Information-psychological warfare in Russian security strategy

Pynnöniemi, Katri Pauliina

Routledge - Taylor & Francis Group
2019

Pynnöniemi , K P 2019 , Information-psychological warfare in Russian security strategy . in R Kanet (ed.) , Routledge Handbook of Russian Security Policy . Routledge - Taylor & Francis Group , London and New York , pp. 214-226 .

http://hdl.handle.net/10138/308903

18

INFORMATION-PSYCHOLOGICAL WARFARE IN RUSSIAN SECURITY STRATEGY

Katri Pynnöniemi

Introduction

The research on information-psychological warfare has been one of the major themes of Russian military science since at least the 1960s and the development of the reflexive control theory (Thomas, 2004). One can go even further in the history, to Chinese strategist Sun-Tzu, or to the publication of Lenin's essay *On Guerrilla Warfare* in 1906, where he anticipated practices and strategies to be used in the political struggle for power. The set of measures ranged from assassination of political enemies to the stimulation of mass consciousness for active, but controlled, actions supporting the Bolshevik Revolution in Russia (Pynnöniemi, 2016, 31–32). Much later, these tactics became known as 'organisational weapon'. This term refers to organisations or organisational practices that are torn from their 'normal' context and used in the ways that are 'unacceptable to the community as legitimate mode of action' (Selznick, 1960, 2). These practices include, but are not limited to, the creation of unconventional tools of intervention, the direct weakening of the propaganda targets and the neutralisation of the opposition. As concluded in a study first published in 1950s, these tools were used 'to control directly the *arena* of conflict' (Selznick, 1960, 7).

Western research in the 1980s renamed the concept 'organisational weapon' as 'active measures' that refer to 'certain overt and covert techniques for influencing events and behaviour in, and the actions of, foreign countries'. One of the pioneering works emphasised information and the psychological nature of these actions, such as attempts to deceive the target and distort the target's perceptions of reality (Shultz and Godson, 1984, 198; see also Clews, 1964, 23). With the collapse of the Soviet Union, the research on propaganda and disinformation was rebranded anew and partly, forgotten. However, in the context of military studies, comparative research on Russian and US views on information operations and other forms of information warfare continued (Thomas, 1998).

The use of 'political technologies' was an important part of the struggle for political and economic power in the 1990s, although research on these phenomena was not articulated in the framework of information warfare. The adoption of a law on information security in 1995 and the subsequent information security doctrine in 2000 signalled the importance given to this sphere in Russia. From the Russian perspective, a series of 'colour revolutions' in the former Soviet countries starting with the 2003 Rose Revolution in Georgia and the 2004 Orange Revolution in Ukraine, became a game-changer. These events demonstrated the possibilities vested in the information-psychological techniques and other non-conventional measures. Since then, the term 'colour revolution' has stuck in the Russian foreign policy parlance and research literature. After 2014, it is used in describing the events in Ukraine and is often used interchangeably with the term 'hybrid war'.

Information-psychological warfare comes in many disguises. Each of the terms briefly discussed above is a product of its time. Some of these terms have been forgotten, whereas others seem to travel through time and become revitalised in a new era. This chapter analyses assumptions underlying the contemporary Russian debate on information warfare. The focus is on research literature and other writings that contribute to the formation of the Russian conceptualization of information security policy, and especially on information-psychological warfare as the information-technological (cyber) sphere was already examined in the previous chapter. The purpose is to illuminate assumptions guiding the official policy that in turn help us to understand differences and similarities between Russian and the Western thinking on this topic. The downside of this choice is that critical voices that challenge the official policy line or conspiratorial interpretations of information warfare that dominate the public debate are not discussed in full (see Berzina, 2018). However, some works from this latter genre are included in the analysis (Panarin, 2010, 2017; Brychkov and Nikonorov, 2017). The argument put forward in this article is that attention to nuances, even in translation, can create new knowledge about the roots of Russian thinking on threats to information security and assumptions guiding Russia's security strategy in this sphere.

Conceptualisation of information-psychological warfare in Russia

A study[1] published by the Primakov Institute of World Economy and International Relations of the Russian Academy of Sciences (IMEMO) notes that

> the ambiguity of the term "information warfare" defined and developed in the doctrines of the USA, gave rise to a *discrepancy in its translation*, resulting in the emergence of a large number of other definitions existing nowadays in the Russian journalistic and scientific sources.
>
> *(Romashkina, 2016, 19, emphasis added)*

Instead of addressing these problems in translation, the authors review the US terminology on information warfare, as well as numerous definitions provided by different Russian authorities.

The definition of 'information war' used in the study is taken from *the Intergovernmental Agreement of the SCO Member States on Cooperation in the Information Space* (Agreement, 2009). Actually, this same definition[2] appears later in the Russian Defence Ministry document known as the *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space* (Conceptual Views, 2011). Accordingly, information war is

> *Confrontation between two or more states* in the information space for damaging the information systems, processes and resources, which are of critical importance, and other structures, to undermining the political, economic and social system, and massive brainwashing of the population for *destabilizing the society and the state*, and also *forcing the state to make decisions in the interests of the confronting party.*
>
> *(Conceptual views, 2011, emphasis added)*

This definition of information warfare addresses key assumptions in the Russian debate. First, information war is a strategic-level confrontation between two or more states. With this, it is understood as a geopolitical struggle for power (Derbin, 2017). Second, information war provides the means to destabilise society and state, and finally, is a coercive tool with which the target (country) can be forced to make decisions that favour the attacking party. Each of these assumptions will be addressed in more detail in the following three chapters.

Information warfare as a form of counter-struggle

The dictionary (encyclopedia) of information-psychological operations published in 2011 provides a good starting point for the analysis of concepts guiding Russian thinking on information warfare. It contains, as the title suggests, terminological explanations for the phenomenon and technologies relevant for waging information warfare. Thus, 'information warfare' is translated as *armed informational confrontation*, aka *information war (voina)*, whereby two (or more) antagonistic systems make use of 'open or hidden targeted informational influences with the purpose of gaining an advantage in material sphere' (Venprintsev et al., 2011, 68). This definition originates from the theory developed by Professor Sergey Rastorguyev who is considered one of the most prominent Russian theorists of information warfare (Berzina, 2018, 164). Later, the entry on 'information confrontation' (*informatsionnoe protivoborstvo*) defines it as rivalry (*sopernichestvo*) between social systems in the information sphere, aimed at gaining control of the strategic resources, as a result of which one participant in the competition acquires advantage required for further development, whereas others will lose that chance (Venprintsev et al., 2011, 318–319).

The two above-mentioned definitions do not distinguish between peace and war, but indicate that information confrontation is a continuous and comprehensive process affecting the whole of society. One of the authors of the dictionary, Andrei Manoilo,[3] later specified that 'information-psychological confrontation' may take any form of social and political competition (*konkurentsii*) and comprises a wide spectrum of conflict situations, from individual-level conflicts to open confrontation of social systems (Manoilo, 2015, 184). The underlying idea, put forward in the dictionary, is that information confrontation is about competition for (strategic) resources and ultimately for (state) power.

The literary translation of the term 'information confrontation' (*informatsionnoe protivoborstvo*) is 'counter-struggle', 'counteraction', or 'countermeasure'. As noted earlier by Ristolainen, 'the verb *protivoborstvovat* can be found in common dictionaries and is translated as "to oppose", or "to fight against"'. Thus, the correct translation would be 'information counter-struggle'. The translation of Russian term as 'information warfare' misses the underlying rhetorical game, aimed at portraying Russia as the one 'under attack' (Ristolainen, 2017, 10–11). The original Russian concept underlines the active role of other countries in the information sphere and, at the same time, masking the ways in which Russia wages information war. Accordingly, Russian academic and popular literature discuss extensively the Western experiences of conducting information warfare and only rarely refer to Russia's own operations (Gapich and Lushnikov, 2014; Gryzlov and Pertsev, 2015; Manoilo, 2015; Brychkov and Nikonorov 2017; Kokoshin, 2017).

Although the general context is different, the argumentation is familiar from the Soviet era when the textbook on psychological war declared that only imperialist countries were conducting psychological warfare, whereas 'the Soviet Union did not need the help of defamation, disinformation and lies', for it had historical truth on its side (Volkogonov, 1983, 8). This did not, however, prevent the Soviet Union from systematically manipulating and mobilising mass movements and other political forces for the sake of the creation and facilitation of tensions internationally and within the capitalist countries (Morozov et al., 1978; Aspaturian, 1980; see also Pynnöniemi and Rácz, 2016). The underlying logic of these 'active measures' (Shultz and Godson, 1984) derived from the relative weakness of the Soviet Union in face of the US military and industrial potential. Consequently, the use of 'non-military factors' was expected to play in favour of the Soviet Union in the overall equation of the 'correlation of forces' (Aspaturian, 1980, 10).

The above-mentioned study published by the Russian research institute IMEMO exemplifies how this logic applies in the current context. The authors of the study argue that *confrontation* in the information space takes place between two groups of states: the Shanghai Cooperation Organisation (SCO) member-states (Russia, Kazakhstan, China, Kyrgyz Republic, Tajikistan and Uzbekistan) and the 'the developed countries'. The latter states 'have established authorities and special committees that are responsible for providing information technology and information-psychological security, as well as for conducting information operations'. Having characterised what is required for a level playing field, authors conclude that 'information security is an integral and increasingly important part of the process of ensuring *strategic stability*' (Romashkina 2016, 21, emphasis added).

The rhetoric used in the above characterisation is typical for the Russian debate. The developed countries are deemed active both in defence of information space and in conducting offensive information operations. Russia, in turn, is represented as passive (especially with regard to the conflicts in Georgia and Ukraine). What is emphasised instead is Russia's role in building a legal basis for the protection of international information security. The study argues that Russia does this because it

> supports demilitarisation of the international information space, the necessity of completion and adaptation of the mechanism of international law in relation to IT, and also creation of new norms, emphasizing that the arms race in information space is capable of destabilising the developed agreements on disarmament and international security in other spheres.
>
> *(Romashkina 2016, 104)*

A more mundane explanation for this interest in rewriting international agreements and policies in the information sphere is that, in this way Russia seeks to 'alleviate dangers posed by its own underdevelopment and to increase the monitoring of information sphere inside Russia' (Pynnöniemi and Kari, 2016; see also Thomas, 2014, 128). Although these concerns are real, and Russia is keen on advancing its interests in the international legal sphere, much of the current debate focuses on the dangers the information warfare poses for the societal and state security.

The colour revolution as information warfare technology

On the eve of the Russian presidential elections in 2018, the Russian Federation Council established a special commission tasked to study 'foreign interference into Russia's internal affairs'. The committee was tasked to offer recommendations how to mitigate this threat. The annual report of the commission identified several types of interference including the foreign financing of Russian non-governmental organisations, the spread of foreign ideas through educational programs, the creation of a negative image of Russia in the foreign media, politisation of the sport events (read World Cup) and stimulation of ethnic and social antagonism within Russia (Doklad, 2018). The report merely registered the mainstream interpretation according to which threat towards Russian information security were increasing. As stated in the Russian military doctrine,

> It is noteworthy that military dangers and threats are also moving into the information space and within the Russian Federation. Against this background, although the likelihood of a major war on the Russian Federation has declined, the military threats to Russia are on the rise.
>
> *(Military Doctrine, 2014, Article 11)*

The underlying assumption is that information technologies are used for the purpose of destabilising society and the state. This basic starting point is expressed with the concept of 'colour revolution' that refers to the set of information-psychological technologies manipulated outside the target country and used for the purpose of initiating a state coup. The typical argument states that the Western countries use colour revolutions as instruments to create a (neo)liberal order at the global scale (Novikov et al., 2017). The most evident use of this rhetorical strategy is among the popular literature intended for wider audiences. In recent publications, the colour revolution concept is replaced with the reference to 'hybrid war' (Panarin, 2016, 2017). Both in the academic literature and in official documents, Western governments, in particular the US, are accused of 'weaponisation of information' and, consequently, for the creation of conditions that have led to the emergence of local armed conflicts and uprisings in different parts of the world (Gryzlov and Pertsev, 2015; National Security Strategy, 2015; see also Thomas, 2014).

Some researchers compare the 'colour revolution technologies' to 'irregular warfare' (Gapich and Lushnikov, 2014, 7), whereas others, such as Andrei Manoilo, suggest that local wars and armed conflicts manifest the objectives and logic rooted in the information-psychological war that ultimately is about 'political struggle for power and authority [...] conducted with the means of information weapons' (Manoilo, 2015, 185). In this context, Russia's own experiences in using information and other non-military measures are rarely mentioned. The war in Georgia in 2008 stands out as an exception to this general rule, for it has been identified both as a success story (Novikov, 2017, 30) and a failure (Gareev, 2008; Evseev and Idayatov, 2016). Little is also said about the use of these methods in the conflicts in Ukraine or Syria, apart from 'showing' their Western origin (National Security Strategy, 2015).

Russian activities in the information sphere are often framed with the concept of 'soft power'. As the original concept suggests (Nye, 2004), soft power (*myahkaya sila, vlast'*) is not coercive but designed to influence the target through attraction. The Russian government agency established for promoting the interests of Russian speakers abroad is used as an example of Russia's attempts in this sphere. Sometimes his concept is used interchangeably with the term colour revolution to underline that the phenomenon in question has negative repercussions for Russia. What is more common, however, is that debate on colour revolution does not address issue of 'soft power' and vice versa (Borisova, 2016, 7).

Reflexive control at the time of war and peace

The third aspect of information warfare, identified in the above definition, refers to a situation where the target is forced to make decisions in the interests of the confronting party (Conceptual Views, 2011). In accordance with this new form of warfare, an attack is successful when it leads to the 'self-disorganisation' and 'self-disorientation' of the adversary, and the subsequent capture of the enemy's resource base and its usage to the benefit of the attacker (Ovtchinskii and Sundiev, 2013, 1). The theory of reflexive control, intensively developed by Soviet military and civilian theorists since the early 1960s, explains and provides practical means for achieving the 'self-disorganisation' of the enemy. According to V. A. Lefebvre, one of the thinkers behind the theory, reflexive control is 'a process by which one enemy transmits the reasons or bases for making decisions to another' (cited in Thomas, 2004, 2). As explained by Tim Thomas, an expert on Russian information war:

> Reflexive control occurs when the controlling organ conveys (to the objective system) motives and reasons that cause it to reach the desired decision, the nature of which is maintained in strict secrecy. A "reflex" itself involves the specific process of imitating the enemy's reasoning or imitating the enemy's possible behavior and causes him to make a decision unfavorable to himself.
>
> *(Thomas, 2004, 5)*

The task, so to speak, is to find a weak link in the enemy's 'filter' and exploit it. The filter is 'made up of concepts, knowledge, ideas and experience', and it can be targeted by an information weapon defined as a 'specially selected piece of information capable of causing changes in the information processes of information systems in accordance with the intent of the entity using the weapon' (Thomas, 2004, 11; see also Pynnöniemi and Rácz, 2016).

This is what in Soviet terminology was meant by *disinformation*. As described by Ladislav Bittman in an essay published in 1985, disinformation is 'a carefully constructed, false message that is secretly introduced into the opponent's communication system to deceive either his decision-making elite or public opinion' (Bittman, 1987, 113). For this purpose, various channels were used, including rumours, forgeries, manipulative political actions, agents of influence, front organisations and other means (Shultz and Godson, 1984, 195). As explained by Bittman, Soviet disinformation operations were,

> Acts of opportunity reflecting the long-term interests of the Soviet Union. Their primary objective is to add another drop of venom to the opponents' internal system which the expectation that eventually, after a certain period of time, quantity will become quality and the patient will die.
>
> *(1987, 119)*

Given this theoretical background, it is perhaps not surprising that many Russian works interpret the demise of the Soviet Union and the subsequent end of the Cold War as a Western victory in the information struggle. According to the popular conspiratorial argumentation, the Soviet Union lost the 'first information war' because the country's leadership acted upon false premises, in other words, was under foreign influence (Panarin, 2010).

In the context of more theoretical debate, a distinction is drawn between 'standard information war' that takes place as a part of a military operation (e.g. use of camouflage) and 'strategic information war' that refers to information-psychological operations aimed to change the perception of the target in a way that is favourable to the attacker (Venprintsev et al., 2011, 72). Researchers identify three general features of what they call 'strategic information war'. First, it is asymmetrical, making it difficult to predict the direction and means of possible attack. Second, different layers of society are attacked separately, while the appearance of peace is maintained (Venprintsevm et al., 2011, 73). With the use of non-military methods, the appearance of peace can be maintained without jeopardising the main objectives (Derbin, 2017, 15–16). Third, the same person can be attacked by multiple attackers simultaneously with each targeting a different sphere of cognition. Consequently, the clear distinction between 'friend' and 'enemy' (e.g. marked by the use of military uniform) is lost, making it more difficult to recognise the direction and the form of attack. This leads to the loss of the sense of danger, which is, in turn, the most dangerous aspect of the information war (Venprintsev et al., 2011, 74).

The definition of the term 'information weapon' offers additional insight on Russian thinking on information war. The dictionary defines information weapon as 'special means, technologies and information that are used in influencing the information space of the target society and in achieving significant damage to political, military, economic and other strategically significant state interests' (Venprintsev et al., 2011, 234). The dictionary, like other Russian studies on the subject, distinguishes between information-psychological weapons and information-technical (cyber) weapons. These two general categories are further specified by distinguishing between programming weapons (computer, or cyber sphere); psychological weapons; chemical, biological and biochemical weapons; electromagnetic weapons; infra-sound weapons; and psychophysiological weapons (Venprintsev et al., 2011, 236).

Vladimir Novikov, a professor at the Russian military academy, provides one of the most extensive descriptions of information-psychological weapons (Novikov, 2017). Professor Novikov specifies different categories of information-psychological weapons, including 'mass-media weapons', 'virtual information-psychological weapons' (e.g. mobile games like Tamagotchi), 'energy-informational psychological weapons' (ultrasound technologies harming physical systems and human organisms), 'psychotropic information weapons', 'bioenergy information weapons' (control of another person through hypnosis), 'information-genetic weapons' and 'somatotropic-psychoinformation weapons' (use of chemical and biological entities to affect human body). Furthermore, he identifies in this category also translation as form of struggle for linguistic meaning, as well as neurolinguistics influence, virtual money, flashmob and finally, geolocation technology (Novikov, 2017, 150; see also Thomas, 2014, 123–124, on other Russian authors discussing nonlethal and cognitive attacks).

What makes information weapons different from other types of weapons is explained with reference to three functions: asymmetry, mimicry and adaptation. *Asymmetry* refers in this context to idea that one element of the system can out-manoeuvre the whole system, thus leading to unpredictability. *Mimicry* is a root concept of deception. It refers to situation where appearance (or form) is maintained, but the content has changed. Thus, recognition of the form and direction of attack, as noted in above, becomes a challenge. And finally, *adaptation*, that refers to the transformation of context to fit the objectives of attacker (Venprintsev et al., 2011, 236). Taken together, these weapons can be used in a controlled manner, provide means to achieve quick results relatively cheaply, and due to their universal character, can be applied in different political and situational contexts (Manoilo, 2015, 197–198).

The main goal of the information struggle is to ensure the protection of the national interests in the information-psychological sphere. This refers, in particular, to the protection of the information-psychological security of the state (Venprintsev et al., 2011, 318). The Russian national security documents define what this means concretely.

The strategic context of information-psychological confrontation

Already in 1996, the Federal Agency of Governmental Liaison and Information (FAPSI), announced that 'the effect produced by information weapons can be compared only with weapons of annihilation', and therefore, in 1997, 'the Duma and the CIS Inter-Parliamentary Assembly had appealed to the UN, OSCE, and Council of Europe with a proposal to pass international ban on information wars and demanded that the turnover of information weapons be limited'. According to Andrei Soldatov, an expert on Russian information security, the security authorities in Russia had succeeded to lobby the government for allocating funding to develop such weapons, that were, subsequently, identified among the 'three priority factors deterring possible aggressions together with the Strategic Nuclear Force and the systems of high-precision weapons' (Soldatov, 2000, 1). Today, Russia considered among the most advanced countries when it comes to the development of state-of-the-art cyber capabilities (see previous article by Carolina Vendill Pallin).

More recently, the Russian National Security Strategy (2015) identifies information warfare among the risks (and dangers) to Russian national security. It states that the 'polycentric world' is shaped by the open-ended struggle for 'resources, access to markets, and control over transportation arteries'. Furthermore, 'competition between states is increasingly encompassing social development values and models and human, scientific, and technological potentials'. The Strategy reflects an idea that traditional military power, although important in intimidating Russia's weaker neighbours, is not sufficient for protecting Russia's strategic interests amid changing security landscape. The new situation requires 'asymmetric approach', where Russia's strengths (weaponisation of information, technology and organisations) are coupled with relative weakness in military-technological (force) development. The main objective of this approach is expressed in Article 36, where it is stated that

> Interrelated political, military, military-technical, diplomatic, economic, informational, and other measures are being developed and implemented in order to ensure strategic deterrence and the prevention of armed conflicts. These measures are intended to prevent the use of armed force against Russia, and to protect its sovereignty and territorial integrity.

This paragraph summarises Russia's strategy of active defence, where a set of non-military measures (informational, political, economic, organisational and cyber resources) are activated in order to neutralise a potential threat to Russia's national interests.

The information security doctrine identifies risks, dangers and threats to Russian national security in four distinct spheres: state defence; state and public security; economy, science, technology and education; and in the sphere of strategic stability and equal strategic partnership (Information Security Doctrine, 2016). The main forms of action in the protection of the information-psychological security of the state and society include:

> - neutralisation of information and psychological impact, including aimed at undermining the historical foundations and patriotic traditions associated with the protection of the Motherland;
> - the countering (*protivodeistvie*) of the use of information technologies for the propaganda of extremist ideology, the spread of xenophobia, the ideas of national exclusiveness, in order to undermine sovereignty, political and social stability, violent change of the constitutional order, violation of the territorial integrity of the Russian Federation;
> - neutralisation of information impact aimed at eroding traditional Russian spiritual and moral values (Information Security Doctrine, 2016, Articles 21d, 23a, k).

Here again a similar rhetoric strategy is adopted, as was discussed in the first section. Russian actions are framed as counteraction against the (aggressive) foreign information-psychological influence. Since this obviously is not the whole picture, the last section of this article will briefly discuss how Russia's opportunities and challenges in this sphere are defined in the context of Russian research literature.

Towards a Russian model of information-psychological warfare

The concept of 'geoinformational threat', developed by Russian researchers, refers to global geopolitical antagonism (*protivostoyaniya*), in the conditions of which 'financial-economic, political groups, and elites of different countries' aim to 'change the balance of political space within particular societies or in the world society at large'. The 'network technologies', first and foremost the Internet, are identified as 'the most important manipulative-propagandistic channel that has both disinformation and destructive potential' (Kochekova and Opaleva, 2018, 104–105, 122–23). Given the high level of development in the Western countries, they are in a better position to 'control and influence information space' and, therefore, form a major threat to Russian information security. Accordingly, the Internet is viewed as a resource that is controlled by the Western states and used 'for the resolution of political missions' against the interests of the Russian state (Kochekova and Opaleva, 2018, 106).

Another strand of argumentation interprets the geopolitical meaning of information space with reference to Russian exceptionalism and its civilisational mission. In their work on state information policy in the framework of information-psychological war, Andrei V. Manoilo, Anatolii I. Petrenko and Dmitri B. Frolov argue that

> real threats to Russia's national interests are not linked to the use of exotic information weapons against Russia, but stem from the danger of Russia losing her current status in the world politics. Authors call for mitigation of information-cultural expansion and consolidation of Russian national-intellectual potential in the global information space and alternative to the Western paradigm of globalisation.
>
> *(Manoilo et al., 2013, 85, 106)*

This Russian alternative is distinguished from four other models of information-psychological warfare, namely the Anglo-Saxon, Middle Eastern, East-Asian and Romano-German models (Manoilo, 2015, 218–270). Manoilo explicitly warns against imitation of the Anglo-Saxon model (a complete control of the information sphere supported by the military dominance) because this would lead to the instrumentalisation of the UN norms and thus would go against the Russian foreign policy principles. Furthermore, the use of 'colour revolution' technology (considered as the core of the Anglo-Saxon model) would make Russia an aggressor in the eyes of international society (Manoilo, 2015,[4] 301–304).

The specific Russian model should be based on Russian mentality and national traditions, as well as on the Russian schools of thought in political, psychological and sociological research spheres. Although Russia has not yet chosen a specific model, its basic features are already emerging. These include the following:

- formation of positive image of Russia as a country that is effectively solving international conflicts;
- conduct of psychological operations at the individual and mass consciousness level both in the conflict zone and beyond;
- the role of Russian special services in conducting psychological operations;

- protection of the domestic audience and state decision-making bodies from the foreign information-psychological influence (Manoilo, 2015, 307–310).

Taking into account later developments, most importantly Russia's actions during the war in Ukraine and Syria, this list provides quite comprehensive view on Russia's 'model' of information-psychological warfare. During the critical periods of conflict, especially in Ukraine, Russia has been able to systematically craft an image of itself as the one 'outside' the conflict, rather than the principal aggressor (Pynnöniemi, 2016). At the same time, the state-owned media companies have 'protected' the Russian domestic audience by creating and maintaining enemy images from Ukrainian 'fascists' to all-encompassing portrayal of the West as a threat to Russia (see, e.g., Giles, 2016; Pynnöniemi and Rácz, 2016). The active participation of Russian special services in specific psychological operations is more difficult to confirm. However, in the course of recent years, there is more and more public evidence about this. From the individual research reports (Aaltola, 2016; Conley, 2016; Kivimäki, 2017), systematic reporting (EUvsDisinfo, 2018) to official acknowledgement by the US authorities about the Russian meddling during the presidential elections in 2016 (ICA, 2017).

Conclusion

In the Western context, the term 'information warfare' usually describes 'limited, tactical information operations carried out during hostilities'. The Russian approach takes a holistic view of information warfare, seeing it as 'an ongoing activity regardless of the state of relations with the opponent' (Heickerö cited in Giles, 2016, 4). In the Russian context, information 'is both the subject and the medium of the conflict' (Giles, 2016, 4).

The deep-rooted image of Russia as a 'besieged fortress' is an important part of the argumentation on information security. The conceptualisation of information warfare as a counter-struggle implies that Russia is in a defensive posture. The comparative disadvantage that Russia has in specific high-technology sectors is sometimes highlighted to further support this claim. The underlying assumption is that information warfare is a struggle for geopolitical power between state actors. This idea is highlighted, especially in those works that see the information warfare in long-term perspective as a form of competition between different cultural-civilisational entities. Thus, the argumentation about information-psychological counter-struggle is construed as a discourse on the Otherness and incompatibility of Russian and Western social-political models. This is particularly the case with present-day academic and, most importantly, policy-oriented research that seeks to contribute to the formation of Russian information security policy. However, this conclusion remains incomplete since the studies that challenge the current policy line are not included in this analysis.

Notes

[1] One of the reviewers of this work is Colonel Anatolii Streltsov, who is an author of several authoritative books on information security strategy and has been attached to the Russian National Security Council since 1995 (Franke, 2015, 28).

[2] The Ministry of Defence documents provide more accurate translation of original Russian definition and are, therefore, used here.

[3] Andrei Manoilo is a professor of Moscow State University and defended his doctoral dissertation in 2008 on the role of information-psychological technologies in the conflict resolution and is a member of the Russian Security Counsel scientific board (Auvinen et al., 2018, 14).

[4] The first edition of the textbook was published in 2008.

References

Aaltola, Mika (2016) 'Cyber Attacks Go Beyond Espionage. Strategic Logic of State-Sponsored Operations in the Nordic-Baltic Region, *FIIA Briefing Paper* 200. Accessed on (May 28, 2018) at www.fiia.fi/en/publication/cyber-attacks-go-beyond-espionage.

Aspaturian, Vernon V. (1980) 'Soviet Global Power and the Correlation of Forces', *Problems of Communism*, Issue 9, May–June, pp. 1–18.

Auvinen, Toni, Martti J. Kari, Toni Puranen, and Anu Shibutani ja Juho Salminen (2018), *Venäjä informaatiovaikuttamisen kohteena*, Jyväskylän yliopisto, informaatioteknologian tiedekunta, KYBS7022, Informaatiovaikuttamisen erityiskysymyksiä, 7 May 2018.

Berzina, Ieva (2018) 'The Narrative of 'Information Warfare against Russia' in Russian Academic Discourse', *Journal of Political Marketing*, Vol. 17. No. 2, pp. 161–175.

Bittman, Ladislav (1987) 'The Language of Soviet Disinformation', in *Contemporary Soviet Propaganda and Disinformation: A Conference Report*, United States Department of State.

Borisova, E.G. ed. (2016) *Soft Power. Mezhdistsiplinnarnyi Analiz*. Moskva: Izdatelstvo Nauka.

Brychkov, A.S. and G.A. Nikonorov (2017) 'Colored Revolutions in Russia: Possibility and Reality', *Vestnik Akademii Voennyh Nauk*, No. 3 (60), pp. 4–9.

Clews, J. C. (1964) *Communist Propaganda Techniques*. London: Methuen.

Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (2011). Accessed on (May 5, 2018), Originally Published in Russian Language at: http://ens.mil.ru/science/publications/more.htm?id=10845074%40cmsArticle#1.

Conley Heather et al. (2016) *The Kremlin Playbook. Understanding Russian Influence in Central and Eastern Europe*. A Report of the CSIS Europe Program and the CSD Economics Program. Accessed on (May 28, 2018) at https://csis-prod.s3.amazonaws.com/s3fs-public/publication/1601017_Conley_KremlinPlaybook_Web.pdf.

Derbin, E.A. (2017) 'Methodological Aspects of Analyzing Modern Warfare', *Vestnik Akademii Voennyh Nauk*, Vol. 1, No.58, pp. 11–18.

Doctrine on Information Security of the Russian Federation (2016) Confirmed through Presidential Decree No. 646, 5 December 2016. Accessed on (August 11, 2017) at http://static.kremlin.ru/media/acts/files/0001201612060002.pdf.

Doklad (2018) 'Ezhegodnyi doklad vremennoi komissii Soveta Federatsii po zashcite gosudarstvennoi suvereniteta i predotvrashcheniyu vmeshatel'stva vo vnutrennie dela Rossiiskoi Federatsii', 5 March, 2018, Accessed on (April 2, 2018) at http://council.gov.ru/media/files/G6hNGZ3VbQNiMdZki1BKbrsrvuRxPwim.pdf.

EUvsDisinfo (2018) 'Everyone against Russia: Conspiracy Theories on the Rise in Russian Media', 22 May 2018, News and Analysis. Accessed on (May 28, 2018) at https://euvsdisinfo.eu/everyone-against-russia-conspiracy-theories-on-the-rise-in-russian-media/.

Evseev, V.V. and A.K. Idayatov (2016), 'Georgian – South-Ossetic Conflict in 2008: Lessons from the Information Warfare', in Romashkina, N.P. and A.V. Zagorskii, eds. *Information Security Threats During Crises and Conflicts of the XXI Century*, Moscow: IMEMO, Accessed on (January 15, 2018) at www.imemo.ru/files/File/en/publ/2016/2016_001.pdf.

Franke, Ulrik (2015) *War by Non-military Means*, *Understanding Russian Information Warfare*, The Swedish Defence Research Agency, March.

Gapich, A.E. and D.A. Lushnikov (2014) *Technology of Color Revolutions*. Moskva: RIOR, INFRA-M.

Gareev, Makhmut (2008) 'Strategicheskoe Sderzhivanie: problemy i resheniya', *Krasnaya Zvezda*, 8 October.

Giles, Keir (2016) 'The Next Phase of Russian Information Warfare', NATO Strategic Communications Center of Excellence, Accessed on (May 6, 2018) at www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

Gryzlov, B.M and A. B. Pertsev (2015) 'Information Confrontation. History and Modernity', *Vestnik Akademii Voennyh Nauk*, No. 2 (51), pp. 124–128.

ICA (2017), 'Assessing Russian Activities and Intentions in Recent US Elections', *Intelligence Community Assessment*, 7 January. Accessed on (May 28, 2018) at www.dni.gov/files/documents/ICA_2017_01.pdf.

The Intergovernmental Agreement of the SCO Member States on Cooperation in Providing International Information Security (2009). Accessed on (April 23, 2018) at http://docs.pravo.ru/document/view/20364925/19329178.

Kivimäki, Veli-Pekka (2017), 'The Cyber-Enabled Information Struggle. Russia's Approach and Western Vulnerabilities', *The FIIA Briefing Paper* 220. Accessed on (May 28, 2018) at www.fiia.fi/julkaisu/the-cyber-enabled-information-struggle.

Kochetkova, Aleksandra and Opaleva, Alekandra, eds. (2018) *Natshionalnaya bezopasnost' Rossii v usloviyah globalizattsii*. Geopoliticheskii podhod, Moskva: Unity.

Kokoshin, A.A. (2017) *Politologiya i Sotsiologiya Voennoi Strategii*. Moskva: URSS. Third edition. First published in 2005.

Manoilo, A.V. (2015) *Tekhnologii Nesilovogo Razresheniya Sovremennyh Konfliktov*. Moskva: Goryachaya liniya – Telekom, Second edition. First published in 2008.

Manoilo, A.V., A. I. Petrenko, and D. B. Frolov, eds. (2013) *Gosudarstvennaya Informatsionnaya Politika v Usloviyah Informationno-psihologicheskoi Voiny*. Moskva: Goryachaya liniya – Telekom, Second edition. First published in 2003.

Morozov, G.I., ed. (1978) *Obshchestvennost' i Problemy Voiny i Mira*. Moskva: Mezhdunarodnye Otnoshenie.

Novikov, V. K. (2017) *Informatsionnoe Oruzhie – oruzhie sovremennyh i budushchii voin*. Moskva: Goryachaya liniya – Telekom. Third edition. First published in 2011.

Novikov, V. K., S.V. Golubhinov, and V.V. Zakharov (2017) 'The Main Reasons and Conditions for Initiation and Waging of an Information War', *Vestnik Akademii Voenniyh Nauk*, Vol. 4. No. 61, pp. 28–32.

Nye, Joseph S. (2004), *Soft Power. The Means to Success in World Politics*. NY: Public Affairs.

Ovtchinskii, V.S. and I.Yu. Sundiev (2013), 'Organizatsionnoe Oruzhie: funktsionalnyi genesis i Sistema tehnologii XXI veka', *Izborskii klub*. Accessed on (October 23, 2013) at http://www.dynacon.ru/content/articles/1466/.

Panarin, Igor (2010) *Pervaya Mirovaya Informatsionnaya Voina*. Razval SSSR. Moskva: Piter.

Panarin, Igor (2016) *Informatsionnaya Voina i Kommunikatsii*. Moskva: Goryachaya liniya – Telekom. Second edition. First published in 2014.

Panarin, Igor (2017) *Gibridnaya Voina Protiv Rossii 1816–2016*. Moskva: Goryachaya liniya – Telekom. Second edition. First published in 2016.

Pynnöniemi, Katri (2016) 'The Metanarratives of Russian Strategic Deception', in Pynnöniemi, Katri and András Rácz, eds., *Fog of Falsehood. Russian Strategy of Deception and the Conflict in Ukraine*, The Finnish Institute of International Affairs, Report No. 45, Accessed on (May 6, 2018) at www.fiia.fi/fi/publication/588/fog_of_falsehood/.

Pynnöniemi, Katri and András Rácz, eds. (2016) *Fog of Falsehood. Russian Strategy of Deception and the Conflict in Ukraine*, The Finnish Institute of International Affairs, Report No. 45, Accessed on (May 6, 2018) at www.fiia.fi/fi/publication/588/fog_of_falsehood/.

Pynnöniemi, Katri and Martti J. Kari (2016) 'Russia's New Information Doctrine: Guarding the Besieged Fortress', *The FIIA Comment* No. 26, The Finnish Institute of International Affairs, Accessed on (April 12, 2018) at: www.fiia.fi/en/publication/russias-new-information-security-doctrine.

Ristolainen, Mari (2017) 'Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cybersecurity between Russia and the West', in Kukkola, Juha, Mari Ristolainen and Juha-Pekka Nikkarila, eds., *Game Changer: Structural Transformation of Cyberspace*, Puolustusvoimien tutkimuslaitos, Julkaisuja 10, Tampere: Juvenes Print.

Romashkina, N. P. (2016) 'Modern Information Security Threats: from Practice to Theory', in Romashkina, N.P. and A.V. Zagorskii, eds. *Information Security Threats During Crises and Conflicts of the XXI Century*, Moscow: IMEMO, Accessed on (January 15, 2018) at www.imemo.ru/files/File/en/publ/2016/2016_001.pdf.

Russian Military Doctrine (2014) Presidential Edict N2976N, Approved 25 December 2014, Accessed on (May 5, 2018) at www.scrf.gov.ru/security/military/document129/.

Russian National Security Strategy (2015) Approved by Decree of the President of the Russian Federation, 31 December, 2015, No. 683, Accessed on (May 5, 2018) at www.scrf.gov.ru/security/docs/document133/.

Selznick, Philip (1960) *The Organisational Weapon. A Study of Bolshevik Strategy and Tactics*. Chiago, IL: The Free Press of Glencoe. First Published 1952 by the RAND Corporation.

Shultz, R. and R. Godson (1984) *Dezinformatsia. Active Measures in Soviet Strategy*. New York: Bergamon Brassey's.

Soldatov, Andrei (2000) 'The Riders of the 'Psychotropic' Apocalypse', *Segodnya*, 11 February.

Thomas, Timothy L. (1998) 'Dialectical versus Empirical Thinking. Key Elements of the Russian Understanding of Information Operations', *The Journal of Slavic Military Studies*, Vol. 11, No. 1, pp. 40–62.

Thomas, Timothy L. (2004) 'Russia's Reflexive Control Theory and the Military', *Journal of Slavic Military Studies*, Vol. 17, pp. 237–256.

Thomas, Timothy L. (2014) 'Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?', *The Journal of Slavic Military Studies*, Vol. 27, No. 1, pp. 101–130.

Venprintsev V.B. et al. (2011) *Operatsii informatsionno-psihologicheskoi voiny. Kratkii entsiklopedicheskii slovar-spravochnik*. Moskva: Goryachnaya Linya - Telekom.

Volkogonov, D. A. (1983) *Psikhologicheskaya Voina. Podryvniye deistviya imperializma v oblasti obshchestvennogo soznaniya*. Moskva: Voennoe Izdatelstvo.