experts and strategic documents that treat the field of defence and security use „state information policy“, „information security“, „information support to foreign policy activities“, and other related terms (Pashentsev, 2020). In

short, the Russians identify the scope of action, forms, and contents of strategic communication with the words „information security“ and „information warfare“. According to Russian thought, today's level of development of means for influencing information enables them to solve strategic tasks (Chekinov and Bogdanov, 2011). They are achieving victory in the confrontation of information results in the achievement of strategic and political goals and the defeat of the enemy armed forces, the occupation of its territory, the destruction of its economic potential, and the collapse of its political system (Slipchenko, 2013). More precisely, information warfare in all domains (social, political, media) impacts the mass consciousness of opponents, which in some instances can completely replace the engagement of the armed forces (Kartapolov, 2015). They are very active towards the general external population, other armed forces, and the governing structure (Mitrovic, 2021). In their performance, they apply a whole range of communication and subversive instruments based on the determinants of strategic communication (Mitrović, 2019b). By acting on the mass consciousness, the population is directed to support the aggressor, acting against their interests (Kuleshov et al., 2014: 106).

In the works of Russian authors, however, the use of the term „strategic communication“ is observed through its manifestations: public affairs, public diplomacy, and information security systems (Pashentsev, 2020: 127). Information is at the centre of both information security and information warfare. Russia's approach indicates that entering corrupted data into a computer over a network or flash drive is not conceptually different from placing misinformation in the media (Giles, 2016: 8).

2.1. RUSSIAN SC STRATEGIC DOCUMENTS AND ORGANISATION

National Security Strategy of the Russian Federation (RFNSS, 2015) states that the increasing influence on international relations is exerted by the increased confrontation in the

global information space. The document, Basics of the state policy of the Russian Federation in the field of international information security for the period until 2020 (FSPRFIS, 2013), recognise the main threats to global information security as the use of information and communication technologies:

a) As an information weapon for politico-military purposes contrary to international law, for committing hostile and aggressive actions aimed at discrediting the sovereignty, territorial integrity of states and as a threat to international peace, security, and strategic stability;

b) For terrorist purposes, including the exercise of destructive action against elements of critical information infrastructure, as well as for the promotion of terrorist and terrorist activities to attract new supporters;

c) Interventions in the internal affairs of sovereign states, disturbing public order, inciting ethnic, racial, and religious hatred, propagating racist and xenophobic attitudes or theories that generate hatred and discrimination, and incite violence.

Information society development strategy (SDISRF, 2017) defines goals and measures for implementing internal and foreign policy in information and communication technologies.

The Doctrine of information security of the Russian Federation (DISRF, 2017) defines information security as a state of protection of individuals, society, and the state from internal and external threats to information that may violate, among other things, sovereignty, territorial integrity, sustainable socio-economic development, and defence and security of the state. The Russian military doctrine (MDRF, 2014) also deals with the aspect of the information space, with a pronounced shift of military risks and threats into the information space and further into the internal sphere of Russian society. At the same time, although the start of the war against the Russian Federation is less and less probable, the Russian Federation's (RF) military risks are

increasing in numerous areas. Accordingly, the RF Armed Forces should develop information and communication technologies for military-political purposes, act against the establishment of regimes whose policies endanger the interests of the RF in neighbouring countries, and prevent subversive operations of special services and organisations of foreign states their coalitions against the RF. In organisational terms, in 2014 established the National Centre for Defence Management, which represents the highest level of information management and functionally directs and synchronises the work of the entire defence system. The centre's role is significant in synchronising hybrid and information warfare (NCDMRF, 2021).

3. INFORMATION SECURITY AND WARFARE

According to Russian authors, information security is a condition that ensures the security of information from unauthorised modification or destruction. Russia's access to strategic communications is divided into two fields of action: internal information security and external information warfare.

3.1. RUSSIAN INTERNAL INFORMATION SECURITY

Information control is a basic form of internal information security and represents the legacy of the Soviet Union. Eavesdropping on telephone conversations was one of the primary methods of controlling the exchange of information within the country and in contact with the world (Soldatov and Borogan, 2015). The danger was also seen in the possible reproduction of information material (Soldatov and Borogan, 2015:17-18).[1] Owners of radios had to register it until 1962, and the KGB also had a record of typewriter machines fingerprints to prevent the multiplication of „dangerous“ materials (Soldatov and Borogan, 2015:21). In addition to direct

[1] The forerunner of today's photocopier was invented and made in the Soviet Union in 1954 Electrophotographic copier machine no.1, [ru: *Электрофотографический копировальный аппарат по. 1]*, and in 1957 it was destroyed by the USSR State Security Committee (KGB). The reason is the danger that "some prohibited materials may be copied and reproduced". (Soldatov and Borogan, 2015:17-18).

communication with foreigners, telephone communication was also prohibited (Soldatov and Borogan, 2015: 22-25).

The current approach indicates that Russia's awareness of information security issues has not advanced significantly since the Cold War. Namely, Russia improves the system for identifying and analysing threats in the information sphere to improve national security. They take measures to increase the protection of citizens and society from the impact of destructive information of extremist and terrorist organisations, foreign special services, and propaganda structures (RFNSS, 2015). In that way, the national information security defined enables the control of the flow of information. The actions and reactions of the authorities indicate that the Russian defence information approach recognises the greatest danger in the possible development of critical thinking of its population. This approach leads to a permanent suspension of internal informative essential content, striving for absolute control and the result of a confrontation campaign against information coming from outside Russia (Giles, 2016: 36).

In organisational terms, the institution dealing with electronic surveillance and cryptography in Russia since 1991 is the Federal Agency for Government Communications and Information (FAPSI, 2021), which was restructured in 2003 into departments located within the intelligence and security services. The direct successor, which took over the information control functions, is the Special Connection and Information Service (SCIS, 2021) (ru. *Спецсвязь России*), which is part of the Federal Security Service of the Russian Federation (FSSRF, 2021). At present, Russia continues to implement active rigorous control measures, in particular Internet communications, through technical surveillance systems, such as the Operational Search Measures System (ru. *СОРМ*) (Soldatov and Borogan, 2015: 63-71). In addition, there is active support for opinion centres based on the media and social networks (Soldatov and Borogan,

2015:103). In the context of information warfare on the Internet, the state's role is organised by Internet *trolls* and *bots*. An Internet *troll* is a person who posts topics and comments on social networks and electronic internet media (forums, social networks, news, virtual chat rooms) to provoke readers and their emotional or other reactions that disrupt regular discussion about the topic. A *bot* is a term that defines electronically generated, artificial intelligence, inhuman, virtual identity, created to create comments and reactions for suspension and visibility of harmful critical content. The so-called „troll farms“ are strongholds of „hacker-patriots“. These groups are particularly active in denying the distributed denial of service (DDOS). Russia's participation in international telecommunications and information exchange systems is not considered possible without a comprehensive solution to the problem of information security, which would mean physical control over the input and output hubs of Internet operators or social network service servers (Smolyan et al., 1995). Based on the example of the role of the Internet in the Arab Spring (Zheltov and Zheltov, 2014; RIA Novosti (2011); Medvedev, (2011), Russia concludes that the lack of control over information, especially that spread by social networks, poses the greatest threat to the internal security of the RF (Szpyra, 2020).

3.2. RUSSIAN INFORMATION WARFARE

Russia defines information warfare as a conflict between two or more states in the information space to damage information systems, processes, and resources, critical and other structures, undermining the political, economic, and social system, mass psychological processing of the population to destabilise society and the state (CIIS, 2011).

Russian thought distinguishes between information conflicts in peace and war. These are primarily covert measures in peacetime (reconnaissance, espionage, building one's own and reducing the enemy's information capabilities). In a war, they are more aggressive and include

„discrediting (the enemy's) leadership, intimidating military personnel and civilians, falsifying events, misinformation and hacker attacks“ (Sharavov, 2000). In the context of information warfare, „the main effort is concentrated on achieving political or diplomatic goals and influencing the leadership and public opinion of foreign states, as well as international and regional organisations“ (Efimovich and Nikitin, 2005). Based on this, Western analysts conclude that current and recent Russian information activities, especially in Ukraine and Syria, and indirectly and lower intensity in many other countries, indicate that Russia considers itself in an (informative) state of war (Giles, 2016:8).

According to Russian authors, the information war is an intense confrontation in the information space to achieve informational, psychological, and ideological superiority, damage to information systems, processes and resources, critical structures and communications, undermining political and social systems, and mass psychological processing of the military staff and the general public (Chekinov and Bogdanov, 2015). Information warfare is viewed in two ways:

- In the broadest sense, refer to the confrontation in the information environment and the media to achieve different political goals;

- In a narrower sense, it is an information war, i.e. a military confrontation in the information sphere to achieve advantages in collecting, processing, and using the information on the battlefield, reducing the effectiveness of enemy actions (Danilevich et al., 2011).

Russian Security Encyclopedia (RSE, 2021) describes information war as measures taken to achieve information superiority, confrontation of states in the information space, and the most significant degree of information conflict between governments when its structures conduct information operations to achieve military-political goals. The same source defines information

weapons as a set of unique methods (physical, information, software, radio-electronic) and means intended for temporary or irreversible disabling of functions or services of information and communication infrastructure as a whole or its elements. Furthermore, an information operation is a set of organised activities for collecting and accumulating, preparing, distributing, restricting access, or processing information to achieve a set goal.

In summary, the Russian concept of information warfare, in principle, sublimates action through and over computer networks, along with psychological operations, strategic communication, influence operations, intelligence and counterintelligence, camouflage, disinformation, electronic warfare, weakening communications, deteriorating navigation support, psychological pressure, and destruction of hostile computing abilities (Sharavov, 2000). All of the listed constitutes „a system, methods, and tasks that affect the perception and behaviour of the enemy, the population and the international community at all levels.“ (Selhorst, 2016: 151).

According to Russian military theorists, information warfare, depending on the goal, object of action, and circumstances of conducting operations, can be viewed as:

- Information-psychological war (which affects the enemy's manpower, armed forces, and population) is conducted in conditions of natural competition, i.e., continuously, permanently; (Kuleshov et al., 2014).

- Information technology war (which affects the technical systems that receive, collect, process, and transmit information) is fought during wars and armed conflicts (Квачков, 2004).

4. INFORMATION AND PSYCHOLOGICAL OPERATIONS

Member of the Scientific Board of the Security Council of the Russian Federation, Andrei Manoilo, believes that aggressive forms of information warfare are inevitable in the conditions of dynamically growing globalisation and modern geopolitical competition (Manoilo, 2003). This

kind of thinking relies on Aleksandar Karajanin, who in 1997 made a considerable contribution to the broadest understanding of information warfare. At the same time, he emphasises the difference between informational and psychological warfare. According to him, information and psychological activities are carried out at all levels (interstate or strategic, operational and tactical), in peace and war, in the informational and spiritual spheres, and according to one's own and adversary forces (Karayani, 1997).

Information warfare is the struggle of opposing parties to achieve supremacy over the enemy through the timely, reliable, complete collection of information, speed, and quality of their processing and communication with the direct performers of information actions. The means used in information warfare are 1) Computer viruses; 2) „Logic bombs“, „werewolf programs“, „information killing programs“ and other previously entered, activated if necessary software; 3) Programs for unauthorised access and theft of information; 4) Means for suppressing information systems, entering them to replace information or open propaganda intervention; 5) Biotechnological tools, created based on cell engineering; 6) Means for introducing viruses, logic bombs, werewolf programs, programs for killing information, programs for influencing staff („zombies“), into information systems (viral rifles, microprocessor bookmarks, international computer networks) (Karayani, 1997).

An information operation is a form of information warfare. It includes a comprehensive term that combines the concept of electronic warfare, computer network operations (electronic warfare), psychological operations, and military deception. All of this is conducted to influence or interrupt normal activities, damage or override the enemy's decision–making command structures, as well as measures aimed at improving their security from relevant enemy activities (Danilevich et al., 2011). At the same time, they have a technical-technological and a socio-

psychological aspect (Slipchenko, 2003). As the most critical segment of the information operation, a psychological operation is recognised, which has a double effect and meaning. According to the narrower approach, military psychological operations are informative activities of the armed forces, which leads to demoralisation and disruption of the opponent's organisation. In a broader context, a psychological information operation is any organised activity of a governmental and non-governmental institution in peace, in times of increased danger and war, which aims to change the attitudes of opponents, allies, or undecided publics, representatives of the armed forces and civilians. Both approaches include agitation, propaganda, and other activities influencing awareness, emotions, motives, reasoning, self-confidence, and finally, the target group's behaviour (Danilevich et al., 2011).

Psychological warfare is a struggle between states and their armed forces to achieve superiority in the spiritual sphere and turn the acquired advantage into a decisive factor in achieving victory over the enemy. It is implemented through 1) Mobilisation and optimisation of moral and psychological forces; 2) Protection of the population and members of the armed forces from the influence of the enemy; 3) Psychological impact on enemy troops and the population (psychological struggle); 4) Influence the attitudes, moods, and behaviour of a friendly and neutral audience. Short-term or narrowly focused informative and psychological actions, carried out in peace and war, in any territory, i.e. population, are called psychological operations (Karayani, 1997).

Psychological operations are divided into strategic, operational, and tactical. Strategic psychological operations are performed globally to achieve long-term goals. Operative psychological procedures are performed in specific regions and strive for medium-term goals. Tactical, psychological operations are performed with short-term goals and are aimed at

supporting combat operations of troops at the tactical level. Psychological operations of all levels form a unique integral complex of related activities, from which it is difficult to isolate one or another (Karayani, 1997). For the needs of psychological operations, modern achievements of psychology are used based on the identification of sensitive characteristics of the human and group psyche, development of effective methods for assessing the psychological state of the enemy, planning effective forms of psychological struggle, developing criteria and procedures for evaluating the effectiveness of psychological effects on people. Special attention in the planning of psychological operations is paid to the application of the results of assessments related to:

- The role of the subconscious in determining human behaviour and the functioning of psychological defence mechanisms and ways to overcome them (psychoanalysis);
-Reflective influence („anchoring“, „zombification“), emotional tone, behaviourism, neurolinguistics programming;
- The role of „mental patterns“ in the perception of the surrounding world, events, and information (cognitive psychology);
- Structure and dynamics of human needs (humanistic psychology) (Karayani, 1997)

In achieving the effects of psychological surgery, psychological assessments have a crucial role, which helps planners of psychological operations identify the weakest links in the opponent's moral and psychological state and build psychological pressure tactics on him.

The differences between psychological and information warfare are pointed out by Sergej Berezin, who states that despite the existence of closeness, especially in terms of effects, there are also differences, which determine the difference in planning and implementation. According to him, information warfare aims to achieve information domination and prevent opponents from

using the information space. Psychological warfare seeks to combine different forms, methods, and means of influence to change psychological characteristics in the desired direction and group norms, mass feelings, and public awareness in general (Berezin, 2003).

5. CASE RUSSIAN'S OF INFORMATION WARFARE IN SERBIA

The Serbia and Western Balkans region is not the current focus of the Russian foreign policy (The Concept of the foreign policy of the Russian Federation, 2016). Moreover, this region is entirely left out from strategic documents, which indicates that they are not at the top of Russian foreign policy engagement priorities (Nikolić, 2019). Nevertheless, a change is possible, and an approach to the Western Balkans could be shaped by: 1) Shifting from bilateral to multilateral cooperation; 2) Creation and support of political forces in Serbia, Slovenia, Croatia, Albania and other countries in the region that would be pro-Russian; 3) Expansion of the Russian media presence in the Balkans; 4) Continuation of economic investments in regional industrial and energy projects; 5) Intensification of educational, trade and cultural cooperation; 6) Constructive approach to religious issues; 7) Development of multilateral cooperation platforms in which Russia actively participates or dominates and attracting the countries of the Western Balkans region to participate in them (Entina and Pivovarenko, 2019).

In contemporary Russian's information warfare toward Western Balkan, Serbia has some specificity: tiny Russian minority, absence of active Russian language usage, war legacy with NATO and US, frozen conflict with „Kosovo", disputes regarding unsolved „Serbian question" in neighbouring states, uncleared and indecisive approach toward EU integration. Based on this, Russia combines different forms of influence, considering its aim and conditions of implementation.

Russians tend to communicate with a broad range of target groups: young, middle-aged, religious, traditionalist, oriented towards culture, Slavic, transition losers, victims of the wars and their families, nationalists, and ultra-right-wing politicians. In addition, a broad spectrum of instruments are applied: economic, energy, media, cultural, religious, and defensive. It is noticeable that the Russian soft power machine forcefully strives towards a unique purpose: strengthening Russian external political positions in the Balkan region by using Serbia as a proxy.

Since 2005 Russia has conducted profiled strategic communication towards the Western Balkans, especially Serbia, using a distinctive offensive appearance that has become more intense since 2015. In this period, Russia has established 109 organisations in Serbia that promote different aspects of Serbian-Russian relations in different areas (CEAS 2016):

Media - two central rows: First, sponsored media is hard to recognise due to the non-ownership transparency and lack of law regulation. However, Russian officials lead all of them (ML, 2021). The second is direct influence by media centre Sputnik Serbia (Sputnik, 2021) and Russia Today. Sputnik is a powerful instrument for creating and disseminating Russian soft power in Serbia. Most of the biggest national publishing agencies (*Večernje Novosti, Politika, Pink, Studio, B, Informer, Pečat, NSPM, Standard, Novi Standard*, and *Pravda*) directly spread Sputnik's news and comments.

- Internet platforms, cultural and informational hubs connected with the Russian Cultural Center in Belgrade (Russian Home, 2021). An Internet-based platform *About Serbia in Russian* (2021), has the supporting role of understanding the Russian – Serbian relations and has a significant contribution in fulfilling the „no limits" pressure on the Serbian public audience.

- Social networks - There are a numerous very proactive open and closed Facebook groups with tens of thousands of members: For brotherhood with Russian brothers (srb. *За братство са браћом Русима*), All of us who are for Putin and Russia (srb.*Сви ми који смо за Путина и Русију*), Vladimir Putin – Serbia (srb. *Владимир Путин – Србија*), Serbia Russia (srb. *Srbija Rusija*), Vladimir Putin Fun Club Serbia (srb. *Владимир Путин фан клуб Србија*), Russians news (srb. *Руске вести*), Russian Friendship Association (srb. *Друштво пријатеља Русије*), Euro – Asia Union (srb./ru. *Евроазијска Унија-Евразийский союз*), Glory to Russia (srb. *Slava Rusiji*), Serbian Russian movement – wolfs (srb. *Srpski Ruski pokret vukovi*).

- Russian compatriot organization in Serbia; Some of them are: *Sveslavica* mainly acting through direct contacts, local media and Youtube; General Cadet Association of Russian Cadet Corps Abroad (ru. *Общекадетское Объединение Русских Кадетских Корпусов за рубежом при Русском Доме в Белграде*); Association of Russian Compatriots „Luč“ (ru. *Общество российских соотечественников* „Луч“); Association of Compatriots and Friends of Russia (ru. *Общество соотечественников и друзей России "Россия"*); Association of Serbian–Russian Friendship Colonel Rajevski [ru. *Общество сербско-русской дружбы "Полковник Раевский"*); The Serbian–Russian Association Bela Crkva (ru. *Сербско-русское общество "Белая Церковь"*); Russian Wave (ru. *Русская волна*), Society for the Preservation of the Memory of Russians in Serbia (ru. *Общество сохранения памяти о русских в Сербии*), Association Homeland (ru. *Общество "Домовина"*). Beside that all of them are listed on website of organisation *Russian Home*, their web pages are unavailable and there are no official records of their membership or activities.

- Political parties; Regarding CEAS (2016) in Serbia acting the 14 active pro-Kremlin political structures (7 are in the Registry of Political Parties, five are in associations of citizens in

the Business Registers Agency, and two movements are not registered at all). Resigned pro-Russian political parties which are active in Serbia: Serbian Radical Party, Democratic Party of Serbia, Dveri, Third Serbia, the Russian Party, the Party of Russians in Serbia, the Serbian Russian Movement, the Time for Action – Serbian League, the Serbian League – New Serbian Right-Wing Movement, the Movement „Svetozar Miletić“, the State Movement, the Serbian Patriotic Front, and the United Russian Party.

- Associations of citizens; According to data, since 2017, 51 pro-Russian associations have been operating in Serbia (CEAS, 2016), with a dominant, strong note of characteristics Euro-skepticism. Some of most influenced are: The Serbian Patriotic Movement Zavetnici (srb. *Српски сабор Заветници*), Serbian national movement „Ours“ (srb. *Српски народни покрет „Наши“*), and Serbian national movement 1389 (срб. *Српски народни покрет 1389*). Those three movements are very proactive in cyberspace, with more than 40 profiles and thousands of members.

Russia officially does not list Serbia’s aspiration to EU membership as an endangering of its interest. Aspects of Serbia's accession to the EU, apart from the Common Foreign and Security Policy and the current sanctions due to the annexation of Crimea, are not significant for Russia and its attitude towards Serbia. Official Moscow declared commitment to implementing UN Security Council Resolution 1244 and encouraged Belgrade and Pristina's talks, supporting any acceptable solution from Serbia's point of view. However, at the same time, through the creation of daily public discourse, by the prevalent dredging up of memories from the 1999 NATO campaign against Yugoslavia, Russia actively attempts to manipulate the emotions and memories of the population. Main channels of influence are primarily through Russian sponsored organisations putting pressure on the public audience against NATO and US. It created an

atmosphere among a broad public audience that does not recognise any good aspects of cooperation with others regarding security and defence, only with Russia (Novaković et al., 2021).

Information instruments, mainly focused on perception management, are recognised in the operation of the Russian cultural associations, media, and manipulations with the over-dimensioned closeness of the two nations, the Orthodox Church, political party, sponsored civic movements. Bešlin explains that „Russian soft power in Serbia in modern times often uses distorted interpretations of historical events, spreading the myth of the 'centuries-old friendship', 'Slavic and Orthodox brotherhood', and 'traditional historical ties' of the Serbian and Russian peoples. Particularly widespread is the myth of Russia as the 'protector' of the Serbs, the Russian 'sacrifice' for Serbia, and how Russian imperial aspirations are not historically verified, but that Russia was coming to Southeast Europe to 'defend centuries-old friends. In contrast to these widespread ideas, rational and critical historical science has a different perspective. Russia is an empire, and like other big powers in the Balkans, it has exercised its imperial intentions. This policy, with certain modifications, has survived over more than two centuries without changing its essential characteristics" (Bešlin, 2016:49).

According to the survey of the Center for Euro – Atlantic Studies (CEAS) in Belgrade, Russian's aims of information warfare in Serbia are 1) Reworks history; 2) Perverts the concepts of democracy, civil society, transitional justice, and EU integration; 3) Demonises NATO; 4) Successfully introduces propaganda into the media; 5) Establishes structures that are only seemingly democratic; 6) Chooses methods of operation that seem democratic, but are not, abusing the achieved level of democratisation in Serbia (CEAS 2016:17).

Expansion strategic communication efforts in Serbia of Russian derived on several main pillars: sponsoring ethnic cultural-related organisations, fostering relations between Serbia and Russian Orthodox Churches, support of political movements, support of political parties, and ownership under Internet and media-based organisations. An example of an offensive approach is in sponsoring ethnocultural organisations. Besides that an ethnic Russians are a tiny ethnic community[2], between 2005 and 2016, eight Russian ethnic-cultural organisations were established in the Autonomous Region of Vojvodina, where live only 1.173 ethnic Russians. Despite the tiny Russian minority in Serbia, pro-Russian public orientation results from intensive Russian informative warfare. Examples as organisation and usage of pro-Russian „Serbian platoon“ in occupied Ukrainian regions and Syria[3], organising military camps for Serbian youth[4], or open espionage affairs[5]suggest that Russia conducts active and aim orientated information and psychological operations in Serbia.

[2] Data from Statistic Biro of the Republic of Serbia indicates that 3.247 ethnic Russians live in Serbia, or 0.5 percent of the population (SORS 2011), which indicates ethnic Russians are a very small ethnic community.

[3] There are no reliable data, but estimates range from a few dozen to 300 extremists from Serbia on the side of pro-Russian forces in Ukraine. They act as organized structures within the pro-Russian forces or independently so that according to specific sources, we can talk about the existence of the „Serbian platoon“ that fought in the east—Ukraine and later in Syria on the side of Russia. Members of extreme right-wing and neo-Nazi organizations act from the position of „helping the Russian brothers“ and with the expressed goal of developing a pro-Russian and anti-Western relationship in Serbia itself. Serbian officials strongly dissociate themselves from such cases and strongly condemn them. The Criminal Law of Serbia prohibits its citizens' participation in such conflicts, and as a result of the proceedings against persons who were engaged in the conflicts in Ukraine, 28 court verdicts have been pronounced so far.

[4] In the summer of 2018, pro-Russia organisation Association of Participants in Armed Conflicts in the Former Area (UOSYU) supported by RF Embassy in Belgrade, conducted the „Youth-Patriotic Camp Zlatibor 2018“ were youth between 14 to 23 were trained in martial and military skills. Shortly after the opening, the camp was closed by the Serbian police, and President Vučić emphasized that the state will not tolerate such forms of training in which children in uniform are taught military skills. Previously, in April 2018, a group of 30 children from Serbia traveled to Russia to the International Camp of War Patriotic Youth, organized under the Russian government's patronage and led by the ultranationalist group ENOT Corp. Considering that motivation and recruitment are realized through social networks, where the Russian interpretation of Serbian patriotism of young generations is glorified, the long-term negative impact on Serbia’s national security is evident.

[5] The registered and recorded subversive actions of the Russian intelligence officers 2019 were recorded in the media, and the security service of Serbia confirmed their authenticity. However, despite that, this spy affair passed with "much noise and little detail", with noticeable comments that many foreign services are working on achieving their goals in Serbia, and not only Russia. Due to the apparent evidence, the Russian side did not deny the activity but tried to present it as a provocation of an unnamed third party.

Conclusively, in the case of Serbia, Russia tends to strengthen their position in South-East Europe, aimed at:

- Stopping or considerably slowing down Serbia's EU integration, encouraging the Euro-skepticism. An intensive negative campaign, supported by real slowed euro integrations and conditioning Serbia to resolve the „Kosovo“ question, contributed to the Serbian public opinion toward Euro-scepticism and strong pro-Russian sentiments (Novaković et al., 2021).

- Minimising Serbia's cooperation with NATO within the framework of the defence-security cooperation, primarily through non-selective and unreasonably critical appearances performed by citizen groups, civil initiatives, and pro-Russian parties. In addition, there is a constant emphasis on the negative experience of armed conflict from 1999, highlighting the role of the United States. (Novaković et al., 2021).

- Binding Serbia to Russia in every vital aspect of social life, economy, energy, security and defence, and international relations, and its transformation into a perpetrator of Russian interests. (Novaković et al., 2021).

Retrospective analyses of the implementation of Russian information warfare to Serbia:

– Creating conditions for the realisation of the Russian policy of compatriots;

– A reworking of history and imposing the self–fulfilling narrative of „traditionally good Russian–Serbian relations throughout history“;

– Using propaganda and abusing media freedom;

– Creating and supporting the functioning of structures and individuals who advocate for various aspects of strengthening Serbian Russian relations;

– Insisting on identity similarities and their policies;

– Intensifying relations between the Serbian Orthodox Church and the Russian Orthodox Church;

– Imposing the designed narrative of Russia as „the primary economic partner“.

In a comprehensive perspective, Russia successfully communicates their interests regarding Serbia by carefully cultivating social life and interest in international relations by a synchronised and strategically balanced approach.

6. CONCLUSION

The Russian Federation approaches strategic communication thoroughly, comprehensively, and in a planned manner, with long-term projections of its interests, through the development of a series of strategic documents, but also the development of organisational units. Modern media, especially the Internet, have been highlighted as potentially the greatest threat to the internal information security of the Russian state. The state is seen as a monolithic unity of the people and the leadership, and this idyllic situation is being eroded by „malignant and malicious Western technologies“ to disrupt the existing situation. It is indisputable that the media, especially the Internet, have a significant role in the organisation and initiation of the masses, but it is overemphasised as the causes of change. Namely, they are channels of communication and an outlet of dissatisfaction, which the state previously did not know or wanted to solve through internal social dialogue. Information warfare is an offensive approach to the realisation of Russian national interests. It is seen as an all-out confrontation in the socio-psychological information sphere, with zero tolerance for a different or critical opinion, recognised as an attack.

For Russia, Serbia is a part of the Western Balkans, polygon for indirect influence, primarily to undermine the political dominance of the influence of the EU, Germany, and the United States in this part of Europe. For this purpose, Russia uses Serbia's support in solving

Kosovo's issue favouring its strategic interests in the Western Balkan region, using Serbia as a base for achieving influence. Acting information and psychological operation through agitation, social network influence, the supported organisation acts, is evident and rising issues in Serbia – Russia relations. Russia projects its influence in Serbia primarily through diplomacy, energy, and strategic communications. They strongly influence Serbian public opinion, intending to develop animosity towards the United States and NATO and create an environment for slowing down EU integration. Russia successfully implements its strategic communication with the combined appearance of propaganda through the media, social networks, sponsored organisations, and influential individuals.

Conclusively, considering the growing importance of information and technical and technological development and geopolitical turbulence on the global scene, the struggle in the information sphere will gain momentum in the coming period. Following Russia's aspirations to establish multipolarity and control its spheres of interest, one can expect the development of information warfare and information security. In the areas of Russian interest, it is possible to expect intensive action of sponsored organisations and political parties, which will affirm misinformation, conspiracy theories, and other instruments of influencing public opinion with the support of the media and social networks. For the sake of a full effect, this kind of performance is synchronised with intensive public diplomacy activity, with a pronounced Russian „benevolent“ influence in the environment in which it operates. By turning public opinion towards Russian interests, it is possible to achieve the effect that the treated public accepts any critical action towards Russia as a negative effect on the public itself. The treated foreign population is mobilised to defend Russia's interests. The present knowledge that Russia

has been declared in a constant information war should create general relations with this geopolitical power.

REFERENCES

About Serbia in Russian, [О Сербии по-русски], 10.12.2021. http://ruserbia.com

Berezin S. (2003), *Differences Between Psychological and Information Warfare*, (electronic edition), „Psyfactor.org“, [Березин С. (2003), *Различия между психологической и информационной войной*, (электронный извор)] https://psyfactor.org/opsywar3.htm.

Bešlin M. (2016), *Serbian–Russian relations 19th to the 21st century: Myths, Misconceptions, and Stereotypes against the rational knowledge of the past and present*, in: *Eyes Wide Shut - Strengthening of Russian Soft Power in Serbia*, CEAS, Belgrade.

CEAS (2016), *Eyes wide shut - Strengthening of Russian soft power in Serbia: Goals, instruments, and effects*, 10.11.2021. https://www.ceas-serbia.org/en/ceas-publications/5168-eyes-wide-shut-strengthening-of-the-russian-soft-power-in-serbia-goals-instruments-and-effects

Chekinov S. G. & Bogdanov S. A. (2011), *The Influence of Indirect Actions on the Character of Modern War*, „Military Thought“, No. 6, 3-13. [Чекинов С. Г. и Богданов С. А. (2011), *Влияние непрямых действий на характер современной войны*, „Военная мысль“, No. 6, 3-13.]

Chekinov S.G. & Bogdanov S.A. (2015), *Forecasting the nature and content of future wars: problems and judgments*, „Military Thought“, No. 10, 41-49. [Чекинов С. Г. & Богданов С. А. (2015), *Прогнозирование характера и содержания войн будущего: проблемы и суждения*, „Военная мысль“, №10, 41-49.]

CIIS (2011) - *Convention on international information security*, "The Ministry of Foreign Affairs of the Russian Federation ", 22.09.2011, https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=en_GB

Danilevich AA, Loskutov DV, Rogozin OK, Rogozin AD, Rogozin DO (2011), *War and peace in terms and definitions: military-political dictionary*, Veche, Moscow [Данилевич А.А., Лоскутов Д.В., Рогозин О.К., Рогозин А.Д., Рогозин Д.О. (2011), *Война и мир в терминах и определениях: военно-политический словарь*, Вече, Москва.]

DISRF - *Doctrine of information security of the Russian Federation*, „Edict of the Russian Federation President“, № 646, (Moscow, December 5, 2016) [*Доктрина информационной*

безопасности Российской Федерации, „Указ Президента РФ“ № 646, (Москва, 5 декабря 2016 г.)] http://kremlin.ru/acts/bank/41460

Efimovich Yu.D. & Nikitin O.G. (2005), *The Place and Role of Special Information Operations in Resolving Military Conflicts*, „Military Thought“, No. 6, 30-34. [Ефимович Ю. Д. & Никитин О. Г. (2005), *Место и роль специальных информационных операций при разрешении военных конфликтов*, „Военная мысль“, No. 6, 30-34.]

Entina, E. and Pivovarenko, A. (2019), *Russia in the Balkans*, „RIAC report“, 13.1.2019. https://russiancouncil.ru/en/activity/longreads/russia-in-the-balkans/

FAPSI - *Federal Agency for Government Communications and Information under the President of the Russian Federation*, „Federal authorities“, [*Федеральное агентство правительственной связи и информации при Президенте РФ* (ФАПСИ)], „Федеральные органы власти“, http://панорама.рус/prav/fapsi.shtml.

FSPRFIS - *Fundamentals of the state policy of the Russian Federation in the field of international information security for the period up to 2020*, „Edict of the Russian Federation President“, No. 1753 (Moscow, July 24, 2013). [Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, „Указ Президента РФ“, Но 1753 (Москва, 24. Июль 2013. г.)]. https://legalacts.ru/doc/osnovy-gosudarstvennoi-politiki-rossiiskoi-federatsii-v-oblasti/.

FSSRF - Federal Security Service of the Russian Federation, „Federal authorities“, [*Федеральная служба охраны Российской Федерации*, „Федеральные органы власти“], http://fso.gov.ru.

Giles K. (2016), *Handbook of Russian Information Warfare*, NATO Defense College, Rome.

Jakovljević M. & Šćekić R. (2019), *Media and conflicts in the era of globalization*, „Vojno Delo“, 3/2019, 64-72. [Jakovljević M. & Šćekić R. (2019). *Mediji i konflikti u epohi globalizacije*. „Vojno Delo“, 3/2019, 64-72]. https://doi.org/10.5937/vojdelo1903064J.

Karayani A.G. (1997), *Information and psychological confrontation in modern warfare* (electronic edition), „Psyfactor.org“. [Караяни А.Г. (1997), *Информационно-психологическое противоборство в современной войне*, „Psyfactor.org“ (электронная публикация)] https://psyfactor.org/lib/psywar30.htm.

Kartapolov A. V. (2015), *Lessons from military conflicts, prospects for the development of means and methods of their conduct. Direct and indirect actions in contemporary international conflicts*, „Bulletin of the Academy of Military Sciences“, No. 2, 28-29. [Картаполов А. В. (2015), *Уроки военных конфликтов, перспективы развития средств и способов их ведения. Прямые и непрямые действия в современных международных конфликтах*, „Вестник Академии Военных наук“, No. 2, 28-29.]

Kuleshov Yu.E., Zhutdiev B.B. & Fedorov, D.A. (2014), *Information and psychological confrontation in modern conditions: theory and practice*, „Bulletin of the Academy of Military Sciences“, No. 1, 104-110. [Кулешов, Ю.Е., Жутдиев, Б.Б. & Федоров, Д.А. (2014), *Информационно-психологическое противоборство в современных условиях: теория и практика*, „Вестник Академии Воуеннукх Наук“, No. 1, 104-110.]

Kvachkov V. (2004), *Spetsnaz of Russia*, Military Literature, Moscow. [Квачков В. (2004), *Спецназ России*, Военная литература, Москва]

Manoilo A.V. (2003), *State information policy in special conditions*, MEPhI, Moscow. [Манойло А.В. (2003), *Государственная информационная политика в особых условиях*, МИФИ, Москва]

MDRF - *Military Doctrine of the Russian Federation*, „Rossiyskaya Gazeta - Federal Issue“ № 298, (December 30, 2014) [Военная доктрина Российской Федерации, Федеральный выпуск № 298, (Москва: Российская газета, 30 декабря 2014 г.], https://rg.ru/2014/12/30/doktrina-dok.html.

Medvedev D. (2011), *Dmitry Medvedev held a meeting of the National Anti-Terrorist Committee in Vladikavkaz*, "President of Russia", February 22, 2011, [*Дмитрии Медведев провел во Владикавказе заседание Националного антитеррористического комитета*, „Президент России“, 22.02.2011.г.], http://www.kremlin.ru/transcripts/10408.

Mitrovic M. (2021), *Assessments and foreign policy implementation of the national security of Republic of Serbia,* "Security and Defence Quarterly ", No. 34(2), 7-19. https://doi.org/10.35467/sdq/135592.

Mitrović M. & Nikolić N. (2022-in print), *Hybrid war - a contribution to defining the concept, content and model of operation*, Media Center "Odbrana", Belgrade. [Митровић, М., Николић, Н. (2022, у штампи), *Хибридни рат - допринос дефинисању концепта, садржаја и модела деловања*, Медија центар "Одбрана", Београд.

Mitrović M. (2018a), *Public diplomacy in the paradigm of the hybrid concept of conflict*, „Vojno delo“, 2/18, 309-325. [Митровић М. (2018а). *Јавна дипломатија у парадигми хибридног концепта сукоба,* „Војно дело“, 2/18, 309-325.] https://doi.org/10.5937/vojdelo1802309M.

Mitrović M. (2018b), *Genesis of propaganda as a strategic means of hybrid warfare concept*, "Vojno delo ", 1/18, 34-79. https://doi.org/10.5937/vojdelo1801034M.

Mitrović M. (2019a), *Strategic communication in the function of national security*, „Vojno delo“, 1/19, 43-45. [Митровић М. (2019а). *Стратешка комуникација у функцији националне безбедности*, „Војно дело“, 1/19, 43-45]. https://doi.org/10.5937/vojdelo1901041M.

Mitrović M. (2019b), *Determinants of Strategic Communication Significant for National Defense and Security*, „Matica Srpska Social Sciences Quarterly“, LXX, № 170, 2/19, 179–194. [Митровић М. (2019b), *Детерминанте стратешке комуникације од значаја за националну одбрану и безбедност*, „Зборник матице српске за друштвене науке“, LXX, Бр.170, 2/19, 179–194.] https://doi.org/10.2298/ZMSDN1970179M.

Mitrović M. (2020), *Media as an Instrument of Strategic Communication in Armed Conflicts – the CNN Effect*, „Vojno Delo“, 3/20, 34-52. [Митровић М (2020). *Медији као инструмент стратешке комуникације у оружаним сукобима - СИ-ЕН-ЕН ефекат*, „Војно дело“, 3/2020, 34-52.]. https://doi.org/10.5937/vojdelo2003034M.

ML - *Media Links*, „Embassy of the Russian Federation in the Republic of Serbia“ [*Медиа Линкови*, „Ambasada Ruske Federacije u Republici Srbiji“], 10.12.2021. http://www.ambasadarusije.rs/sr/strana/medie-linkovi

NCDMRF - *National Center for Defense Management of the Russian Federation*, "Ministry of Defense of the Russian Federation" (Ministry of Defense of Russia) [Национальный центр управления обороной РФ, „Министерство обороны Российской Федерации“ (Минобороны России)],10.11.2021,https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=11206@egOrganization.

Nikolić, N. (2019), *The place of the Western Balkans in the agenda of Russia and Turkey in the context of hybrid threats*, „Vojno delo“ 7/2019, pp. 289-305. [Nikolić, N. (2019), *Mesto Zapadnog Balkana u agendama Rusije i Turske u kontekstu hibridnih pretnji*, „Vojno delo“ 7/2019, str. 289-305.] http://10.5937/vojdelo1907289N

Novaković I., Albahari N., Bogosavlevic J. (2021), *GLOBSEC Vulnerability Index 2021*, „ISAC Found“. file:///C:/Users/Tarmi/Downloads/Vulnerability-Index_Serbia.pdf

Pashentsev E. N. (2020a), *Strategic Communication of Russia in Latin America*, in: *Russia's Public Diplomacy-Evolution and Practice*, (eds.) A. Velikaya, G. Simons, Palgrave Macmillan London, 219-232.

Pashentsev, E.N. (2020b), *Russian information presence at the Balkans: Challenges and Prospects*, in: *The Russia and Serbia in the contemporary world: bilateral relations, challenges, and opportunities,* (eds.) B. Stojanović & E.G. Ponomareva, Institute of international politics and economics, Belgrade.

RFNSS - *The Russian Federation's National Security Strategy* (2015), „Edict of the Russian Federation President“, № 683 (Moscow, December 31, 2015). https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf.

RIA Novosti (2011), *The revolution in Egypt was 'promoted' via Facebook-TV*, „RIA Novosti“, 12.02.2011. [*Революция в Египте была 'раскручена' через Facebook–ТВ*, „РИА Новости“, 12.02.2011], https://ria.ru/20110212/333637995.html.

RSE - *Encyclopedia of security*, „IB-BANK.RU“, 29.11.2021 [Энциклопедия безопасника, „IB-BANK.RU“, 29.11.2021] https://ib-bank.ru/glossary/

Russian home, [Руски дом], 12.12.2021. https://ruskidom.rs/sr/

SCIS - *Special Communication and Information Service*, „Federal Security Service of the Russian Federation“, [*Служба специальной связи и информации*, „Федеральная служба охраны Российской Федерации“], http://fso.gov.ru/struct/sssi/.

SDISRF - *On the Strategy for the Development of the Information Society in the Russian Federation for 2017 - 2030*, „Edict of the Russian Federation President“, № 203, (Moscow, May 9, 2017). [*О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы*, „Указ Президента РФ“, № 203, (Москва, 9 мая 2017 г.)], http://www.kremlin.ru/acts/bank/41919.

Selhorst A. (2016), *Russia's Perception Warfare*, "Militaire Spectator ", 185 No. 4, 148-164.

Sharavov I. (2000), *On the issue of information warfare and information weapons*, „Foreign military review“, No. 10., 2-5. [Шаравов И. (2000), *К вопросу об информационной войне и информационном оружии*, „Зарубежное военное обозрение“, № 10., 2-5.]

Slipchenko V. (2003), *Information resource and information confrontation*, „Army collection“, No. 10, 52-57. [Слипченко В. (2003), *Информационный ресурс и информационное противоборство*, „Армейский сборник“, No. 10, 52-57.]

Slipchenko V. (2013), *Information resource and information conflict*, „Army Collection“, October, No. 52. [Слипченко В. (2013), *Информационный ресурс и информационное противоборство,* „Армейский сборник“, Октябрь, No. 52.]

Smolyan G., Tsygichko V. and D. Chereshkin, (1995), *A weapon that can be more dangerous than a nuclear one. The realities of the information war*, "Independent Military Review ", No. 3 [Смолян, Г. Цыгичко, В. и Черешкин, (1995), *Оружие, которое может быть опаснее. ядерного. Реалии информационной войны*, „Независимое военное обозрение“, № 3.]

Soldatov A. & Borogan I. (2015), *The Red Web – the Kremlin's Wars on the Internet,* PublicAffairs, New York.

Sputnik, 12.12.2021. https://rs.sputniknews.com

Szpyra R. (2020), *Russian information offensive in the international relations*, "Security and Defence Quarterly ", 3/2020, Vol. 30, 30-47.

The concept of foreign policy of the Russian Federation, (2016), „President of the Russian Federation“, [*Концепция внешней политики Российской Федерации*, (2016), „Президент Российской Федерации“]. http://kremlin.ru/acts/bank/41451

Zheltov V.V. & Zheltov V.M. (2014), *The Internet, Protest Movements and the Arab Spring - A Territory of New Opportunities*, „Bulletin of Vladivostok State University of Economics and Service“, No 1, 189-203. [Желтов В. В., Желтов, В. М. (2014), *Интернет, протестные движения и арабская весна-Территория новых возможностей*, „Вестник Владивостокского государственного университета экономики и сервиса“, No 1, 189-203.]