SECURITY & DEFENCE QUARTERLY
https://securityandefence.pl/

Russian information offensive in the international relations

Ryszard Szpyra

r.szpyra@akademia.mil.pl

https://orcid.org/0000-0001-7687-4538

Faculty of National Security, War Studies University, gen. Chruściela "Montera" 103, 00-910 Warsaw, Poland

Abstract

The information war is beginning to play a dominant role in international relations. It is important because it occurs intensively in peacetime and determines the results of international clashes. This article aims to identify offensive elements in Russian theoretical and doctrinal views on the role and content of the information offensive in international relations. To meet this aim, a comparative analysis of research studies, documents and official statements was carried out. The study sets out to investigate how Russia assesses the usefulness of the information offensive for conducting international policy. The study revealed that the information war and information warfare in modern conditions in the Russian scientific debate occupy a prominent place. Regardless of the declared defensive nature of the Russian information offensive, both the scientific and doctrinal views emphasise the value of the information offensive for conducting international policy. Russia takes the information offensive in international relations very seriously and treats it as one of the main forms of international confrontation. This has serious consequences for countries close to Russia as it creates a new threat to their national security in peacetime.

Keywords:

information war, information warfare, Russian information offensive

Article info
Received: 16 March 2020
Revised: 15 May 2020
Accepted: 22 June 2020
Available online: 28 August 2020
DOI: http://doi.org/10.35467/sdq/124436

Introduction

One of the non-traditional areas of struggle is currently the quality of the information sphere. This consists mainly in the fact that in the past, information used mainly in power decision-making processes has now become a means of struggle, i.e. a weapon. As a result of rapid technological development, especially in the area of electronics, there has been a considerable dependence on information and, in a narrower sense, also on computer networks. As a result, an information struggle has arisen in both the sphere of practice and theory.

The Soviet Union was an active participant in the information offensive in international relations. The collapse of the Soviet Union and the emergence of Russia, on the one hand, and the development of information civilisation on the other, has created a new situation. The informational nature of the struggle in the in contemporary international relations is beginning to play a dominant role. It is important because it occurs intensively in peacetime and determines the results of international clashes. The media often expresses opinions about Russian information activity. However, the literature does not often match the analysis of official doctrinal documents and views of important representatives of the science for studying the discussed issues. This article aims to identify offensive elements in Russian theoretical and doctrinal views on the role and content of the information offensive in international relations. The study is based on a comparative analysis of research studies, documents and official statements. The study sets out to investigate how Russia assesses the usefulness of offensive information for conducting international policy. The central thesis of this paper is that regardless of the declared defensive nature of the Russian information offensive, both the scientific and doctrinal views emphasise the value of the information offensive for conducting international policy.

The Russian perception of the contemporary information environment

The modern Russian perception of military and political views was outlined by Russia's former prime minister Dmitriy Rogozin (2011) in a military dictionary that describes military-political terminology commonly used in the Russian power apparatus, as well as by international organisations that led by Russia. Rogozin argues that "the main and decisive form of struggle in a war is armed. It consists in organised application of the Armed Forces and other militarised formations, it is a collection of various scales of war operations being conducted in all spatial and physical spheres" (Rogozin, 2011).

Numerous Russian studies and doctrinal sources acknowledge civilisation changes and the evolution of the security environment. Manoylo (2003) draws attention to the emergence of the information society, which he defines as a society whose basic subject of work is information and knowledge, and the tool of work - information technologies. Manoylo draws attention to the possibility of the information society evolving in an offensive direction. He argues that the main result of the emergence of the information society is the creation of a global information space for social systems in which the fierce battle for achieving information superiority is ongoing. In this situation, the level of information development has a decisive impact on the basic spheres of society, i.e. the socio-political sphere, the economic sphere and the cultural and ideological sphere. The researcher also recognises that Russia has a natural predisposition to play a superpower role.

Similarly, Karaganov (2016, p. 8) argues that "under the influence of the information revolution, the psychology of the masses and a significant number of political leaders who are willing to respond more and more to the latest information stimuli change towards

simplifying the world vision". Karaganov maintains that the ideological and information sphere is extremely mobile and variable, and also plays an enormously important role in everyday politics. In this situation, it creates an important task for Russia: it must actively influence the ideological and informational sphere globally internally.

From the doctrinal sphere, one of the most important strategic documents is *the National Security Strategy of the Russian Federation* (*Strategiya natsional'noy bezopasnosti Rossiyskoy Federatsii*, 2015, p. 6) which emphasises that "the increasing impact on the nature of the international situation is exerted by increased confrontation in the global information space caused by the desire of some countries to use information and communication technologies to achieve their geopolitical goals, including through manipulation of public awareness and falsification of history". It is worth paying attention to the manner in which the adverse phenomena are attributed to their causes in the actions of other countries, mainly the West.

According to *the Information Security Doctrine of the Russian Federation* (2016, p. 1) information sphere is defined as "all information, computerised items, information systems, websites in the information and telecommunications network, communication networks, information technology, entities whose activities are associated with the production and processing of information, development and use of these technologies, security of information security, as well as all regulatory mechanisms of relevant social relations". We see here a broad perception of this category. It covers both information and its social sphere as well as IT systems and related cyber security.

Very important statements on this topic have also been made by representatives of the authorities. Vladimir Putin (2012) in his article *Russia and the changing world* confirms this by citing a number of examples. He claims in it that "world public opinion is nowadays shaped by the extremely active participation of advanced information and communication technologies. It can be said that the Internet, social networking sites, mobile phones etc. have evolved – along with television – into an effective tool for both internal and international policy."

Notwithstanding doctrinal records, the military sphere is also changing. In March 2019, at the Military Academy of the General Staff of the Armed Forces of the Russian Federation, a military scientific conference was held devoted to the development of military strategy in modern conditions. The lecture on the main directions of development of the military strategy was given by the Chief of the General Staff of the Armed Forces of the Russian Federation, the first deputy minister of defence of the Russian Federation, army general Valery Gerasimov.

With regard to the informational aspects of contemporary geopolitical conditions, Gerasimov (2019) argues that the analysis of the nature of modern wars showed a significant increase in the importance of the informational sphere of confrontation. The new reality of future wars will include, in particular, the transfer of hostilities to this sphere. At the same time, information technology is in fact becoming one of the most promising weapons.

The Russian perception of threats to national security in the information sphere and concept of information security

As Gerasimov (2019) convinces us, the information sphere, which has no clearly defined state borders, provides the possibility of a remote, hidden impact not only on the critical information infrastructure, but also on the population of the country, directly affecting the national security of the state.

As formulated in *Fundamentals of the state policy of the Russian Federation in the field of international information security for the period until 2020* (2013), the main threat in the area of international information security is the use of information and communication technologies:

a) as an information weapon for political-military purposes contrary to international law, to carry out hostile acts and acts of aggression aimed at discrediting the sovereignty, the territorial integrity of states and pose a threat to international peace, security and strategic stability;

b) for terrorist purposes, including for the provision of a destructive impact on the critical elements of the information infrastructure, as well as for the promotion of terrorism and terrorist activities to attract new supporters;

c) to intervene in the internal affairs of sovereign states, disturbance of public order, incitement of ethnic, racial and religious hatred, propaganda of racist and xenophobic ideas or theories that generate hatred and discrimination and incitement to violence.

According to *Information Security Doctrine of the Russian Federation* (2016), the expansion of the application of information technology creates new information threats. Opportunities for cross-border circulation of information are increasingly used to achieve military-political, as well as terrorist, extremist, criminal and other unlawful geopolitical goals, contrary to international law, to the detriment of international security and strategic stability. At the same time, the practice of implementing information technologies without linking them with ensuring information security significantly increases the likelihood of information threats.

The use of special information services of individual states for providing information and psychological influence is also aimed at destabilising the political and social situation in various regions of the world and at the undermining of sovereignty and violation of the territorial integrity of other states and is expanding. Religious, ethnic, human rights and other organisations, as well as certain groups of citizens, are involved in this activity, while the capabilities of information technologies are widely used.

Likewise, various terrorist and extremist organisations widely use mechanisms of informational influence on individual, group and public consciousness in order to escalate interethnic and social tension, incite ethnic and religious hatred or enmity, extremist ideology propaganda, as well as attract new supporters to terrorist activities. For illegal purposes, such organisations are actively creating means of destructive impact on critical information infrastructure objects.

The Strategy for Russia (2016, p. 29) outlines dangers to Russian culture, which include "the blurring of traditional Russian moral and spiritual values, the weakening of the unity of the multi-ethnic nation of the Russian Federation through external cultural and informational expansion (including the dissemination of low-quality mass culture products), propaganda of permissiveness and violence, racial, national and religious intolerance, as well as weakening the role of the Russian language in the world, the quality of its teaching in Russia and abroad, attempts to falsify Russian and universal history, and unlawful attacks on cultural goods". Therefore, Russia's great fear is of strategic information influences on Russian society in order to remodel its cultural model.

The Military Doctrine of the Russian Federation (2011, pp. 4–5) formulates basic assumptions of war policy and military-economic assurance of state defence on the basis of an analysis of threats to the Russian Federation and the interests of its allies. In

Chapter II on the danger of war and threats to the Russian Federation, there is a strong reference to the information sphere. The authors of the doctrine write that "there has been a tendency to shift the danger of war and the threat of war to the information space and the internal sphere of the Russian Federation. At the same time, despite the decrease in the likelihood of a large-scale war against the Russian Federation in a number of directions, the danger of war for the Russian Federation is increasing". As we can see, information threats have come to the fore, or at least have become one of the main ones. Other triggers of war include:

- activities in the field of information impact on society, primarily young citizens of the country, aimed at breaking historical, spiritual and patriotic traditions in the field of defending the homeland;

- provoking national and social tensions, extremism, and inciting ethnic and religious hatred or hostility.

The strategy also states that an important strategic threat in the economic field is the vulnerability of its information infrastructure.

In one of the most important strategic documents, *the National Security Strategy of the Russian Federation* (2015), information security occupies an important place. It is one of the types of national security also mentioned in the constitution. Information security is defined as "a condition that ensures the security of information, information media, resources, channels, information systems against unauthorised or unintentional modification or destruction of information while providing timely access to it for subjects with relevant tolerance, and the denial of this right by unauthorised entities" (Rogozin, 2011). Here we see a broad comprehensive approach including all the information, together with the sphere of human and all forms of modern processing, transmission and storage of information taking place mainly in the global network. Information security can be achieved on several levels: legal, organisational, routine, software, technical, spiritual and psychological (in the latter case, information security is a component of the spiritual security of society).

The spiritual sphere plays an extremely important role in information security, since currently "under the guise of freedom of speech a policy of implementation is carried out in the minds of citizens' information and cultural standards, which in a certain way orients and motivates their activities, substituting traditional spiritual values and, ultimately, leads to degradation of national identity and the erosion of national sovereignty" (Rogozin, 2011).

This statement, as can be seen, emphasises the importance of being able to influence people in an informative way. Influencing such as highlighted in the Dictionary (Rogozin, 2011) can even lead to "erosion of national sovereignty." This concern finds expression in the existence of a category such as „spiritual security", which is understood as "a component of national security expressed in the quality of national identity, reflecting the tradition of living arrangements of society, its culture and history, as well as the level of moral and political unity of society."

The authors of the Dictionary are convinced that "the tragedy of nations and states, as a rule, begins with the destruction of their spirituality, with the introduction of public consciousness of alien ideas, values, and unacceptable ways to achieve them. Therefore, provision of spiritual security is a priority for the government, as it expresses the morale of the nation and its ability to solve historical problems" (Rogozin, 2011).

Forms and content of the Russian information offensive in international relations

The Russian Federation, aware of the importance of using "information weapons", is working on concepts for the intensive introduction of foreign information technologies into the sphere of activity of the individual, society and the state. In this context, according to Professor Manoylo, member of the Scientific Council of the Security Council of the Russian Federation, the use of aggressive forms of information warfare is inevitable in the face of dynamically growing globalisation and contemporary geopolitical competition (Manoylo, 2003).

According to Alexandr Karayani (1997), a known expert professor of Lomonosov Moscow State University, the broadest of the concepts discussed, is "informational and psychological confrontation", reflecting the different levels of conflict activity and pursued informational and psychological measures for political and psychological purposes.

He claims that this kind of broad interpretation of this phenomenon may include information and psychological activities carried out:

a) at various levels (interstate or strategic, operational and tactical),

b) both in peacetime and in war,

c) both in the informational and spiritual sphere,

d) among both its soldiers and enemy soldiers.

In the information and psychological system of confrontation conducted for war purposes, one can distinguish between phenomena that qualify as "information war" (*informatsionnaya voyna*) and "psychological war" (*psikhologicheskaya voyna*). He also assumes that the term information war can be understood as the parties' struggle to gain control over the opponent in timeliness, reliability, completeness of information acquisition, speed and quality of its processing and delivery to contractors. Such a war covers the following areas of activity: acquiring necessary information; processing the information received; protection of information channels against enemy penetration; timely and high-quality delivery of information to recipients; misinformation about the opponent; disorganisation or disruption of the systems of acquiring, processing and disseminating information of the opponent; destroying, distorting, acquiring information from the opponent; and developing information processing processes more effective than the opponent. He also accepts that psychological warfare can be considered as a struggle between states and their armed forces. This struggle is fought to achieve superiority in the spiritual sphere and to transform the gained advantage into a decisive factor in achieving victory over the enemy.

Karayani (1997) argues that within psychological warfare, the following areas should be distinguished: mobilisation and optimisation of the moral and psychological forces of the nation and the armed forces in order to carry out war tasks; protection of one's own population and armed forces against the spreading of information and the psychological influence of the opponent (psychological countermeasures, psychological cover, counter propaganda, psychological defence); psychological impact on the army and the opponent's population in order to confuse them, demoralise and disorganise (psychological struggle); influencing the views, attitudes, and behaviour of friendly and neutral recipients (countries, social groups, armed groups) in a direction conducive to achieving victory over the enemy.

As Karayani (1997) maintains, short-term or narrowly targeted information and psychological activities carried out both in peacetime and during war in many countries of the world are called psychological operations. He also points out that in Russian military science information and psychological interactions according to the criterion of action, currently exist:

a) preventing and defending troops against an opponent's psychological operations;

b) psychological struggle (impact on enemy troops and hostile population, friendly and neutral countries is an area that foreign experts classify as psychological operations).

And although this division is not completely correct in terms of terminology, it generally reflects the need to direct the effort of staff commanders and educational work bodies as part of the informational and psychological interaction with the opponent. Thus, according to him, informational and psychological confrontation is a battle between states and their armed forces in order to achieve dominance in obtaining, processing, retaining and providing users with the necessary military, political, technical and other information, as well as in the sphere of the moral and psychological abilities of the nation, its army and fleet to achieve political and military goals.

Karayani (1997) also refers to psychological operations, noting that in ancient times, attempts were made to exert psychological influence on an opponent in order to disinform him, intimidate, and demoralise. It is believed that the deliberate psychological interaction of a person with another person to change the behaviour of the other has been used since the first contacts between people were made. He also assumes that psychological actions also include the implementation of specific measures, both in peacetime and during war, aimed at weakening the potential or actual prestige and influence of the opponent on hostile, neutral or allied countries and strengthening their influence and prestige. According to him, psychological activities are divided into strategic, operational and tactical. Strategic psychological operations are conducted on a global scale to achieve long-term goals for creating a favourable psychological environment for conducting combat operations. Operational psychological operations are conducted in some regions to achieve medium-term goals and to support war campaigns or major war operations. Tactical psychological operations are carried out with short-term goals and are conducted to support military operations at the tactical level.

For the purposes of psychological operations, the achievements of psychological sciences are used to: identify appropriately sensitive features of the human and group psyche; developing effective methods to assess the psychological state of the enemy; planning effective forms of psychological struggle; developing criteria and methods for assessing the effectiveness of psychological effects on people. He emphasises that by creating the scientific foundation of psychological operations, military psychologists rely on the achievements of various psychological schools. The following assumptions are taken as a basis:

- the decisive role of the subconscious in determining human behaviour and the functioning of psychological defence mechanisms and ways to overcome them (psychoanalysis);

- in terms of reflective impact ("anchoring", "zombification") in some way correlating perceptions, experiences, actions; with impressive structural strength, emotional tone, space-time characteristics of information (behaviourism, neurolinguistic programming);

- on 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), etc.

He also recognises that psychology helps organisers of psychological operations to identify the weakest links in the moral and psychological state of the opponent and to build tactics of psychological pressure on him. This is achieved by using the laws of human perception, so-called "effects". Among them, most well-researched to date are: the primacy effect, the authority effect, the „prophet's voice" effect; the repetition effect; the effects of imposing liability etc.

Sergey Berezin (2003) also writes about information and psychological wars in a number of publications. In one of them, he claims that information and psychological wars are closely related to the concept of information space. By this name, he not examining all the media located in a certain territory, but mass information generated by that media and accepted by the population of a given territory. This is a kind of media reality. According to him, the structure of events in this reality consists of four elements:

1. Verbal, i.e. verbal signs that are used to describe the subject;

2. Visual, i.e. video, image, as well as photographic materials;

3. Acoustic - all possible street noises etc.;

4. Interpretative, i.e. assessment of the event and its interpretation.

He is also convinced that the goal of the information war is to achieve information dominance. This dominance is aimed at preventing the opponent from using the information space. He believes that psychological warfare is a combination of various forms, methods and means of influencing people to change their psychological features (views, opinions, orientation of values, moods, motives, attitudes, stereotypes of behaviour) in the desired direction, as well as group norms, mass feelings, and public awareness in general.

Rogozin (2011) defines information war as "intense confrontation in the information space in order to achieve information, psychological and ideological superiority, damage information systems, processes and resources, critical structures and communications (Information technology, network-centric and cyberwar), undermining the political and social systems, and also massive psychological processing of military personnel and the general public (information-psychological war)." Similarly, Konventsiya (2011) defines information war as a confrontation between two or more states in the information space with the aim of damaging information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, massive psychological processing of the population to destabilise society and the state, and also forcing the state to take action in the interests of the opposing party.

As mentioned above, Rogozin (2011) refers to "competition in the information space", the goal of which is „information superiority". Although the Americans (JP 3-13 Information Operations 2006, p. GL-9) gave up using the name "information war or warfare" in official documents, the purpose of such rivalry in their view remains the same: "information superiority." In addition, we can clearly see the symmetry of this perception from the content of this definition. It manifests itself in the fact that in such an undertaking, there are at least two entities simultaneously conducting both offensive and defensive combat. It is emphasised that the term „information war is used in two meaningful ways:

- in the broadest sense – to refer to the confrontation in the information environment and the media to achieve various policy objectives;

- in the narrower sense – as information warfare, military confrontation in the information sphere in order to achieve unilateral advantage in the collection, processing and use of information on the battlefield (in operation, the battle), reducing the effectiveness of the relevant actions of the opponent" (Rogozin, 2011).

Another confirmation of the thesis that the informational-ideological confrontation never ceases are the next record that characterises the information war. It states that an information war is being fought during peacetime, as illustrated by the following entry: "information war in peacetime takes place in the form of information confrontation in all spheres of public life: economics, politics, social relations, in the spiritual sphere, and especially in ideology." This record surprises with the complexity of this phenomenon covering "all spheres of social life."

The ideological sphere is an important ground for conducting information warfare. The information war waged in this sphere aims to: "blur the philosophical and methodological foundations of the cognitive activities of the people of the enemy state, sow chaos in their minds, and deprive them of confidence in their future, and introduce false economic and moral attitudes" (Rogozin, 2011). It is again confirmed that "the ultimate goal of information confrontation is the conquest and retention of information superiority - the advantages over the enemy in the collection, processing, dissemination of information, as well as counteracting the relevant activities of the enemy" (Rogozin, 2011).

An important element of the information war is disinformation which is "realised usually by all kinds of media for a long time. The introduction of agents of influence in the media of the opposing states allows the public consciousness of the people to be manipulated, to use special means of their 'zombification'" (Rogozin, 2011). So as one can see, an important component of the information war is influencing people and controlling their consciousness.

Subordinate to the information war, the term information operations is understood as "a comprehensive term that combines the concept of electronic warfare, computer network operations (electronic warfare), psychological operations, military deception in order to influence, disruption of normal activities, damage or seizure of decision support tools of the enemy commanding staff, as well as measures aimed at improving one's own security from the relevant activities of the enemy" (Rogozin, 2011). Therefore, information operations are organised forms of information war. Information operations are conducted both against automated computer-information systems and people. Their purpose is to effect information systems and influence the staff of the opponent's armed forces, the population of any region or any social group.

In turn, it is assumed that "the most important part of the complex of information operations are psychological operations" (Rogozin, 2011). These operations have a dual meaning, more narrowly as "information activities of the armed forces, leading to the demoralisation and disorganization of the opponent" and, in a broader sense, as the intentional activity of any government and non-governmental institution in peace and in times of danger and war, which aims to change attitudes of an opponent, ally or indifferent recipients, representatives of the armed forces and civilians, in a direction favourable to the initiator of these activities" (Rogozin, 2011). So we can see that while the first form has a limited scope, the second one is very extensive and can be conducted universally by any entities against a wide spectrum of objects of influence.

It is noteworthy that "psychological operations include agitation, propaganda and other planned activities carried out to influence awareness, emotions, motives, reasoning, self-confidence and ultimately the behaviour of the target group" (Rogozin, 2011). It is also emphasised that "the object of influence of psychological operations can be both

individuals (including decision-makers and „opinion-forming authorities") as well as foreign governments and organisations in their entirety" (Rogozin, 2011). In this context, one should also see a wide spectrum of forms and entities involved in such activity. It also acknowledges that in such activities, "mass psychological manipulation measures developed by science, known as mass (crowd) psychology, are used. It is based on the fact that individuals grouped into a crowd have a number of features not individually found in them, such as: increased emotionality and irrationality, a sense of unity and universality of declared views and opinions, and a reduced level of responsibility caused by anonymity" (Rogozin, 2011).

It is assumed that "in most cases, propaganda is the primary tool for managing mass psychology. It is distinguished by white (a source sufficiently known), grey (a source not sufficiently known or unknown) and black propaganda (a source replaced by another)". It is also noted that "as a rule, initiators of relevant activities do not use the term „propaganda" when describing their activity, as it involves fraud and manipulation, and in many foreign environments it is associated with Soviet Cold War propaganda" (Rogozin, 2011). Rogozin (2011) also assumes that information warfare also applies to information weapons which are tools, methods and techniques used for the purpose of waging information war.

The semantic analysis shows (Rogozin, 2011) that the definition of peace already contained the statement that "peace prior to the war contains overt and covert elements of preparation for future military confrontation. The world after the war is a continuation of the policy pursued during the war, given the significant changes that occur in the lives of at least one of the warring parties as a result of military action" and "peaceful coexistence does not exclude the ideological and informational confrontation, economic rivalry, military-technical competition". Confirmation of this can be seen in the description of war in the statement "simultaneously (with the armed forces), other war and non-war forms of war are used in a war, including the organisation of sabotage and terrorist activities on the enemy's territory" (Rogozin, 2011). Therefore, apart from classic military forms, non-military forms of combat are expected.

Analysing war, Rogozin (2011) notes that "armed struggle in modern warfare preceded a fierce advocacy "barrage" (information and psychological operations) for the political isolation of the enemy and to weaken its fighting spirit, legitimising their actions. In this case, the active information warfare, disorientation of public opinion in individual states and the international community as a whole does not stop during the war". This is another confirmation of the thesis that the informational and ideological confrontation never stops. As for war itself, it is even emphasised that „ideological, psychological and information influencing" is currently one of the main war activities that affects the results of a war.

It should also be noted in the content of the definitions that the two-sidedness of this phenomenon is described, expressed in its offensive and defensive nature. This will manifest itself in many of the doctrinal contents analysed. However, more obviously, this phenomenon is analysed from a defensive position by describing it as a threat and seeking forms and methods to oppose it.

International perception of the Russian information offensive

Russian views and activity in the use of influence in international relations are systematically followed. International researchers on this issue point out various aspects of such activity.

As Erik Nisbet and Olga Kamenchuk note, scientific and political debates about disinformation usually focus on the technological aspect of state-led influence operations. However, this approach "has led to insufficient attention being paid to the underlying human factors driving the success of state-sponsored disinformation campaigns. (…) Academic research on disinformation strongly suggests that belief in false or misleading information is driven more by individual emotional and cognitive responses — amplified by macro social, political and cultural trends — than specific information technologies" (Nisbet and Kamenchuk, 2019, p. 65). According to André Gerrits, disinformation in the context of international relations should be understood as "the deliberate spread of false or unbalanced information by foreign states (or relevant non-state actors) with the primary objective to confuse and mislead, to sow disagreement and discord among parts of the population in other countries" (Gerrits, 2018, p. 4).

The goal of a misinforming a country is to achieve strategic benefits from decisions made by misinformed governments. Therefore, both misinformation and information manipulation are instruments of international policy (Gerrits, 2018, p. 5). In this context, according to Sergiy Gerasymchuk, Russian influence should be understood as "explicit and implicit actions by the Russian state and related actors (including intellectuals, businessmen, journalists etc.) or organisations, aimed at creating changes in the political behaviour and/or agenda of certain political actors through political means and/ or financial instruments" (Gerasymchuk, 2017, p. 75).

Holger Mölder and Vladimir Sazonov note that Russia belongs to this group of countries that were pioneers of influence in international relations. This was particularly manifested in the use of information warfare in achieving the political goals of international politics. In this way, Russia not only promotes its policy goals but also shapes the entire international system (Mölder and Sazonov, 2018, p. 309). The roots of this activity date back not only to the Soviet times but also to the tsarist era. Also in Russia's current views on information warfare, not only Soviet but also tsarist experiences can be seen (Kuzio, 2019). Therefore, Russia has long maintained great capabilities in the scope of information warfare. In addition, it is based on an extensive information theory of confrontation resulting from extensive scientific activity. This theory covers a wide spectrum of activities in the field of information offensives in international relations. These activities range from cultural to the ideological, historical, scientific and philosophical spheres. It can be assumed that "the information space lends information resources, including "weapons" or other informational means, to affect both internal and external audiences through tailored messaging, misinformation, and propaganda campaigns" (Iasiello 2017, p. 51).

Like Mölder and Sazonov, Stephen Blank also emphasises that Russia, because of its long historical experience and the acquired part of the Soviet strategic culture, perceives information warfare as a new means of resolving a large-scale political struggle. It remodels the thinking of the entire international environment (Blank, 2013). As well as this, the dominant mood is that Russia, for the present, is at war with the West in the informative environment (Berzina, 2018).

According to McGeehan (2018, p. 50), the essence of war is to achieve strategic political goals through various forms of violence. A country that achieves these goals without resorting to physical violence avoids great costs and bloodshed. In addition, it neutralises the enemy's military potential because it becomes useless. "Russia is attempting to offset Western technological superiority by going straight to the population and shaping their opinions in favour of Russian objectives". As Klein (2018, p. 137) notes that "giving to the Russian analysis the application of digital technology to democratic practices constitutes a strikingly effective new way of waging war."

Mölder and Sazonov (2018, p. 308) note that since 2013, Russia has been developing a non-linear approach to developing international policy strategies. According to this approach, the border between war and peace is blurring. As a result, a state of permanent war appears as a normal phenomenon in international politics. This condition was recognised and propagated by the English philosopher, Thomas Hobbes. "Information warfare forms an influential part of this non-linear strategy. The Russian information warfare machine is quite flexible and easily adaptable to new situations" (Mölder and Sazonov, 2018, p. 308).

The hybrid warfare category appeared in the debates about the modern security environment. In this context, Miroslav Mitrovic (2019, p. 11) points out that Russian military doctrine treats modern warfare as an integrated use of both military and non-military means. This doctrine places great emphasis on the use of information struggle to achieve the strategic political goals of the state. Moreover, these results should be achieved without direct use of military force and through operations affecting public opinion. As part of developing the ability to conduct this non-military warfare "the Russian government is actively developing its information warfare capabilities, including the weaponisation of mass media" (Lupion, 2018, p. 352). Russian information warfare expert, Timothy Thomas, notes that since the mid-1990s, two subcategories have appeared in the Russian information warfare model. One is information-technical and the other is the information-psychological. This is an integrated approach different from the Western approach (Thomas, 2014, p. 51).

It should be noted that the essence of the concept of information warfare strategy, operation, or tactic is to gain information superiority or even dominance. This advantage in the current environment is a prerequisite for achieving strategic political goals in international politics (Berzina, 2018; Farwell and Arakelian, 2016, p. 79). "Achieving dominance has defensive and offensive aspects" (Farwell and Arakelian, 2016, p. 80). This is well understood by the Russian authorities and that is why they are making many efforts to improve their ability to conduct information warfare. "Since 2008, Moscow has significantly improved its ability to weaponise digital news media. In the 2014 case, outlets seemed to take better advantage of the virtually unlimited publication space afforded by online publication, publishing articles from a variety of thematic perspectives and relying less on repackaging official statements" (Lupion, 2018, p. 352).

According to the opinion of Russian Defence Minister, Sergey Shoigu, the Russian authorities perceive mass media as a weapon, which is why the Russian government takes control of traditional Russian media, television, radio and newspapers (Aro, 2016, p. 121). Furthermore "by utilising the internet as a direct conduit to individual Western citizens, Russia has created an extremely efficient asymmetric weapon" (McGeehan, 2018, p. 51). Currently, the Russian authorities are also taking control of social media. To this end, a new tool for this interaction was created, called the troll factory. Not only professionals are involved in such activity, but also crowds of power supporters are involved (Aro, 2016, p. 121). According to Frida Ghitis (2020, p. 1) "Russia was engaging in an incendiary and divisive disinformation campaign in Latin America waged over social media similar to Russia's political interference in the 2016 elections in the US".

Stephen Blank also sees a different internal dimension of the usefulness of weapons and information operations in Russian views. According to him, they are also to be used for any internal counterinsurgency actions (Blank, 2013). In turn André Gerrits (2018, p. 3) emphasises that although all major countries conduct information manipulation in international relations, Russia conducts this activity on an unprecedented scale. The special extent of this activity has manifested itself in the intervention in foreign elections taking place in recent years.

In conclusion, it is worth quoting the opinion of Roy Godson, Ph.D., Emeritus Professor of Government, Georgetown University delivered during hearing before The Select Committee on Intelligence of The United States Senate One Hundred Fifteenth Congress Thursday, on March 30, 2017. He thinks, "if one looks at the history of the last 100 years you're going to find that the Russians and their Soviet predecessors have believed that active measures is a major tool for their advancement. They actually believe, whatever we think about it, that this gives them the possibility of achieving influence well beyond their economic and social status and conditions in their country. I think when you look at what they say now, what they do now, and the way they act and practice and talk about their active measures, they take this subject very seriously" (Rid, 2017, p. 6). It should be clarified that "active measures is a term that came into use in the 1950s to describe certain overt and covert techniques for influencing events and behaviour in, and the action of, foreign countries" (Rid, 2017, p. 20). This old name has now been replaced by the information war, which includes activities implemented under former active measures.

Conclusion

The Russian approach to security problems is particularly relevant in the context of the escalating conflict in Ukraine and the general cooling of Western relations with the Russian Federation. The aim of this article was to identify offensive elements in Russian theoretical and doctrinal views on the role and content of informational confrontation in international relations. The research focused on the question as to how Russians assess the usefulness of the information offensive for conducting international policy?

Studies have proven that the views of theoreticians conducting extensive scientific research are important for understanding the approach of the elite to the studied issues. These elites shape the thinking of power representatives and thus influence doctrinal views. They are often ahead of the awareness of the representatives of the doctrinal sphere. Studies have revealed that the Russian Federation, aware of the importance of using „information weapons", is working on concepts of intensive introduction of foreign information technologies into the sphere of activity of the individual, society and the state.

All the theorists mentioned emphasise that the goal of information warfare is informational superiority. Since Russia has a natural predisposition to play a superpower role in the face of dynamically growing globalisation and contemporary geopolitical competition, the use of aggressive forms of information warfare is inevitable (Manoylo, 2003).

In the information offensive sphere, the broadest of the concepts discussed is "information and psychological confrontation", reflecting the different levels of conflict activity, and informational and psychological measures for political and psychological purposes. And in the information and psychological system of confrontation conducted for war purposes, one can distinguish between phenomena that qualify as "information war" and "psychological war" (Karayani, 1997).

Information and psychological confrontation is a battle between states and their armed forces in order to achieve dominance in obtaining, processing, retaining and providing users with the necessary military, political, technical and other information, as well as in the sphere of the moral and psychological abilities of the nation, its army and fleet to achieve political and military goals (Karayani, 1997). Another important category recognised by various authors (Karayani, 1997; Berezin, 2003), i.e. psychological warfare, is understood as a struggle between states and their armed forces. This struggle is fought to achieve superiority in the spiritual sphere and to transform the gained advantage into a decisive factor in achieving victory over the enemy.

Doctrinal findings are extremely important as they form the basis of organisational and training activities. The research revealed that the information warfare and information war in modern conditions in the Russian doctrinal sphere are at the centre of the state's activity that lead to securing its interests. The information war, being an intense competition in the information space, aims to achieve information superiority. At the same time, information is widely perceived here, almost as a synonym of culture. This war also concerns the destruction of information systems, processes and resources, and critical structures and means of communication, i.e. the material part of the information sphere.

According to Russian doctrinal views, the information war is not only part of the war when it breaks out but also a constantly present phenomenon during the crisis and, importantly, in peacetime. Its intensity and forms of conduct change according to the conditions existing at a given time. In addition, the information war is of major importance because, existing in the background of peaceful activity of states and societies, it can significantly degrade the various components of the state imperceptibly, leading to degradation of the state's potential and even loss of sovereignty. The „insidious" nature of this war should force states to be constantly vigilant and to constantly improve their ability to counteract it. On the other hand, such opportunities for obtaining strategic effects make this war a convenient instrument for securing the state's own interests. So, regardless of the nature of the state, it should be expected that this war is and will be a common phenomenon.

In their considerations, the Russians are obsessed with the information threat from the West. In their opinion, the threat lies in the fact that (Karaganov, 2016) strategic information influences Russian society in order to remodel its cultural model. At the same time, according to Gerasimov (2019), information technology is in fact becoming one of the most promising weapons. This is confirmed by Manoylo (2003), who recognises that the use of aggressive forms of information warfare is inevitable.

Therefore, both in theory and in the doctrinal sphere, Russia is quite extensively developing the theory of offensive information war. They decompose the "information war" category into subcategories. Among them, the most important are information operations, psychological operations and propaganda. Various sources describe the methods of information warfare, which is part of the classic war, in some detail. War in which an armed struggle is fought by the armed forces and other types of struggle are being fought simultaneously.

Meanwhile, both theorists and representatives of the Russian authorities are convinced that the modern information war should also be waged in peacetime in all spheres of social life (Rogozin, 2011). However, the periods between wars that we call peace are treated as a time of peaceful coexistence in which there is competition but not confrontation or hidden war. What is more, they are convinced that the informational-ideological confrontation never ceases.

Another offensive part of the Russian approach is treating all means of mass communication as a weapon. Therefore, the authorities, having the right to direct the war, take control over the activities of these measures. According to Russian logic, this is because they serve to wage war.

It is worth emphasising that according to these views, wartime activity conducted in peacetime is directed not so much at the personnel of the armed forces as at the entire civilian population. The goal of this is to control the consciousness of the entire society and, as a result, to its „zombification". This creates a threat to Western civilisation where freedom of expression and pluralism are its foundation. This attitude of the Russians

creates an extremely dangerous situation in international relations because it blurs the existing boundaries between peace and war. It also increases distrust and tension in international relations. For Western civilisation, this creates a big challenge because it forces it to look for asymmetrical answers. A symmetrical similar response is not possible due to the essence of this civilisation, the so-called "free world" in which government cannot subordinate the means of mass communication to itself. And the Russians are taking advantage of this situation to conduct their offensive information warfare not only from the outside but also from the inside of the countries under attack.

As a result of research, it appears that Russia takes the information offensive in international relations very seriously and treats it as one of the main forms of conducting international confrontation. This has serious consequences for other countriesas it creates a new threat to their national security in peacetime too. In this situation, these findings confirm the adopted hypothesis.

It should also be noted that the research is limited. It boils down to examining the views of several representatives for the studied issues and representatives of Russian science and the main doctrinal documents in the original language. Therefore, the opinions of external researchers of Russia were studied in a limited scope. In addition, research focused on a strategic level and does not go too far into descriptions of individual forms of information offensive activities.

Funding

This research received no external funding.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Aro, J. (2016) 'The cyberspace war: propaganda and trolling as warfare tools', *European View*, 15(1), pp. 121–132. doi: 10.1007/s12290-016-0395-5.

Berezin, S. (2003) *Razlichiya mezhdu psikhologicheskimi i informatsionnymi voynami*. Available at: http://psyfactor.org/opsywar3.htm (Accessed 12 August 2019).

Berzina, I. (2018) 'The Narrative of "Information Warfare against Russia" in Russian Academic Discourse', *Journal of Political Marketing*, 17(2), pp. 161–175. doi: 10.1080/15377857.2018.1447762.

Blank, S. (2013) 'Russian Information Warfare as Domestic Counterinsurgency', *American Foreign Policy Interests*, 35(1), pp. 31–44. doi: 10.1080/10803920.2013.757946.

Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii (2016) Available at: http://www.scrf.gov.ru/security/information/document5/ (Accessed 12 June 2019).

Farwell, J. P. and Arakelian, D. J. (2016) 'Using Information in Contemporary War', *Parameters: U.S. Army War College*, 46(3), pp. 71–86.

Gerasimov, V. (2019) `Vektory razvitiya voyennoy strategii`, *Krasnaya Zvezda* 04 March 2019, Available at: http://redstar.ru/vektory-razvitiya-voennoj-strategii/?attempt=1 (Accessed: 11 November 2019).

Gerasymchuk, S. (2017) 'Russian non-linear warfare in Ukraine and Moldova: lessons for Visegrad countries', *International Issues & Slovak Foreign Policy Affairs*, 26(3/4), pp. 68–92. Available at: http://www.sfpa.sk/wp-content/uploads/2018/01/Gerasymchuk_ThinkVisegrad.pdf (Accessed: 24 February 2020).

Gerrits, A. W. M. (2018) 'Disinformation in International Relations: How Important Is It?', *Security & Human Rights*, 29, pp. 3–23. doi: 10.1163/18750230-02901007.

Ghitis, F. (2020) 'Russia's Disinformation War Reaches Latin America, Challenging U.S. Influence', *World Politics Review* (19446284), pp. 1–5. Available at: https://www.worldpoliticsreview.com/articles/28489/for-putin-venezuela-and-latin-america-are-key-to-challenging-u-s-influence (Accessed: 24 February 2020).

Iasiello, E. J. (2017) 'Russia's Improved Information Operations: From Georgia to Crimea', *Parameters: U.S. Army War College*, 47(2), pp. 51–63.

JP 3-13 Information Operations (2006) Joint Chiefs of Staff, Washington.

Karaganov, S. (2016) *Strategiya Dlya Rossii Rossiyskaya Vneshnyaya Politika: Konets 2010-KH — Nachalo 2020-KH Godov*. Available at: http://svop.ru/wp-content/uploads/2016/05/тезисы_23мая_sm.pdf (Accessed 12 August 2019).

Karayani, A. (1997) *Informatsionno-psikhologicheskoye protivoborstvo v sovremennoy voyne*. Available at: http://psyfactor.org/lib/psywar30.htm (Accessed 12 August 2019)

Klein, H. (2018) 'Information Warfare and Information Operations: Russian and U.S. Perspectives', *Journal of International Affairs*, 71, pp. 135–142. Available at: https://jia.sipa.columbia.edu/information-warfare-and-information-operations-russian-and-us-perspectives (Accessed: 24 February 2020).

Konventsiya ob obespechenii mezhdunarodnoy informatsionnoy bezopasnosti (kontseptsiya) (2011) Available at: https://www.mid.ru/ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666(Accessed: 14 May 2020).

Kuzio, T. (2019) 'Old Wine in a New Bottle: Russia's Modernization of Traditional Soviet Information Warfare and Active Policies Against Ukraine and Ukrainians', *Journal of Slavic Military Studies*, 32(4), pp. 485–506. doi: 10.1080/13518046.2019.1684002.

Lupion, M. (2018) 'The Gray War of Our Time: Information Warfare and the Kremlin's Weaponization of Russian-Language Digital News', *Journal of Slavic Military Studies*, 31(3), pp. 329–353. doi: 10.1080/13518046.2018.1487208.

Manoylo, A. (2003) *Gosudarstvennaya informatsionnaya politika v osobykh usloviyakh: Monografiya*. MIFI. Available at: http://www.klex.ru/jlj (Accessed 12 August 2019).

McGeehan, T. P. (2018) 'Countering Russian Disinformation', *Parameters: U.S. Army War College*, 48(1), pp. 49–57. Available at: https://www.hsdl.org/?view&did=812849 (Accessed: 24 February 2020).

Mitrovic, M. (2019) 'Influence of Global Security Environment on Collective Security and Defence Science', *Security and Defence Quarterly*, 24(2), pp. 5–20. doi: 10.35467/sdq/106088.

Mölder, H. and Sazonov, V. (2018) 'Information Warfare as the Hobbesian Concept of Modern Times — The Principles, Techniques, and Tools of Russian Information Operations in the Donbass',*Journal of Slavic Military Studies*, 31(3), pp. 308–328. doi: 10.1080/13518046.2018.1487204.

Nisbet, E. C. and Kamenchuk, O. (2019) 'The Psychology of State-Sponsored Disinformation Campaigns and Implications for Public Diplomacy', *Hague Journal of Diplomacy*, 14(1/2), pp. 65–82. doi: 10.1163/1871191X-11411019.

Osnovy gosudarstvennoy politiki Rossiyskoy Federatsii v oblasti mezhdunarodnoy informatsionnoy bezopasnosti na period do 2020 goda (2013) Available at: http://www.scrf.gov.ru/documents/6/114.html (Accessed: 11 November 2019).

Putin, V. (2012) `Rossiya i menyayushchiysya mir`, Komsomol'skaya pravda 27 February 2012, Available at: https://www.kp.ru/daily/25842/2813756/ (Accessed: 11 November 2019).

Rid, T. (2017) *Disinformation: A Primer in Russian Active Measures and Influence Campaigns. Testimony to United States Senate Select Committee on Intelligence*. Available at: https://www.intelligence.senate.gov/sites/default/files/hearings/S%20Hrg%20115-40%20Pt%201.pdf (Accessed: 24 February 2020).

Rogozin, D. (2011) *Voyna i mir v terminakh i opredeleniyakh. Voyenno-politicheskiy slovar*, Veche.

Strategiya natsional'noy bezopasnosti Rossiyskoy Federatsii (2015) Available at: http://www.scrf.gov.ru/security/docs/document133/ (Accessed 12 August 2019).

Thomas, T. (2014) 'Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?', *Journal of Slavic Military Studies*, 27(1), pp. 101. doi: 10.1080/13518046.2014.874845.

Voyennaya doktrina Rossiyskoy Federatsii na period do 2020 (2011) Available at: https://doc.mil.ru/documents/quick_search/more.htm?id=10363898@egNPA&_print=true (Accessed 12 August 2019).