50

POINT OF VIEW


OSW

# THE DEVIL IS IN THE DETAILS

## INFORMATION WARFARE IN THE LIGHT OF RUSSIA'S MILITARY DOCTRINE

Jolanta Darczewska

POINT OF VIEW

NUMBER 50
WARSAW
MAY 2015

# THE DEVIL IS IN THE DETAILS

## INFORMATION WARFARE IN THE LIGHT OF RUSSIA'S MILITARY DOCTRINE

Jolanta Darczewska

OSW | CENTRE FOR EASTERN STUDIES
OŚRODEK STUDIÓW WSCHODNICH im. **Marka Karpia**

Editor
Anna Łabuszewska

Co-operation
Halina Kowalczyk, Katarzyna Kazimierska

Translation
Jim Todd

Graphic design
PARA-BUCH

DTP
GroupMedia

Photograph on cover
Eugene Sergeev / Shutterstock.com

PUBLISHER
**Ośrodek Studiów Wschodnich im. Marka Karpia**
Centre for Eastern Studies

ul. Koszykowa 6a, Warsaw, Poland
Phone + 48 /22/ 525 80 00
Fax: + 48 /22/ 525 80 40
osw.waw.pl

ISBN 978-83-62936-57-1

Contents

## INTRODUCTION

This paper is an attempt to consider the question of information warfare in the latest edition (December 2014) of Russia's military doctrine. I shall consider it in the light of similar assumptions in the editions of the doctrine from the years 2000 and 2010. It is based on the idea that information warfare is a pre-emptive response to both assumed and potential political threats to Russia. The starting point of this analysis is a description of the information campaign accompanying the publication of the doctrine. In Part 1, I discuss the doctrinal assumptions of information warfare, extracting those details that allow the identification of some general trends in the Russian Federation's security and defence policy. In Part 2, I interpret the concepts used in the doctrine by recalling the statements made by military theorists, the main themes of public discourse over the last few years about the dangers of informational threats, and the concept of strategic culture.

Information on the military dimension has been consistently presented in official documents since 2000. A more detailed analysis of these issues makes it possible to identify some general trends in Russia's security policy, which have become more pronounced in the years 2000-2014. These boil down to a blurring of the boundaries between internal and external threats, the introduction into armed conflict of non-military methods and organisational structures, and the conferral of an ideological character on this conflict. This erases the contours of conflicts between states, allowing Russia to participate in armed conflicts in which it is not officially a party.

In highlighting the informational threat and presenting it as a new type of danger, the authors of the doctrine are outlining the contours of information warfare. In their opinion, this is a kind of battle between parties which is conducted by conventional and unconventional, open and secret means, using both military and non-military organisational structures (special forces, irregular

armed forces, internal opposition in the enemy country). In the Russian military doctrine and thinking, information warfare has two dimensions: broader (as a separate kind of combat waged at all levels: political, economic, diplomatic, humanitarian, military) and narrower (as an element of support for military action).

## KEY POINTS

**1.** The military doctrine of the Russian Federation, and the informational and interpretive campaign accompanying it, are one element of Russia's overall information strategy. The functional aspect of the strategy reflects the concept of information warfare as outlined in the doctrine. It is identical to the concept of information warfare which is regularly pushed forward by journalists and civilian analysts. Its objectives, means and methods do not fit into the conventional notion of war. This concept is a sign of the militarisation of the Kremlin's policy; it allows society to be mobilised, and (through manipulation of domestic and foreign public opinion) for Russia's actions on the domestic and international stage to be legitimised. For this reason, the doctrine has significant practical value: it sets the stage for potential military interventions, and creates excuses for the Russian Armed Forces to be used.

**2.** The doctrinal assumptions about information warfare demonstrate not so much a change in the theory of its conduct (the changes mainly relate to the form of its description, and not the content), but rather a clinging to old methods (sabotage, diversionary tactics, disinformation, state terror, manipulation, aggressive propaganda, exploiting the potential for protest among the local population). In describing the methods of active intelligence and counterintelligence doctrine developed since the 1920s, a new type of war has been adapted from Anglo-Saxon theories: asymmetric, non-contact, indirect operations. By adapting Western terms to their own system of concepts and their own needs, the Russians have also given them their own specific content. This conceptual apparatus serves to emphasise that Russia's actions are no different from those taken by the West, including the 'masking' of their real aims.

**3.** The theory of information warfare is part of Russia's strategic culture. It is characterised by, among other features: the

'besieged fortress' syndrome; the desire to guarantee their own security without respect for the security of other countries; the authoritarian regime's fear of revolt; mythologising its own army and special forces; the desire to regulate all aspects of security, including the use of force beyond the letter of the law; imposing the principle of limited sovereignty upon its allies and neighbours; the militarisation of social and political life; and forcing an ideological image of the world upon other countries (now being presented as a confrontation between the 'American world' and the 'Russian world').

**4.** In the latest edition of its military doctrine, Russia implies that it has built up its potential of modern instruments for waging war; reached a state of combat readiness; and has announced its readiness to escalate tensions with the West. It has also promised to conduct information warfare in a more integrated way. After the Russian aggression against Georgia and Ukraine, this announcement can be seen as preparing public opinion for further violations of the international order based on geopolitical motives – especially since the concept of information warfare emerging from the doctrine has already been reflected in Russia's political and military practices for years, in times of both war and peace.

# I. THE MILITARISATION OF INFORMATION

## 1. Information warfare in practice

On 29 December 2014, the government newspaper *Rossiyskaya Gazeta* published a new edition of the Military Doctrine of the Russian Federation. This text also appeared on the webpage of the Security Council of the Russian Federation, which prepares this kind of document[1]. Representatives of the Ministry of Defence's leadership also offered their interpretations, explaining to the public the fundamental change in the international situation and the new methods the West is using to combat Russia, which have forced the Ministry to prepare an appropriate response. This is to consist of "new, non-traditional methods combining military and non-military measures in the four-dimensional combat area". These were discussed during the Ministry of Defence's council meeting of 30 January 2015, which was reported on all Russian television channels. As Valery Gerasimov, the Chief of the General Staff of the Armed Forces of the Russian Federation, announced, the new measures will be included in the new defence plan for the period 2016-2020.

According to the Interfax agency[2], the Ministry of Defence plans to expand its information campaign abroad. The doctrine is to be presented at the OSCE forum in Vienna, during the next review conference in Geneva on the observance of the Biological Weapons and Toxin Convention (BTWC), and also at the review conference of the nuclear non-proliferation treaty (NPT) in New York. Deputy Minister Anatoly Antonov has also announced a series of meetings with representatives of the military *attachés* accredited in Moscow. This is supposedly linked to anti-Russian reviews of the new doctrine, in which Russia is presented as a 'source of military threats'. The

[1] See http://www.scrf.gov.ru/documents/18/129.html. The term 'military doctrine' first appeared in the USSR in the 1920s. It can be succinctly defined as 'the system of views prevailing in a country on the state's military tasks and how to implement them.'

[2] 24 February 2015.

Russian campaign has a clear aim: Moscow will tell the world what it wants the world to hear about its 'defence' doctrine.

The comments accompanying the Russian doctrine emphasised the importance of informational operations in contemporary conflicts, and the inclusion of information into the country's defensive arsenal. The tone of the commentary was set by the communiqué from the meeting of the Security Council of the Russian Federation held on 20 December 2014, which approved the existing text of the doctrine. This work was supposedly undertaken "in view of the situation in and around Ukraine, as well as events in North Africa, Syria, Iraq and Afghanistan (...) by a decision of the RF Security Council of 5 July 2013 [sic], which recommended a consideration of the changing nature of threats to the RF"[3]. By emphasising the need for a reassessment of the global situation (the struggle of the world's leading countries for their interests are characterised by indirect actions, exploiting the potential for protest among local populations, radical and extremist organisations, as well as private military companies), the Security Council reiterated the anti-NATO and anti-American mantra which has constantly been present in successive editions of the Doctrine: "NATO's offensive potential is being developed directly on the borders of the Russian Federation. Measures are being actively taken to construct a global anti-missile defence system."

General Gerasimov reiterated to the Security Council; "The Atlantic Alliance is taking advantage of the events in Ukraine to move its own military infrastructure closer to Russia's borders. In Poland, in the Baltics, in the waters of the Black Sea and the Baltic Sea, NATO's land, air and sea groupings are being reinforced"[4]. In the quotes given, the world is a simple place: America and NATO are encircling Russia, which must defend itself. The West is arming and demonstrating its power; so Russia must seek a response

3 http://www.scrf.gov.ru/news/838.html

4 http://vz.ru/politics/2014/12/29/722699.print.html

to the American concept of the rapid global strike, and fight for the demilitarisation of space and the global information network, because it cannot permit the country and its surroundings to come under American "quasi-occupation"[5].

A different interpretation was put forward in a report on 26 December 2014 from the RIA Novosti agency, which is part of the state's propaganda company. By extracting a different quote from the doctrine ("A trend to move military challenges and threats to the information space and the domestic sphere of the Russian Federation is appearing"), it highlighted the domestic risks associated with information warfare which, according to the opinions perpetuated in the media, is an instrument of Western interference in Russia's internal affairs. This trend was demonstrated, for example, in a statement by Gen. Yuri Baluyevsky, the former Chief of the General Staff of the Armed Forces of the Russian Federation, and currently an advisor to the commander of the Interior Ministry of the Interior Troops. In it, he states: "the doctrine emphasises the need not only to defend the interests of the state, but also the state itself, with the emphasis on internal threats. This makes it possible to create a firewall against Western soft power, and also revises the relations between the various military elements in the organisation of the state"[6].

The campaign described above is a manifestation of the 'information war' Russia is conducting, which the military refer to as 'information warfare'. It is an enduring element of Russia's information strategy. By actively participating in this campaign, representatives of the military establishment are perpetuating the official message. The authorities' appeals are consistent with a long tradition in Russia. The words of the military men here have acquired the form of a particular kind of new-speak, although this does not change the

5 Владимир Путин, 'Россия не будет жить в полуоккупации' (http://www.rg.ru/2015/02/07/prezident-site.html).

6 http://www.vpk-news.ru/articles/22618

fundamental truth of the phenomenon. Their statements signify the militarisation of the Kremlin's domestic and foreign policy, and the calling into question of the principles of international law and the security order of Europe. They are addressed to both domestic and foreign audiences. They remind the domestic hearer that Russia is an object of aggression from the West, and the Kremlin and the security agencies, which are pillars of the state, guarantee its stability – despite the enemy's attempts to destabilise it. By mobilising and sensitising the public to the threat from the West, the Kremlin legitimises its military policy on both the domestic and foreign arenas. The message to the foreign audience is more nuanced. The doctrine supplies the so-called opinion-formers, and in practice the moderators of the informational campaigns, with both positive and negative arguments. It also allows them to make threats and issue warnings not to disregard Russian interests. As an anonymous Russian soldier on the information frontline, writing under the pseudonym 'Alex Wellington', has written: "The new doctrine is addressed to the governments and military elites of the states in Russia's sphere of influence; it offers them a guarantee of protection against the hostile influence of the so-called NATO partners. It is also addressed to the enemies of Russia, because it clearly sets a red line that should not be crossed".[7]

## 2. The 'new' comes back like a boomerang

In announcing the era of information warfare, most Russian commentators have emphasised the new quality which information warfare brings to the state's arsenal. This is an obvious exaggeration, because all the previous editions of the doctrine have already discussed the matter. Its importance was already addressed in the military doctrine from the year 2000, in which the basic external threats included (point 5) "informational activities (informational-technical and informational-psychological) which are hostile and detrimental to the military security of the Russian Federation

7 http://politrussia.com/vooruzhennye-sily/novyy-vzglyad-na-987/

and its allies". In this edition, the basic features of modern war included "active information rivalry, and the confusion of public opinion in the individual countries and in all global public opinion" (point 3). According to that document, the international situation at that time was characterised by "intensifying information warfare and the use of information and other technologies (including non-traditional technologies) for aggressive (expansionist) purposes". By including "humanitarian interventions" into this kind of technology, the doctrine implied the possibility of "achieving political goals by means of indirect actions".

The military dimension of this question was highlighted in particular by the separate Information Security Doctrine of the Russian Federation, which was adopted in September 2000 and is still in force today. Information security is treated in this document as the basis of national security, and 'information weapons' are described as a tool to achieve political goals. The document introduced most of the concepts used today in Russian literature on the subject ("information warfare", "information weapons"). The list of sources of external threats to Russia's information security includes the actions of foreign structures "(...) aimed at the RF's interests in the information sphere, the intensification of international rivalry to obtain technology and informational resources (...), and also the actions of foreign organisations, including foreign media, which are aimed at unfavourably presenting the image of Russia and the actions it takes." Also in this edition of the doctrine, the government warns of violations of the rights of Russian citizens and legal persons abroad, as well as the dissemination abroad of misinformation about Russian foreign policy. The main domestic threat, in turn, was described as "the illegal use of special measures to influence the individual, social, and group consciousness". This comprehensive document, which discusses in detail the informational threat and suggests ways to improve the methods of combatting it in various spheres (the economy, domestic and foreign policy, science and technology, spiritual life, the areas of defence and law enforcement), is a kind of storehouse of the concepts and

expressions used in Russian official documents and the extensive literature on the subject of information security. However, in this context it should be noted that while journalists and civilian experts commonly use the slogan of 'information war', the military experts prefer the term 'information warfare'.

The 2010 edition of the military doctrine lists "disruption of the functioning of organs of state power, important state and military facilities and the information infrastructure of the Russian Federation" among the main domestic threats to military security (point 9). Information warfare is given both a wider and a narrower definition: "actions of information warfare are being used to achieve political objectives without the use of force, and then to shape a favourable reaction from the international community to the use of military force" (point 13). In point 41, concerning supplying the Armed Forces with weaponry and military equipment, the need is signalled to "improve (...) the common information space of the armed forces and other troops as part of the information space of the Russian Federation (by the different actors in the information war conducting integrated activities), and to develop the forces and means of information warfare".

As a result, in the December 2014 edition of the doctrine, it is difficult to find any new contexts for the issues under discussion. The current version of the doctrine does not define any new, information-based frontline of the fight – this was already laid out in the 2000 version, like the other frontlines (political, diplomatic, economic, media, humanitarian, etc.). The new quality is the exposition of the role of information warfare, of the supposedly non-traditional methods of conducting it, and the non-military organisational structures that implement it. Another new element is the clearer link with Western theories of non-lethal, non-conventional or hybrid war (a combination of conventional and unconventional methods of combat). In this way, it is emphasised that Russia's actions are no different from how the West supposedly acts. This treatment, also used in the specialist literature, often leads foreign analysts

astray; they treat the Russian conceptual apparatus as a mirror image of their own. Meanwhile, **although they are adapting Western terms, the Russians are following their own assumptions and logic, adapting them to their own needs, traditions and culture. While transferring Western theories to Russian soil, they are mixing up the concepts of defence and attack, and adapting them for their own geostrategic retaliation**[8]. As a result, the phenomenon described in Western theories as asymmetric threats (social radicalisation or organised terrorism) has in the Russian theory become a method of asymmetric response to actions which are detrimental to Russia's geopolitical interests.

## 3. The doctrinal concept of information warfare

At first glance, the latest edition of the doctrine does not contain any surprising innovations: it preserves the structure and reproduces most of the assumptions of the previous editions. The changes lie in the details, and generally appear in the passages devoted to threats to Russia, the characteristics of contemporary conflicts, and the assessment of the current international situation. They are based on harsher versions of some of the language, and the removal or restoration of several subsections of the previous versions. A more in-depth analysis of these details allows us to identify several general trends in Russia's security policy which have become stronger in the period 2000-2014. These boil down to:

(1) blurring the boundaries between internal and external threats,
(2) stressing the importance of non-military means for putting pressure on potential adversaries, and
(3) giving armed struggles an ideological character.

By highlighting the informational threat and presenting it as a new type of danger, the doctrine's authors have outlined the

[8] See Владимир Горбулин, '«Гибридная война» – как ключевой инструмент российской геостратегии реванша' (http://gazeta.zn.ua/internal/gibridnaya-voyna-kak-klyuchevoy-instrument-rossiyskoy-geostrategii-revansha-_.html).

contours of information warfare. It is treated primarily as an ideological struggle waged by indirect methods (both open and concealed), using a variety of military and non-military organisational structures (special forces, irregular armed forces, internal opposition in the enemy country). In the doctrine, information warfare has two dimensions: broader (as a separate type of combat) and narrower (as an element of support for military activities). Both share the assumption that information warfare allows old politico-military tasks to be carried out in new ways.

The concept thus outlined is a synthesis of military and non-military methods of struggle, traditional methods (sabotage, diversionary tactics, psychological campaigns), and those which employ new cyber-technologies. It is based on an ideology and an imperial vision of Russia and the world which justifies the struggle. The main strategic goal of this struggle (the informational advantage) is defined in terms of geopolitical positions, in the confrontation with the United States and NATO. In practice, this concept leads to a blurring of the contours of inter-state conflict, creating an excuse or justification for Russia's participation in wars in which it is not officially a combatant.

## 4. Blurring the boundaries between internal and external threats

This trend has been expressed in the assertion of the idea that threats to Russia from NATO and the United States are growing, including the indirect informational and military influence of the US and the NATO states on the Russian sphere of influence. The current edition of the doctrine maintains the previous classification of these threats as follows:

(1) the main external threats to military security (point 12),
(2) the main internal threats to military security (point 13), and
(3) the main military threats (paragraph 14).

This approach has allowed the Russian military to expand its catalogue of potential challenges and goals. Whereas point 14 discusses direct threats, it has remained essentially unchanged (it is in line with the idea contained in the preamble ruling out the likelihood of war being unleashed against Russia on a large scale using conventional means of destruction and nuclear weapons), but the wording on potential external threats to the Russian Federation's military security (point 12) has definitely been made stronger; for example, the section which currently reads "the North Atlantic Treaty Organisation (NATO) is developing its potential strength; taking on global functions, which it is carrying out in violation of international law; the infrastructure of NATO member states is approaching the borders of the Russian Federation, with the aim of expanding the bloc" said only that "NATO is *striving* to develop (...)" in the previous version of the doctrine. The hierarchy of threats is also significant in this context: the threat of terrorism is listed at number 10, after the dangers which NATO and the US pose to Russia. Compared with the 2010 text, the section on potential external threats has been expanded with four more subsections:

- the existence (uprising) of outbreaks of inter-ethnic and interfaith tensions, international activities by radical armed groups, **foreign private military firms in areas adjacent to the state border of the Russian Federation and the borders of its allies**, as well as the **existence of territorial** conflicts, the rise of separatism and extremism in specific regions of the world;

- the use of information and communication technologies for political-military ends, to carry out actions contrary to international law, directed against the sovereignty, political independence and territorial integrity of states, and posing a threat to international peace, security, global and regional stability;

- **installing regimes whose policies threaten the interests of the Russian Federation, including as a result of the**

**overthrow of legitimate state authorities in countries bordering Russia;**

- subversive activities against the Russian Federation conducted by special services and organisations of states and their coalitions.

The only new element is a warning to countries bordering Russia on the inadmissibility of any policy threatening its interests. This section deserves attention for several reasons. First, the threat to the political regime has been raised to the rank of a military threat to the state. This kind of reflection is consistent with the traditional approach, in which political security[9] is considered as the security of the institution of the state. Secondly, this section establishes the principle of the limited sovereignty of the allies and immediate neighbours of Russia: they are required to comply strictly with the interests of Russia. Thirdly, Russia's sphere of influence has thus been expanded: in previous editions it was defined as the area of the CIS, but in the present edition it now constitutes the area of the former Soviet Union and part of the former Eastern bloc countries. Fourthly and finally, this is the wording used by Russian commentators referring to the situation in Ukraine, which has allegedly been forcibly colonised by the West.

Two other sections of the 2000 text have been changed; the first has had the phrase 'foreign private military companies' added, and the term 'territorial claims' has been replaced by the more imprecise term 'territorial conflicts (противоречия),' which opens up wider room for interpretation than the word 'claims' (this may also signal Russia's desire to stimulate new 'conflicts', for example in the Baltic states). The second item, referring to

[9] The concept of 'political security' (sometimes 'internal political security') has been developed in Russian scientific discourse since the mid-90s. It is defined as the protection of a political system against destructive and destabilising actions (for example, see Сергей Араев, 'Некоторые аспекты политической безопасности Российской Федерации', *Власть*, № 10, 2007).

subversive activities by the special services of foreign states using informational-psychological means, was included in the Information Security Doctrine, which in Part 2 refers to methods for ensuring informational security in the area of defence.

The section on internal threats also appears to have new content. In addition to the sub-section highlighting the devastating impact of psychological campaigns on young people, the remaining elements essentially repeat the threat contained in the 2000 text. These are risks that are more political than military in nature. They present a development of the external threats to the Russian Federation's internal political security, and also justify the assumption that challenges and threats are being posed to the information space and the domestic sphere of Russia. From official propaganda we also know that whereas in 2000 this primarily referred to so-called Chechen terrorists, this now refers to a 'fifth column' and 'foreign agents' financed from abroad, which is indeed emphasised elsewhere in the doctrine. This would confirm the hypothesis that the doctrine's new wording has not so much fixed a change in the perception of risks, but rather a change to the ideological motivation.

The list of internal threats now runs as follows:

- activities focused on overthrowing the constitutional system of the Russian Federation by force, the destabilisation of the domestic political and social situation in the country, the disruption of the functioning of the organs of state power, important state and military facilities and the informational infrastructure;

- activities by terrorist organisations and individuals aimed at violating the sovereignty and territorial integrity of the Russian Federation;

- **activities aimed at informational activity targeted at the general population, primarily young people, which is**

**intended to undermine historical, spiritual and patriotic traditions in defence of the Fatherland;**

- the provocation of inter-ethnic and social tensions, extremism, the incitement of hatred or ethnic or religious hostilities.

It should be added that the internal and external threats as defined in the doctrine serve to reinforce the image of the enemy which is omnipresent in Russian journalism and analytical texts. The enemy is identified in geopolitical terms (we/the Other). The enemy has a confrontational, mobilisation potential which is difficult to overestimate; this lends legitimacy to the Russian authorities, masking their failures and strengthening the ideological nature of the information war.

## 5. The growing importance of non-military methods of combat

The trend of the rising importance of non-military methods of struggle has its roots in the perception of threats. This has been emphasised by the removal of the chapter entitled 'The sovereignty of the Armed Forces in Russian military policy' (which disappeared in 2010), suggesting that all military formations have now been subordinated to the Armed Forces. This can be interpreted as a desire to legitimise the role of the civilian special services as key actors in the doctrine of the so-called non-military methods of struggle. This trend has also been highlighted by an analysis of the changes in the section entitled 'Characteristic features of contemporary armed conflicts.' Although the increasing role of information warfare and the ability to achieve political ends by means of indirect actions has been consistently emphasised since 2000, in the 2014 text the description of contemporary conflicts has taken on the clear outline of so-called asymmetric, hybrid war.

This has been contributed to by the assembly in one place of the following forms of wording:

- the complex use of the armed forces, as well as political, economic, informational and other non-military measures, implemented with the broad use of the potential of public protests and special operations forces;

- striking at the enemy throughout its entire territory, in the global information space, air and extra-terrestrial space, land and sea;

- the participation in armed clashes of irregular armed units and private military companies;

- the use of indirect and asymmetric methods of action;

- the use of political forces and social movements financed and managed from outside.

This trend also includes the new concept of 'the system of non-nuclear containment', defined in general terms as "a range of foreign policy measures, military and military-technical measures aimed to prevent aggression against the Russian Federation without the use of nuclear weapons". It should be added in passing that this move does not in any way diminish the role of the nuclear containment system, as was highlighted in points 16, 27 and 32 of the doctrine. Moreover, Gen. Gerasimov has stressed that it still has priority[10]. The concept of 'non-nuclear containment' highlights the role of the non-military component in contemporary conflicts, and also covertly links the special services to the military organisation of the state[11]. Beside the Armed Forces which form its

[10] http://arsenal-otechestva.ru/gerasimov-o-sostoyanii-vooruzhennyx-sil-rf.html

[11] The doctrines and laws (for example in the Russian national security concept to the year 2020) include the more broadly defined national security system, which includes "the Russian Federation's Armed Forces, other troops, militarised formations and bodies, which under federal legislation includes military service and/or law enforcement, as well as the federal government authorities involved in guaranteeing the national security of the state".

basis, together with the so-called other troops traditionally listed in previous editions, there are two new forces: militarised formations and bodies, and special formations created for the duration of a given war. In the first occurrence in the text (in point 8 explaining the basic concepts), these new forces are given the abbreviated term 'organs'. In the rest of the text, the phrase "the Armed Forces, other troops and organs" is used consistently. This approach confirms the *modus operandi* applied in practice, with a key role for the special services using the indirect methods and means outlined in the doctrine (diversionary tactics, sabotage, the organisation of irregular armed formations). In the Russian language, the word 'organs' as commonly used describes the authorities of law and order, which include the prosecutor's office, the police and the secret services.

The strictly military objectives and tasks related to information warfare are rather poorly defined. These are associated with the clearly emphasised need to take integrated action in the information space (the task of qualitatively improving the unified information space of the Armed Forces, other troops and organs, as part of the unified information space of the Russian Federation), the need to continue to improve the forces and means of information warfare; to improve and insulate the security systems of the Armed Forces, other troops and organs; and to create the conditions to reduce the risk of the use of information and communication technologies for political-military ends which do not accord with the law.

## 6. Presenting the ideological nature of the battle

In the previous editions of the doctrine, the ideological image of the world and international relations was reflected in the wording regarding global competition for a multipolar model of the world, a wording which defined Russia's sphere of influence; as well as in reports of discrimination against Russian citizens abroad, which contained a declaration that they would be defended. In 2000,

after the NATO operation in Kosovo, any criticism of the Alliance for ignoring the existing mechanisms of international security (the UN, the OSCE) was subdued and veiled. Also in the 2010 edition, "global development has been characterised by a weakening of ideological confrontation, a reduction in the economic, political and military influence of some states and alliances, and an increase in the influence of other countries aspiring to world domination, multi-polarity and the globalisation of various kinds of processes". In the 2014 version, in contrast, the ideological confrontation has taken on a clear shape, taking the form of competing value systems and models of development: "The current stage of global development is characterised by **an intensity of competition, tension in various areas of inter-state and inter-regional cooperation, competition between systems of values and models of development**, and instability of the processes of economic and political development at global and regional levels, which affects the overall complexity of international relations. A gradual diversification of influences on the new centres of economic growth and political attraction is taking place".

This confrontation / ideological rivalry is highlighted by different details scattered throughout the text of the doctrine; for example, the US is accused of destabilising the situation in the countries bordering Russia; of deploying its forces on the territory of countries bordering Russia; creating strategic missile defence systems; implementing the concept of the global strike; planning to place weapons in space, etc. This is also highlighted in the doctrine's image of the current geopolitical situation: the United States is not the only centre of attraction, Russia has become a centre of attraction for weaker partners, and is also a leader in the field of observing and reinforcing international law. The United States is the ideological opponent of all countries opposed to its hegemony in the world, whereas Russia offers a model of development and values different than those of America. The US is also, as may be presumed, an ideological opponent to... Europe, which is still being encouraged to "create mutually beneficial bilateral and

multilateral mechanisms to counter potential missile attacks, including if necessary the creation of common anti-missile systems with equal participation from Russia". This is an echo of the Russian Federation's strategic objective, which is to break up the American-European alliance. Meanwhile, Russia's place in the world is further emphasised by a declaration that it is maintaining an equal dialogue about European security with the European Union and NATO, as well as a declaration (...) of dialogue with countries concerned about new kinds of risks associated with the use of information and communication technologies for political-military purposes.

The information space has also been ideologised. Enemy action in this area is aimed not only at "undermining the Russian historical, spiritual and patriotic tradition", but also "against the sovereignty, political independence and territorial integrity of states, and also constitutes a threat to international peace, security, global and regional stability".

The question of revising the established order in the field of global security had already appeared in earlier texts and doctrines. However, until now it had never taken on such a confrontational tone. Russia portrays the United States as being almost its only problem, and has declared its willingness to escalate tensions, by extending its common field of security and defence to South Ossetia and Abkhazia[12] (which hitherto had included Russia and Belarus) and giving a military dimension not only to its Arctic

[12] President Vladimir Putin also announced the creation of a common security and defence space after the signing in March 2015 of a treaty of alliance with South Ossetia. (For example see http//rg.ru/2015/03/18/souz-site.html). A similar agreement was signed with Abkhazia in November 2014. The agreements signed by Moscow with the para-states – which are *de jure* part of the territory of Georgia but declared independence after the Russian-Georgian war in 2008 (which provided for the abolition of their borders with Russia, and for the establishment of common foreign and security policies with Russia) – were *de facto* a disguised way of incorporating them into the Russian Federation.

policy, but also to policies supporting regimes hostile to Russia in countries bordering the Russian Federation. This emphasis on the destructive role of the United States raises the prospect that Russia is fighting not so much for a multipolar world, but rather for the restoration of a bipolar world, guaranteeing it a comfortable security environment.

## II. AN ATTEMPT AT INTERPRETATION

### 1. An asymmetrical response to the West's hybrid war?

In the doctrine, we do not find any ideas regarding the 'cybernetisation' of armed conflicts, or any mention of electronic tools for 'cyberwar', i.e. the destruction of the enemy's information resources, which – as we might think – would be the responsibility of the Armed Forces, and should be reflected in the document we are analysing. We will not find in it any precise definitions of 'information space', 'information warfare', 'asymmetric operations', 'non-military means of warfare', 'non-nuclear containment' or the other terms referenced. At the same time, they appear to us as part of the general circulation of ideas in Russia, which are presented as a Russian response to the so-called Western hybrid war (against Ukraine, Russia and other countries), aiming to block the post-Soviet states' integration strategy with the EU and NATO.

Statements made by official representatives of the Ministry of Defence and military experts are helpful in explaining the content of these concepts. They show a high level of consistency with the doctrine's conceptual apparatus, as well as with the terminology used in Western military thought. The theoretical quarterly *Informatsyonnye Voyny* (Информационные войны) is a mine of information on the subject; it has been published since 2008 by the Russian Academy of Sciences in cooperation with the Academy of Military Sciences as part of the Academy for Informational Self-Defence project[13]. Their analysis leads to the conclusion that on the one hand, they enable the methods of 'disguise' (маскировка) perfected over decades by first the Soviet and then the Russian special services; and on the other, they sanction those methods by borrowing the fruits of Western ideas and putting them to their own purposes, which thus enables Russia to use modern methods and means of warfare.

[13] See http://www.iwars.su/

The growing importance of non-military means of warfare, indirect and asymmetric activities was emphasised *inter alia* by Valery Gerasimov, the Chief of the General Staff of the Armed Forces of the Russian Federation, at a conference at the Academy of Military Sciences in January 2013: "**The emphasis in the methods of combat being used is shifting towards political, economic, informational, humanitarian and other non-military measures, and implemented by exploiting the potential of protest among the local population.** All this is supported by indirect methods, including the execution of information warfare operations and the operations of special forces." Elsewhere, the general specified: "**The importance of asymmetric and indirect actions is rising. They may be based on political isolation, economic sanctions, the blockade of lines of communication via sea, air and land, violent intimidation, as well as the introduction of international peacekeeping forces under the pretext of defending human rights and humanitarian operations.** In the system of indirect actions, special and informational campaigns and operations will have a specific place"[14].

Gerasimov emphasised therein the role of the non-military component of warfare at every stage of the conflict – from the assessment of the situation, through the implementation of special operations with its involvement, up to the maintenance of order and the establishment of a loyal government. These indirect asymmetric measures also include the inspiration and mobilisation of the enemy's internal opposition, classified operations by special forces, and the accompanying informational activity. His statement also shows that these asymmetric and indirect non-military measures as defined are new elements in the doctrine, referred to as 'non-nuclear containment'. This hypothesis was confirmed by Gen. Leonid Ivashov, the head of the Military Academy of Geopolitical Problems, who **understands the concept of non-nuclear**

[14] See http://arsenal-otechestva.ru/gerasimov-o-sostoyanii-vooruzhennyx-sil-rf.html; http://www.vpk-news.ru/articles/14632

**containment to include bringing about political and economic losses with the support of conventional strike forces[15], that is, the combination of three factors: political, economic and military.**

These doctrinal concepts can also be found in the work of Igor Panarin, a professor at the Diplomatic Academy of the Foreign Ministry, a former analyst for the KGB and FAPSI, and a leading representative of Russian informational geopolitics. In his article 'The doctrine of Russia's information warfare'[16], **he defines information warfare as "a kind of warfare between parties in which special (political, economic, diplomatic, military, and other) methods and measures are used to influence the informational environment of the enemy, and to defend one's own environment in order to achieve one's defined goals"**. Like the authors of the 2000 edition of the doctrine, Panarin distinguishes two types of information warfare: informational-technical (where the targets are communication channels, telecommunications systems, radio-electronic transmissions) and informational-psychological (the impact on the minds of the opponents' political elite and the general public; opinion-forming and decision-making centres).

The model of information warfare outlined by Panarin includes three components:

(1) strategic political analysis,
(2) informational operations and
(3) informational counteraction (counteroffensive).

[15] http://www.pravda.ru/politics/military/defence/08-01-2015/1241179-doktrina-0/

[16] Игорь Панарин, 'Система информационного противодействия' (http://vpk-news.ru/articles/3677); see also http://www.km.ru/spetsproekty/2012/07/17/otnosheniya-rossii-i-stran-zapadnoi-evropy/0-doktrine-informatsionnogo-proti

In his model of the system (which he identifies with the system of informational containment) Panarin includes the Armed Forces and special services, which – as he states – should develop the capacity to defend the country against informational aggression by the enemy in peacetime. To do this, a special rapid reaction force supported by the space-based Glonass information monitoring system must be created. This model for defending the country's informational sovereignty, according to Panarin, requires Russia to strengthen its informational presence in all the strategically important regions of the world. This will enable an operational response to any crisis, and will at the same time encourage the establishment of a strategic balance of power in regions of vital interests to Russia.

By bringing together the strategies of indirect action, soft power and the technology of 'managed chaos' ('controlled destabilisation'), Vladimir Kariakin, a military expert for the Russian Institute for Strategic Studies[17], estimates that these are currently the most effective methods of international geopolitical struggle. **Indirect action and soft power can lead to the aggressor-state inflicting ideological sabotage and subversion on the victim-state.** These techniques lay the groundwork for an environment favourable to the aggressor, which offers the potential for protest, that is, a factor for destruction and change in the political regime hostile to the aggressor.

Kariakin also makes recommendations on how to develop strategies for informational counteraction. The dissemination of reliable (read: desirable for Russia) information requires the translation of the other's language of images and symbols into one's own language of interpretation, which accords with tradition – within one's own system of ideological and cultural terms and concepts.

[17] Владимир Карякин, 'Стратегии непрямых действий, «мягкой силы» и технологий «управляемого хаоса» как инструменты переформатирования политических пространств', *Информационные войны*, № 3 (31), 2014 (for the electronic version, see http//www.iwars.su).

Kariakin stresses the importance of knowing how to impose one's own rules of the game, and how to defend one's own arguments in the context of the global information space.

In the understanding of Gerasimov, Ivashov, Panarin and Kariakin, information warfare includes, on the one hand, the protection of one's own information space; and on the other, acting in the information sphere of one's potential adversary. Information space here has both a virtual (a space including symbols and ideological values, considered as a field of psychological influence) and a material nature (informational infrastructure, physical resources, databases, computer networks and telecommunications). By giving information warfare a confrontational dimension, these authors are also emphasising that it requires the involvement of both military and non-military tools. It is to be carried out by a number of entities (special forces, intelligence and counterintelligence offensives, irregular formations, the potential for protest, traditional and electronic media), and draws upon a broad spectrum of activities (political, economic, social, military, intelligence, counter-intelligence, diplomatic, propaganda et al.). The Russian state has been cramming every means it has in its arsenal into this concept: from investments to economic boycotts; from pipeline diplomacy to energy blackmail; from diplomatic pressure to corrupting the political elites of other countries; from soft power to provocations and threats of a military nature, state terrorism, and so on. When non-military preventative measures fail, the strategy provides for the use of conventional military means: the argument of force. This battle is taking place on many fronts: domestically (emphasising the stability of the Russian regime, projecting the role of a ruling elite which has a vision for the development of Russia, as well as mobilising their own public by means of tried and tested mechanisms for imposing images of the internal and external enemy, etc.) and externally (with the aim of management by fear, or by neutralising the damage to Russia's image caused by its real military aggression).

The military doctrine and the Russian theorists have sketched out a theory that can be applied in both peace and war. They underline that effective combat must be carried out on the basis of a plan, a system, consistently and over the long term. The strategic goal of this combat is to achieve informational superiority. The catalogue of tactical objectives is extensive: bullying and discriminating against the opponent, causing him physical and economic losses, destabilising the domestic situation in the country which is the target of information warfare, demonstrating one's own military, political and economic superiority, military blackmail, retaliation (revenge) on the enemy which rejected Russian offers, et al.

## 2. The endless public debate

The RIA Novosti news agency, the RT television station, and the other Russian media in their wake, have for some time been reporting on the new information security doctrine for Russia. As they explain it, the 2000 edition did not take into account today's realities, associated with the explosive development of IT, as well as the risks to which Russian society is now exposed: information warfare, cyber-espionage, cyber-crime. The doctrine's new edition is intended to clarify a number of terms such as 'information sphere', 'information policy' and 'national sovereignty in the global information space'. It concludes that there is only one effective way to ensure information security: a joint effort by all Internet users, journalists, local authorities, civil society organisations, etc. This is another manifestation of the consistent development of the 'besieged fortress' syndrome and a communal sense of responsibility for the state. Similar announcements have been made in the past. In 2012, for example, the website of the upper house of the Russian parliament posted a plan for a 'Concept of cyber-security strategy'[18], and also called for a broad public discussion on threats to information security. The project did not

[18] http://council.gov.ru/press-centre/discussion/38324

make it to the implementation phase, however, because the Federal Security Service opposed it. During hearings in the Federation Council on the subject, representatives of the FSB questioned the very term 'cyber-security' as used in the West, claiming that it narrowed down the definition of the wider phenomenon, and merely referred to the protection of equipment and communication channels.

The public debate in Russia about informational threats, which was initiated by the Security Council of the Russian Federation in the late 1990s, has continued to this day. Since the beginning this debate has been distinguished by the role of the so-called institutions of force, which have been presented as the main executors of the strategy for adaptation to the requirements of cyber-security. This also includes the so-called Chekist ideology, which treats the security sector as a pillar of power derived from the special forces of Vladimir Putin's team. Over time, the debate has coincided with the appearance in the ex-Soviet space of the so-called 'colour revolutions'[19], which led to a renaissance of traditional topics related to the psychological struggle between East and West. In Russian literature, the colour revolutions are regarded as "the most socially dangerous form of clashes between intelligence services"[20].

Despite the stated objectives (the conceptualisation of a new field of security, informational security; clarification of the basic concepts; preparation of the necessary legislation and new organisational solutions), the participants in the debate have focused on a diagnosis of the impact of IT on the overall political, economic and social development in Russia, making the public aware of the problems of informational threats, and analysing the Western

[19] The term describes the social movements in Georgia (2003), Ukraine (2004), in Kyrgyzstan (2005), as a result of which socio-political changes took place.

[20] See for example А.В. Манойло, Государственная информационная политика в особых условиях, Moscow, 2003, p. 293.

theoretical, legal and organisational ideas in the field of cybersecurity. Some of these ideas have been transposed onto Russian territory. Since 2003, just as in the West, the 'cyber' aspect of security has appeared in the context of the 'critical infrastructure of the state', a term borrowed from the area of crisis management. This includes top-secret 'critically important objects' (КВО) and 'key information infrastructure systems' (КСИИ, such as the information and communication systems of the organs of the state authorities, the special services, law enforcement and the Armed Forces, systems for warning about and combating the effects of emergencies, navigation systems, credit and financial systems, satellite communications systems, systems for managing the production and transport of oil and gas, transportation systems, water supplies, electricity, et al.).

Hence the conclusion that the Russians have adapted Western theories, technologies and solutions, adjusting them to their own concepts and their own "ideological and cultural system of concepts and terms" (to quote Kariakin). However, 'cyber-security' has apparently has not yet been included in this system. Nor is it to be found in the conceptual system of the military doctrine. Nevertheless, the latter does include active intelligence methods, such as have been developed in the Soviet Union since the 1920s; these have now been enriched with IT technologies (cyber-espionage, trolling), which are presented as an asymmetric, indirect component of information warfare. The doctrine also refers to 'non-lethal soft power', implemented by 'civil society' organisations run along military lines. Contrary to expectations, the doctrine does not even include any suggestions on the delimitation of the competences and responsibilities of the Armed Forces and civilian special services in the various fields of information warfare. This is – as the position of the FSB stated above confirms – exactly the intended outcome: strict definitions would pose constraints, both on the state apparatus which obtains and secures information, as on the state system of information warfare.

## 3. Cultural conditions for information warfare

Western theories of international relations attempt to explain this Russian doublethink (taking over someone else's ideas while at the same time rejecting them; appealing to international law, such as the right of peoples to self-determination, while at the same illegally crossing Ukraine's borders, etc.) in terms of a cultural paradigm, within the concept of strategic culture. Generally speaking, this defines the relationship between political culture and the strategy of using force for political purposes. This concept appeared at the end of the Cold War, mainly as a result of research into the USSR's policy on the international stage, which in terms of political realism was inexplicable.

The specific characteristics of Soviet/Russian strategic culture (as it was defined) were defined by the pioneers in this line of research, Jack Snyder and Colin S. Gray. They brought it down to a few items, such as: the constant desire to ensure national security without regard to the safety of other nations; the assumption that war and peace are different phases of the same process of the struggle for power; mythologising one's own army and special services; an unwillingness to make concessions even in response to the concessions of other countries. Similar conclusions were drawn by Thomas Graham, who moreover noted the authoritarian regime's age-old fear of revolt; the alienation and passivity of its citizens, whom the regime keeps in a state of constant mobilisation; and the experience of imperial Russia (the memory of the times of territorial conquest, and the empire's collapses in 1917 and 1991)[21]. These are expansionist experiences:

[21] J. Snyder, *The Soviet Strategic Culture: Implications for Limited Nuclear Operations*, Rand Corporation, Santa Monica, 1977; C. Gray, 'National Styles in Strategy. The American Example', *International Security*, Vol. 6, No. 2 (Autumn, 1981). See also Rafał Wiśniewski, 'Kultura strategiczna, czyli o kulturowych uwarunkowaniach polityki zagranicznej i bezpieczeństwa' [Strategic culture, or Cultural determinants of foreign and security policy]. *Strategic Overview*, 2012, No. 1, pp. 163-175.

the building of a security buffer is always transformed into their absorption into Russia.

Most theorists emphasise the continuity of Russian strategic culture throughout history, regardless of the shape of the state (be it the Russian Empire, the Soviet Union, or the Russian Federation). The cultural factor helps explain the constancy of the Russian military doctrine's political assumptions (based on the 'besieged fortress' syndrome, the preference given to the importance of domestic political security above other sectors of state security such as external, social or economic security; the constant striving to bring the population to a state of readiness for mobilisation, et al.). The specific strategic culture can be explained by the perception of risks as outlined above: the spectres of delegitimisation of power (a crucial element in the collapse of the USSR in 1991) and social radicalisation seem more dangerous to the Russian Federation's authorities than the fear of economic collapse or terrorism, which recede into the background. It also explains the glaring anachronism in the doctrine's wording: Russia, like the Soviet Union before it, is a global nuclear power, fighting for peace and the denuclearisation of the world, the demilitarisation of outer space and information space, and for its own system of values and its own model of development.

Moreover, in the light of Moscow's real political practices, the geopolitical method of the Russian theory of information warfare allows us to expand the list of the characteristics of Russian strategic culture:

(1) a tendency to guarantee the interests of the state through preemptive intervention (for example the invasion of Ukraine, or conferring a military dimension to Russia's Arctic policy);
(2) the syndrome of legalisation (the desire to superficially regulate all aspects of security, and also the use of force above the law);
(3) imposing the principle of limited sovereignty on neighbouring countries and allies (which has been confirmed not only by the

invasion of Ukraine, but also by Russia's inclusion of Abkhazia and South Ossetia into the common security field, despite the fact that none of Russia's allies have recognised these para-states);

(4) cultivating the principles of social life based on military patterns (the military-patriotic education of the young; the top-down militarisation and securitisation of the so-called civil society institutions; projects such as the Academy of Informational Self-Defence or the Russian Intelligence School; and above all,

(5) imposing a persistent ideological image of the world, in terms of confrontation between the 'American world' and the 'Russian world', between liberal and conservative values.

This specifically Russian cultural factor is helpful in explaining the motivations and arguments used in its information warfare. It also helps to identify many sustainable features of this struggle: the diversity of the tools it uses (from manipulation, intimidation by historical warfare and so on, up to state terrorism and armed attacks); a global, flexible approach; operations conducted simultaneously on many levels (diplomatic and military, economic and media). And because both the doctrine and the official propaganda have announced its intensification, the role of cultural analysis will increase. This should be taken further into account in considerations of security and defence policy, as well as when forecasting the fate of Russian geopolitical projects associated with this policy, including its leading project – **the Eurasian Union (EaU). This project is dictated by imperial egotism and a disregard of the interests of sovereign states.** In its pursuit to extend the EaU to include Ukraine, the Russians did succeed in exploiting the cultural inconsistencies in this country, but at the same time, processes were initiated which led to the strengthening of Ukrainian national culture and the creation of new symbols (the Euromaidan, the 'Heavenly Hundred'). At the moment, this is undermining the efforts of the Russian propaganda front, because neither Ukrainian nor global public opinion believes in the sincerity of

the intentions of an aggressor which presents itself as a 'guarantor of security'. In the case of Ukraine, the 'informational' bombs and mines have turned out to be duds.

The Russian military doctrine, however, gives us to understand that it has built up its potential of modern instruments for waging war, reached a state of readiness to mobilise, and is promising to escalate tensions. It has announced the further development of the forces and means to conduct information warfare, and that it can carry it out in a more integrated way. After the Russian aggression against Georgia and Ukraine, this announcement can be seen as preparing public opinion for subsequent violations of international order for geopolitical reasons – especially as the militarised theory of information warfare mentioned above has for years been reflected in political and military practice in Russia, in times of both war and peace.

## III. CONCLUSIONS

The information warfare emerging from the Russian Federation's military doctrine is the same phenomenon that journalists and civilian analysts have been describing as 'information war'. Its objectives, means and methods do not fit into the conventional notion of war.

Defining these in terms familiar from Western theories is pointless. **The Western terms borrowed into Russian theory and practice have been adapted to traditional activities.** The doctrine's civilian and military authors think in terms of sabotage, subversion, disguising their targets and leading their opponents into error; and not in the terms of categories of asymmetric threats or unconventional, non-lethal warfare borrowed from Western military thought.

As a result, **the Russian concept of information warfare is in fact a synthesis of traditional, old and modern methods (resulting from the current state of universal access to IT technology), military and non-military structures and means of influence.** By introducing non-military elements into the military organisation of the state, the doctrine confirms the *modus operandi* used hitherto. By giving a military dimension to ideological confrontation, the doctrine highlights the geopolitical motivations of Russian policy. Hence the conclusion that monitoring ideological and cultural trends will allow us to grasp the current objectives and motivations of this policy, of which information warfare is now a permanent part.

The continual referral to Western models for carrying out information warfare, and the emphasis on the need to improve the forces and means of this warfare, is a diversionary tactic designed to distract attention.

**Information warfare in Russia is a systemic phenomenon**; no other country deals with this issue on such a scale; no-one invests so much organisational and financial effort in it. Information warfare, as it has been conducted for decades, reveals enduring, long-term qualities based on Russian strategic culture.

**JOLANTA DARCZEWSKA**