57

OSW STUDIES

OSW

RUSSIA'S ARMED FORCES ON THE INFORMATION WAR FRONT

STRATEGIC DOCUMENTS

Jolanta Darczewska

OSW STUDIES

NUMBER 57
WARSAW
JUNE 2016

RUSSIA’S ARMED FORCES ON THE INFORMATION WAR FRONT

STRATEGIC DOCUMENTS

Jolanta Darczewska

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

EDITOR
Anna Łabuszewska

CO-OPERATION
Halina Kowalczyk, Katarzyna Kazimierska

TRANSLATION
OSW

CO-OPERATION
Jim Todd

GRAPHIC DESIGN
PARA-BUCH

ILLUSTATION ON COVER
Shutterstock

DTP
GroupMedia

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 978-83-62936-87-8

Contents

EXECUTIVE SUMMARY

1. The current militarisation of the public space in Russia is the result of a long process. Since 2000, the so-called information threats have been the subject of widely publicised strategies justifying the military's information policy and its tasks related to information warfare. Those tasks have not been limited to domestic projects; Russia's ambition is to act regionally and globally, and is building a common Eurasian information space. The country has put forward drafts of international conventions and codes of conduct concerning the international information space, thus demonstrating its own vision and asserting its right to co-decide on matters of global security.

2. Even though the military dimension of information security has long been acknowledged, until recently it was the Russian security services that had held a monopoly in this area, officially focusing on protecting the public against destructive external influences as well as the protection of critical information infrastructures. The situation changed at the start of the present decade when the activities of the military segment of the information security system, conducted on an unprecedented scale, became dominant in the public space. The main aim of these activities has been to legitimise the Kremlin's confrontational policy towards NATO and the West, which has been stepped up since Vladimir Putin returned to the Kremlin in 2012.

3. According to official declarations, the defence sector has "taken on the challenges concerning the security and defence of the Russian Federation", demonstrating its capability to counter information threats and co-operate with the security services. This linking of Russia's internal security strategy and defence strategy tied the strategic dimension of defence closely to the political dimension. As a result, the defence sector has started to perform certain functions in the public sphere that go beyond its defence competences (and into the realm of worldviews and education): it has demonstrated its readiness to prevent a wave of colour revolutions against the government of Russia, challenge NATO's hegemony in the information space, and defend the status of the Russian language and Russian-speakers in neighbouring countries as well as Russia's national interests outside Russian territory.

4. The question about the role of the armed forces in the information space is in fact a question about the role of the factor of force in the Kremlin's domestic and foreign policy. Over the course of history, this factor has invariably been treated as a hallmark of Russia's position as a global power, an instrument

of deterrence, and a way to exert political pressure and build spheres of influence. Today it has become an argument to support Russia's claims to the status of a Eurasian centre of power and development, in opposition to the Euro-Atlantic community. For the Kremlin, whose ambition is to change the current paradigm of international relations, this has served as the main justification for the annexation of Crimea, the war in Donbas and the military intervention in Syria.

INTRODUCTION

The present paper analyses the contents of several documents on strategy. This comprehensive approach highlights the various aspects of the Russian Armed Forces' activities in the field of information, including its activities in the area of cyberpower. It offers a basis to formulate conclusions about the continuity of Russia's strategic approach and the durability of the mechanisms employed to achieve the strategic objectives.

The paper consists of two parts: the first delves into the specifics of official documents, and the second discusses several examples of how the Russian Armed Forces' information activities have been operationalised in the information space at the national, regional and international levels.

I. OUTLINING THE PROBLEMATIC – THE MILITARY DIMENSION OF THE INFORMATION SPACE

1. Strategic duality

The significance of information systems increased considerably in the wake of the technological breakthrough in the last decade of the twentieth century, with the development of the Internet and the emergence of new information and communication technologies. The **Military Doctrine of the Russian Federation** adopted in 2000 noted for the first time that the computerised security and defence environment required new instruments and strategies. The Doctrine also showed the specificity of the Russian terminology in the field, underscoring the separateness of the Russian strategic approach. Unlike Western strategists, for whom the space of technologised information, i.e. cyberspace, was the main context in which to consider the new, computerised systems of combat and defence, from the beginning the Russians recognised the need/necessity for their armed forces to operate in the 'information space' and the existence of 'information threats' faced by the Russian army, while emphasising that these were psychological in nature.

The **Information Security Doctrine of the Russian Federation**, adopted in September 2000 and still in force today, also emphasises the military dimension of the information question (as construed in Russian terminology). It represents information security as the foundation of the security of the state, and identifies 'information weapons' as one of the instruments to pursue political objectives. A closer analysis of the section devoted to the state's 'information activities' in the sphere of defence also reveals the duality of the Russian strategists' thinking, which combines a technological approach to information with a psychological one. This duality is particularly visible in the assessment of information threats, which mentions foreign information-technological activities (radio-electronic warfare, penetration of computer networks, the use of outer space, air, marine and land means of intelligence and reconnaissance, etc.) alongside the information war concepts developed by a number of states, the ambition of some states to dominate and contain Russia's interests in the global information space, and potential sabotage activities by foreign secret services based on psychological and informational influence. Moreover, the Doctrine identifies the main directions for the further enhancement of defence measures[1], addressing both the technological and the psychological aspects.

The Doctrine is an extensive document that discusses in great detail the information threats affecting various domains (the economy, internal policy, foreign policy, science and technology, spiritual life, defence and the safeguarding of the legal order in Russia), and as such it introduces most of the terms subsequently used in other official documents and the broad literature popularising the question, including the notions of 'information war', 'information weapon', and the 'concealment of information counteraction'). The **2000 Information Security Strategy of the Russian Federation** remains the official blueprint on which later strategic documents often draw, because it offers an exceptionally broad conceptual framework: in that early document, the Russian government already warns of violations of the rights of Russian nationals and legal persons abroad and the spread of misinformation on Russia's foreign policy, and identifies "the Russian language [as] the factor fostering the spiritual unity of the nations of a multi-nationality Russia and the language of inter-state communication among the members of the Commonwealth of Independent States" as one of the objects of protection.[2]

An equally broad approach, which allows and deepens the terminological imprecision, can be found in the new draft of the **Information Security Doctrine of the Russian Federation,**[3] which has already been presented to the public for some time and is expected to be adopted in 2016. In paragraph 17, which con-

[1] These include: systematically detecting information threats and the sources thereof (...); certification of general and specialist software, utility packages and information protection measures in existing and new automated command systems and computerised military communication systems; constantly enhancing measures to protect information against unauthorised access, developing secure communication systems, military command systems and weapons guiding systems, improving the reliability of specialist software; enhancing the structure of the functional elements of the system to ensure information security in the field of defence and co-ordinating their co-operation; perfecting the methods and means of strategic and operational masking, intelligence and electronic warfare, the methods and means of actively countering the potential enemy's information/propaganda and psychological operations; and training specialists in the field of information security in defence.

[2] This approach is still unchanged. For instance, in a statement on 27 January 2016, General Sergei Chvarkin, deputy chief of the Military Academy of the General Staff, said that the declining position of the Russian language globally was one of the key threats to the Russian Federation's national security. In his view, the sphere of language and culture constitutes an important field of confrontation in the information wars of today (see: www.russkiymir.ru/news/202777).

[3] For the draft Doctrine text, see http://infosystems.ru/assets/files/files/doktrina_IB.pdf

cerns the specific tasks of the defence department in the information space, it mentions long-term tasks that are set to continue (monitoring threats, improving the information security system and developing the means and capabilities to engage in information warfare), as well as new guidelines concerning, for instance, the creation of adequate conditions to prevent information aggression under international law, the development of a military information policy, the strategic containment of conflicts in the information space, neutralising informational influence on civilians and young people in particular, through information, strengthening the historical, spiritual and patriotic tradition in society, etc. As a side note, the practical implementation of the 'strategic initiatives' mentioned in the Doctrine has long been underway, so its provisions should effectively be seen as providing a legal basis for the Defence Ministry's activities.

In comparison to the framework Doctrine discussed here, the successive editions of the Russian Military Doctrine (2010, 2014) are less precise and merely repeat the very generally-worded guidelines and postulates of the framework document.[4] The question of information security is rendered more abstract in those documents, and its strictly military aspects are barely discussed. However, there is an obsessive focus on the social and political-military elements. The 2014 edition emphasises the tendency of military threats to shift into the information space and the domestic sphere (p. 11), and warns of the use of information and communication technologies for military-political purposes to carry out actions that are incompatible with international law, and which target the sovereignty, political independence and territorial integrity of states (p. 12). It also habitually stresses the need to enhance the interoperability of the armed forces' information security system and the systems of other forces and bodies (p. 35) as well as with information management systems at the strategic, operational and tactical levels (p. 46).

2. Terminological newspeak

These vague and sweeping wordings, which resemble propaganda slogans, present a major problem of interpretation to external experts, and the glossaries included in some of the documents are not very helpful. For instance,

[4] For more information, see Jolanta Darczewska, The devil is in the details. Information warfare in the light of Russia's military doctrine, *Point of View*, OSW, No 50, May 2015; http://www.osw.waw.pl/en/publikacje/point-view/2015-05-19/devil-details-information-warfare-light-russias-military-doctrine

the Russian Defence Ministry's document entitled **The Russian Federation Armed Forces' Information Space Activities Concept** (2012)[5] defines the key notion of 'information space' as "the sphere of activity related to shaping, creating, transmitting, using and storing information, which influences individual and social awareness, as well as the information infrastructure and information in the strict sense". By using such a definition, the authors have in a way replaced the notion of the 'information system' which in Russia and all other states stands for the set of resources, people and technologies (including IT and ICT), as well as the methods and processes for obtaining, collecting, processing and presenting information. As defined, the information space, which is a military field of confrontation and information warfare, is simultaneously geographical, political, economic, social and civilisational (i.e. spiritual, linguistic and cultural) in nature. The notion of a system is also used in the document to traditionally emphasise its omnipotence: the armed forces are referred to as "part of the information security system of the Russian Federation", which, in turn, is vaguely defined as "the part of the national security system devoted to implementing the state's policy in the sphere of information security". Both notions are widely used in the military's information practice, but they serve different propaganda purposes.

3. The army as part of the information security system

This kind of composite notion, however, should not obscure the main message of the documents discussed here, which is that the Russian armed forces undertake defensive measures (protecting their own information system from impact, destruction and disruption by the enemy), as well as offensive activities (aimed at impacting, damaging and destroying the enemy's information system). In this, the Russian army is no different from the armies of other states. The principal difference lies in the fact that the Russian armed forces, together with the other actors in charge of the Russian Federation's internal and external security, have been assigned the task of defending the Russian information space against competing models of political, economic, social and cultural development, i.e. effectively defending the autocratic Russian regime, and have since at least the year 2000 been preparing for conflicts in the information space and building up their capacity to engage in such conflicts.

[5] Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве – see http://function.mil.ru/news_page/country/more.htm?id=10845074@cmsArticle

Moreover, the 'information weapons' employed against the West today have been tested internally as Russia has built up the "single information space of the Russian Federation", i.e. as the state took over control of the information system, and its main pillar, the major media outlets. The Russian secret services have been the main actor in charge of this task. They have used various measures, ranging from repression against NGOs ('foreign agents') and the establishment of a massive number of GONGO (state-controlled non-governmental organisations), the development of analytic institutions (the so-called social think tanks) and journalism, cyber-attacks against opposition activists and media, and the forced closures of opposition media and social portals under the pretext of fighting extremism. Until recently, the secret services held a monopoly on information security in the Russian Federation. The situation changed at the start of the present decade: the information space became dominated by the activities of the military sector of the system, and the main focus of these activities has been to legitimise the Kremlin's confrontational policy towards NATO and the West.

In this context it should be noted that the bias towards information activities which is notable in the strategic documents is deliberate. By drawing the public's attention to the importance of the factor of force in external relations, the Russian strategists can trigger a confrontational mode of thinking and instil a distrust of and hostility towards the West, especially the United States and NATO. According to this widely disseminated propaganda, whose conceptual framework is laid down in these publicly available strategic documents, it is the West that has declared an information war on Russia and started an information arms race.

II. GENERAL DISCUSSION OF THE RUSSIAN STRATEGIC DOCUMENTS

1. Sources

Apart from the above-mentioned **Military Doctrine of the Russian Federation** and the **Information Security Doctrine of the Russian Federation**, indications as to the strategy of the Russian armed forces' activity in the information space can be found in a number of other documents (see Appendix 1). Some of them, such as the **National Security Strategy of the Russian Federation** adopted on 31 December 2015, offer a superficial treatment of the matters in question, while emphasising the importance of new military technologies and the need to defend both Russia's public and its "cultural sovereignty" against destructive informational influences. Others, such as the **Basic principles for the Russian Federation's state policy in the field of international information security to 2020,** adopted in July 2013, are dedicated exclusively to the topics discussed here, but they do not particularly highlight the role of the armed forces (or the other actors involved in Russia's information security). It is worth noting that the documents named here are publicly available; for instance, they may be consulted via the website of the Security Council of the Russian Federation.[6] They have been authorised by the Council, which also holds information patronage over them, that is, it has been promoting them in a long-term propaganda campaign.

The **Russian Federation Armed Forces' Information Space Activities Concept**, drafted by the Ministry of Defence and published in January 2012, is another publicly available ministerial document. It is the least-known strategic document, and for this reason it is treated in more detail here (see Appendix 2). However, many ministerial documents of a strategic nature remain classified. Documents that have not been publicly released include **Basic principles for military-technological policy to 2020 and beyond** of 26 January 2011, **The main directions of the state's policy with regard to the security of automated systems for the management of the technological and production processes of critical infrastructure facilities in the Russian Federation** of 3 February 2012, and the **Concept paper on the development of information and communication technologies of the Russian Armed Forces to 2020**, mentioned by defence minister Sergei Shoigu on 30 March 2015 during a meeting of the Defence Ministry College.

[6] See Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года; http://www.scrf.gov.ru/documents/6/114.html

A comprehensive analysis of these strategy documents makes it possible to capture the specificity and see the continuity of the Russian strategic approach towards attaining the Russian army's short- and long-term objectives in the information space.

2. Basic problem: social engineering

The way in which Russia considers the army's role in the information space fundamentally differs from the Western model. In the latter, 'cyberspace' is the key notion, which is more appropriate to the military context. The Russian strategists, however, use the notion of 'information space', which they put in the context of social, political and civilisational threats. This is a deliberate manoeuvre that helps to justify the Kremlin's domestic and foreign policies. By emphasising the 'informational' nature of the Russian army's activities and not their 'cybernetic' nature, the strategists focus on information (and its content), as well as the political agitation and mobilisation it engenders, which is in line with the mission entrusted to the armed forces of neutralising the influence of information on their own personnel and the civilian population. Emphasis is laid on the army's involvement in government propaganda via a separate, military module of the propaganda apparatus, of which the *Krasnaya Zvezda* media holding and its associated traditional and electronic media are part.

At the same time, **the Russian strategists clearly draw upon Western military thought; for instance, they have been popularising the concept of hybrid wars in recent years. In this way, they seek to show that Russia's activities are no different from the equivalent measures by Western actors. This manoeuvre, also used in professional literature, often leads foreign analysts astray if they treat the ambiguous Russian terminology as a mirror image of their own terminological apparatus. Yet the Russians are guided by their own assumptions and logic in adopting Western notions, which they adapt to their own needs and traditions and their distinct strategic culture. When transplanting Western theories onto Russian soil, they deliberately confuse the concepts of attack and defence, adjusting them to Russia's own geostrategy of revenge.**[7]

These differences are reflected in the propaganda: for instance, if the NATO doctrine emphasises military reconnaissance and protection of reconnaissance data

[7] See Владимир Горбулин, „Гибридная война" как ключевой инструмент российской геостратегии реванша, *Зеркало Недели,* 23 January 2015; http://gazeta.zn.ua/internal/

using new technologies COMSEC (communication security) and COMPUSEC (computer security) the Russian doctrine warns its military against the enemy's 'information weapons'; and while Western forces are expected to provide 'psychological cover for the combat theatre', the Russian military is tasked with neutralising the enemy's psychological impact on civilians with a view to 'safeguarding the historical, spiritual and patriotic traditions of defending the Homeland', and so on.

3. The fourth threat

The notion of the so-called fourth threat, which occupies a priority position in military strategic thinking, is a telling example of this tendency to blur the division between the political and the military. The Western triad of cyber-threats (cyberwar, cyberterrorism and cybercrime) has been expanded in Russia to include information interference in the internal affairs of sovereign states. The 2013 document **Basic principles for the Russian Federation's state policy in the field of international information security to 2020** defines such interference as "the use of information and communication technology as an information weapon for political and military purposes with a view to interfering in the internal affairs of states, (...) undermining public order, inciting ethnic, racial or religious hostility, promoting racist and xenophobic ideas and theories leading to hate and discrimination and encouraging violence".

In the 2000 **Information Security Doctrine of the Russian Federation**, the 'fourth threat' appears in the form of factors threatening spiritual life, such as "the possible undermining of social stability, harming the lives and health of citizens as a result of activities of religious associations preaching religious fundamentalism and totalitarian religious sects; the use by foreign secret services of mass media operating on Russian territory in order to undermine the country's security and defence capability; the spreading of disinformation; the inability of contemporary civil society in Russia to ensure that the young generation embraces, and the society at large maintains, the desirable ethical and patriotic values and responsibility for the country".

In this context, there have been calls for a mechanism to control the formation of spiritual values in the society in line with the country's national interest, educate young people in the spirit of patriotism and responsibility for their home country, and enact laws to regulate the constitutional restrictions on the rights and liberties of people and citizens; as well as calls for state support for actions aimed at reinvigorating the cultural heritage of the nations and nationalities of the Russian Federation and creating "legal and organisational mechanisms to prevent unlawful information and psychological influence on the public's mass awareness and the uncontrolled commercialisation of culture and science, and mechanisms to guarantee the preservation of the cultural and historical values of the nations and nationalities of the Russian Federation".

The fourth threat has a practical dimension, in that it serves the pursuit of various political objectives. This is clear for instance from the way this notion has evolved. In 2000 it served to emphasise the importance of "countering the negative influence of foreign religious organisations and missionaries", but the subsequent wordings in doctrinal documents and the opinions of military experts on the issue emphasised the need to counter the colour revolutions, which were called "a political technique of the United States' and NATO's expansionism."[8] The fourth threat has given rise to an avalanche of theoretical papers on contemporary information wars, which – as has been emphasised – lead to "the psychological extermination" of the people and catastrophic political and social consequences. It has become the common denominator of actions undertaken by various state actors (the Armed Forces, the security and public order services) or public-private bodies (analytic centres and associations, foundations, etc.). In the daily practice of the army's information activities, phrases such as "the US and NATO's criminal interference"[9] offer on the one hand a universal key to interpreting contemporary conflicts, and on the other, an argument to justify the Russian armed interventions in Ukraine and Syria.

4. The civilisational context

The documents discussed here are in keeping with the general line of contemporary strategic thinking in Russia, which seeks a revision of the post-Cold War international order on the grounds of the civilisational distinctness (different values) of the so-called Russian World (русский мир), understood in a wider sense as the 'Eurasian world'. They are also in line with Russian strategic culture, with its enduring tendency to treat force as a means to political ends. The

[8] This does not mean that Russia has given up the fight against the 'worldview saboteurs', whom it juxtaposes to those confessing Orthodox Christianity. The journalistic and popularising writings of Tatiana Grachova, dean of the Military Academy of the General Staff, offer numerous examples. Phrases such as "the Vatican's militant network" can be found in abundance in her book Татьяна Грачева, Память русской души. Алгоритмы геополитики и стратегии тайных войн мировой закулисы, Рязань 2011.

[9] The words of Prof. Alexander Bartosh, member of the Academy of Military Sciences, director of the Information Centre for International Security at Moscow State. Linguistic University; see Александр Бартош, Цветные революции и гибридные войны современности; http://nvo.ng.ru/gpolit/2016-01-22/1_revolutions.html

geopolitical and civilisational rivalry with the United States and their allies has determined the visible evolution of the Russian strategic documents, whose rather moderate rhetoric at the onset of the previous decade has gradually given way to the language of confrontation. The rivalry with a 'situational' enemy (the enlarging NATO) has morphed into a clash with an 'absolute enemy', one which questions Russia's role as an important centre of global power. This evolution found its condensed expression in the new **National Security Strategy of the Russian Federation** (2015), which verbalised Russia's strategic bloc thinking. The document names NATO and the United States, with its ambition to "preserve its dominance in global affairs", as the main enemies whose "growing potential in terms of force and global functions constitutes an obvious violation of international law". In articles 14 and 16 the document introduces the notion of the "Euro-Atlantic region", which it juxtaposes to the "Eurasian region" in order to contrast the geopolitical concept of Eurasia with the Euro-Atlantic concept, and the North Atlantic Alliance with the Collective Security Treaty Organisation (CSTO). In paragraph 90 the document states: "Russia's aim is to transform the CSTO into a universal international organisation capable of responding to military-political threats, military-strategic threats and threats in the sphere of information".

The fact that reinvigorating the CSTO (the 'Eastern NATO') has once again been included in Russia's national security strategy shows that the Russians are not particularly inventive in this regard and are not producing any new strategic ideas. As has been said before, they often borrow concepts and ideas from Western doctrines. Likewise, many Russian strategic concepts may be seen as reactions to Western strategies. For instance, the **Russian Federation Armed Forces' Information Space Activities Concept**, published in early 2012 on the Ministry of Defence website, was a reaction to the document **The U.S. Department of Defence Strategy for Operating in Cyberspace** released in 2011.[10]

The Russian concept paper echoes the US Department of State document, which laid down five strategic initiatives:

- recognising cyberspace as an operational domain of the armed forces;
- enhancing the DoD's means of defending its communication networks;
- partnering with other government bodies and the private sector to implement the cybersecurity strategy;

[10] U.S. Department of Defense, Strategy for Operating in Cyberspace, July 2011; www.defense.gov/news/d20110714cyber.pdf

- collective defence and collective prevention of cyber-attacks within NATO and other alliances;
- innovation to develop cyber-security capabilities.

The Russian document also recalls the US **International Strategy for Cyberspace**, adopted in the same year,[11] which said that hacker attacks against US critical infrastructure would be treated as acts of aggression, and listed the political and military consequences, including the use of all necessary means. The Russian documents treats the information space in a similar way to how the US strategy treats cyberspace, recognising it as a strategic field and a new theatre of military operations. Russia reserves the right to "enforce the law using all available military means" (while at the same time decrying an equivalent provision in the US strategy as "confrontational"). The reactive nature of the Russian documents is also visible in the chronology of their publication:

United States	**Russian Federation**
The U.S. Department of Defence Strategy for Operating in Cyberspace (2011)	Russian Federation Armed Forces' Information Space Activities Concept (2012)
International Strategy for Cyberspace (2011)	Foundations of the Russian Federation's policy in the field of international information security to 2020 (2013)

5. The internal and external addressees of Russia's strategic reflection

Western military strategies are usually addressed to state governments, and are a way for the military to present action plans, set new directions of action and highlight existing deficiencies. Russian strategic documents, however, are initiated from the top, as one can see in the relevant decrees by President Putin.[12] Russian strategy documents are part of the Kremlin's broader information strategy and are addressed to specific actors, both in Russia and abroad.

[11] https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[12] In this context, it is worth mentioning the **Concept paper on the state system for monitoring, preventing and eliminating the consequences of computer attacks against the information resources of the Russian Federation** of 12 December 2014 (No K 1274), which was drafted under a relevant decree issued by President Vladimir Putin on 15 January 2013 and has been partially published. As a side remark: the system of territorial centres is coordinated by the Federal Security Service, and it is also known that individual sections of the system, including the Armed Forces, may set up their own centres, for which they are permitted to take sole responsibility.

The anti-Western rhetoric serves domestic policy purposes: initially, it helped foster the citizens' demands for a strong and internationally respected state, and today it boosts their readiness for mobilisation by fuelling a sense of threat from the West.

The strategy documents are also addressed to public opinion in the countries of the Commonwealth of Independent States. By winning it over, the Kremlin hopes more easily to attain its geopolitical objectives, such as preserving its influence in the former Soviet area and preventing the post-Soviet states from integrating with the West. The external and internal dimensions are closely intertwined, thanks to the 'Eurasian world' concept mentioned above. Consequently, measures to counter the so-called fourth threat are presented as the defence of a civilisational community against the intrusion of a foreign cultural code. Again, the same type of narrative built on the opposition between 'us and them' is employed here. By engaging the CIS countries in closer military co-operation, the Kremlin strengthens its instruments of domination in the post-Soviet area, while at the same time intimidating the countries concerned by emphasising the consequences should they attempt to pursue a multi-vector policy and seek integration with actors other than Russia. In an effort to expand its circle of allies, Russia has been representing itself as the defender of "national sovereignty in the global information space". The new draft **Information Security Doctrine of the Russian Federation** defines this kind of sovereignty as "the state's capability to pursue an independent and single-handed policy in the global information space in order to defend its national interest and its information space". The provision in the 2010 Military Doctrine, which expanded the catalogue of situations in which Russia could use force by including the defence of Russian-speaking populations, was also addressed to audiences both inside Russia and in the region. The manoeuvre had a dual purpose: to increase pressure on countries in the nearest neighbourhood and mobilise their Russian-speaking citizens, and inside Russia, to consolidate the belief that that the Russian state is effectively protecting the interests of its citizens.

A third group to which the Russian strategy documents are addressed comprises opinion leaders in the West or, more broadly, international public opinion. External experts tend to treat Russia's strategic planning documents as a reliable source for analysing the Russian perceptions of threats and identifying the real intentions of Russia's political and military leaders. However, it should be remembered that – like all other information concerning Russian government departments in charge of security and defence – these documents are subject to procedural limitations imposed by the strict regime of the protection of state secrets. This means that public documents and official statements by representatives of the military should not be trusted unconditionally. Their primary purpose seems to be to convince Russia's potential enemies of the futility and purposelessness of any attempts at influencing Russia and its allies. Thus, these documents should be treated as instruments of diplomacy and military propaganda rather than a declaration of real intentions.

Moreover, given the fact that Russia has actually resorted to the use of force, we are also justified in not trusting the 'defensive' rhetoric of these documents, which invariably emphasises Russia's peaceful intentions, its commitment to act in accordance with international law and to seek de-militarisation of the information space, and its calls for a halt to the information arms race. The same narratives are used in relation to those actions by the Armed Forces which amount to involvement in open geopolitical confrontation, such as the operations in Ukraine and Syria. For instance, Nikolai Patrushev, secretary of the Security Council of the Russian Federation, has said in this context that "the United States, supported by Western states, intends to maintain its dominance in global affairs and aims to limit the Russian Federation's ability to pursue an independent internal and foreign policy".[13]

6. New trends?

Recently, 'Anglo-Saxon' terms such as 'cyberstrategy', 'cyberthreats' and 'cyberwar' have started to appear in the discourse of the Russian military (albeit not in the mainstream). They have been introduced into public debate by researchers, diplomats calling for 'an internationalisation of moves towards cyber-disarmament' and politicians such as Irina Yarovaya, head of the State Duma Committee for Security, who mentioned them in the context of Russia's 'digital sovereignty', and Dmitry Rogozin, the deputy prime minister in charge of supervising the Russian arms industry, who announced in March 2012 that Russia would create a military cyber-command modelled on the U.S. CyberCom, and at whose initiative the establishment of the Foundation for Prospective Research (which Rogozin saw as the Russian equivalent of DARPA[14]) was widely reported to the

[13] Вызов принят, Николай Патрушев: подготовлена обновленная Стратегия национальной безопасности РФ, *Российская Газета,* 22.12.2015, http://rg.ru/2015/12/22/patrushev-site.html

[14] DARPA (Defence Advanced Research Projects Agency) – a US agency established in 1958 to pursue research and develop key military technologies. The Russian Foundation for Prospective Research (http://fpi.gov.ru) was set up in late 2012 and is headed by General Andrei Grigorev, former chief of the Federal Service for Technical and Export Control, which is in

public. However, it is clear from Rogozin's lecture, which was delivered as part of the so-called patriotic platform of United Russia[15], that he views 'cyberthreats' as equivalent to 'information threats', and that he is exploiting the stereotype of 'digital sovereignty' (i.e. Russia's technological self-sufficiency) for political propaganda purposes. It should also be noted that despite some attempts in that direction,[16] cyberstrategy has yet to become the subject of a dedicated doctrinal discussion. However, these attempts at overcoming the terminological tradition dominated by the adjective 'information' do not mean that the Russian military strategists' approach to the issue has changed: the priority is still on threats related to the social and political aspects of information warfare, and not on cybernetic threats of immediate concern to the military. What they do mean is that the calls by the military and experts to strengthen Russia's strategic military cyber-potential are being heeded at the top levels of government.[17] It may also be the case that the idea to develop Russia's cyber-potential is simply an instrument of certain lobbies within the Russian arms industry and the top echelons of the institutions of force.[18]

7. A systemic approach

The documents which make up this element of Russia's information strategy (including military strategy) serve different functions than their equivalents in the West.

charge for the technical side of Russia's information security. The Foundation organises and finances research into military and dual-purpose technologies.

[15] Лекция Рогозина в рамках проекта партии «Гражданский университет»; http://er.ru/news/102261/

[16] In 2012–2014, at the initiative presented to the Federation Council by the United Russia activist Ruslan Gattarov; Комиссия СФ инициирует обсуждение стратегии кибербезопасности РФ; http://ria.ru/defense_safety/20140110/988508179.html

[17] As evidenced indirectly in a statement by Nikolai Nikiforov, the minister for telecommunications, who said during last year's *Tavrida* youth forum near Sevastopol in Crimea that Russia needed one million programmers in order to achieve "full digital sovereignty". The minister also recalled the objectives of the **Strategy for the development of the IT industry in the Russian Federation in the years 2014–2020 and to 2025,** published in 2013 (Стратегия развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года, http://www.minsvyaz.ru/ru/documents/4084/), under which the number of programmers in Russia should reach 700,000 by 2020.

[18] It is noteworthy that the quarterly *Вопросы кибербезопасности* (www.cyberrus.com), which has been on the market since 2014, was founded and is published by a closed joint stock company called NPO Echelon (http://npo-echelon.ru/) and the Research Centre for Legal Information at the Ministry of Justice.

The **forecasting** function is of only marginal importance because the documents manipulate international realities, while other functions are at the forefront, including:

- the **worldview** function (defining Russia's place in the world and its struggles with the major global centres of power),
- the **methodological** function (developing a coherent approach to the problems faced by the Kremlin in internal and foreign policy),
- the **educational or didactic** function (building up the morale of the army and the people, expanding the country's mobilisation potential),
- the **mobilisation** function (making sure that all available resources and means are used, and managing this potential effectively).

Taking a systemic approach allows Russia to demonstrate power while at the same time presenting its non-military instruments, i.e. political, economic, information, humanitarian, diplomatic and other means, as well as its potential for indirect action (sanctions, blockades of transport routes, threats to use force, sabotage, etc.). In the 2014 Military Doctrine, these can be found in the section devoted to contemporary armed conflicts which are characterised *inter alia* by "the comprehensive use of armed forces as well as political, economic information and other non-military means, as well as extensive use of the potential of protests and special force operations (...)". The **Basic principles for the Russian Federation's state policy in the field of international information security to 2020** include a fragment saying that the document was created, among other purposes, in order to "build interagency co-operation in implementing the Russian Federation's state policy in the field of international information security" and "achieve and maintain technological parity with major world powers through an increased use of information and communication technologies in the real economy" (point 5). The systemic approach is also highlighted in the **Russian Federation Armed Forces' Information Space Activities Concept**, which establishes the principle of close co-operation between the army and the secret services within a unified information security system of the Russian Federation.[19]

[19] The annual joint exercise by the Ministry of Defence, the Federal Security Service, the Ministry of Communications, the Ministry of the Interior and other bodies, during which the participating institutions assess the risks related to external influence on the Russian information space, is a practical implementation of this principle (the exercise has been reported to the public since 2014). The Ministry of Defence also initiated the First Interdepartmental Conference on 'The System of Interdepartmental Co-operation in the Field of Information', which took place on 19 November 2015. Moreover, at the initiative of Defence

It should be noted that describing the information security system of the Russian Federation presents some major difficulties, for several reasons. Firstly, information security is a trans-sectorial domain, i.e. it spans various fields ranging from defence, security, social matters, the economy, culture, etc. Secondly, the task of safeguarding Russia's information security has been entrusted to many institutions and state bodies. **At the core of the system there are the secret services, the armed forces, the police formations, sections of the administration, as well as expert, training, research and production institutions. The public segment of the system is complemented by private security institutions with which it co-operates closely. The interdependencies between these actors and the legally imposed obligation to co-operate are intended to produce a synergy effect.**

Each of the elements mentioned above has its specific characteristics related to its assigned scope of responsibility. Some of the information security structures operate covertly (e.g. the intelligence services), while others are fully transparent (e.g. the Federal Service for Supervision in the Sphere of Telecommunication, Information Technologies and Mass Communications[20]). Some services have very broad competencies and wide catalogues of tasks, while others are more narrowly specialised. This also applies to the elements of the information security system autonomously managed by the Ministry of Defence.[21]

Minister Sergei Shoigu, a presidential decree on the procedures for collecting and exchanging information relevant to the defence of the Russian Federation was issued in September 2014 (http://stat.ens.mil.ru/science/conference/smiv2015/about.htm).

[20] Госкомнадзор in Russian. The Service is supervised by the Ministry of Communications and Mass Media. It keeps registers of telecom operators and mass media, grants operating permits to media and bans them (including internet portals and blogs), authorises publications by foreign publishing houses in the Russian Federation, etc.

[21] For instance the National Defence Centre has been assigned many functions, as it comprises elements of the systems of command, control, communications and reconnaissance, integrating command systems with reconnaissance and logistics systems; it also serves as a videoconferencing centre for military information and propaganda, while a company of researchers set up at the Central Military Archive has been tasked with demystifying any distortions of Russia's military history.

III. HOW THE INFORMATION SYSTEM OPERATES: SELECTED CASE STUDIES

The military information policy is a part of the Kremlin's militarist policies. Its direct consequences include a militarisation of the language of politics and propaganda, a kind of 'martial law thinking' being imposed on the public opinion, and a radical change of the Russian army's image. The Armed Forces are no longer the '*lumpenmilitariat*', or the negative protagonist they had become in the aftermath of the wars in Chechnya and other developments. The army is now seen as the main pillar of Russia, a strong state holding the status of a world power. Most importantly, however, the army has now switched to offensive and pre-emptive mode as a result of this policy. Today Russia forcefully demands that other countries respect its spheres of influence in the neighbourhood (as seen from its aggression against Ukraine and its armed intervention in Syria). It claims to be the guarantor of peace processes, even as it demolishes the European and global security architecture. Using the factor of force to build up its international position, it makes clear that the West should discuss the resolutions of these conflicts primarily with Russia (in order to avoid large-scale war). By pushing through its distinct understanding of international information security, Russia asserts its right to co-decide on global security issues.

Selected examples of the activities of the Russian information system will be presented below, with special emphasis on the military section of that system. The activities presented are taking place at the global, regional and national levels.

Our premise here is that Russia's long- and short term strategic objectives can only be identified through an analysis of its actual activities at the operational level.

1. The objectives of international co-operation in the information space

Russia has been promoting its own information security concepts internationally for many years, and has undertaken a number of initiatives in this domain, presenting them as its contribution to the development of the global information security doctrine.[22] In the Russian Information Security Doctrine

[22] See for instance: Бедрицкий А.В., Информационное доминирование США и асимметричное информационное противоборство / США и Канада: экономика, политика, культура. – М.: ИСКРАН, 2007. – № 2. – С. 91–102; Бедрицкий А.В., Международные договоренности по киберпространству – возможен ли консенсус (http://www.riss.ru/images/pdf/journal/2012/4/10_.pdf).

discussed above, this approach found its expression in the section on strategic containment, which includes a provision stating that "The main objective of international co-operation is to establish an international legal system to regulate activity in the global information space, including military activities by state actors". The external context has two levels here: the global and the regional ("It is a priority for the Armed Forces of the Russian Federation to co-operate with states that are parties to the Collective Security Treaty and members of the Commonwealth of Independent States and the Shanghai Co-operation Organisation, and the Armed Forces will seek to expand the number of partners and develop co-operation on the basis of common interest.")

It is not possible to correctly identify Russia's broader political and military objectives vis-à-vis the external world on the basis of the laconic wordings in the strategy documents. Moreover, the declared strategic objectives do not match those which Russia has actually been pursuing in practice. The country's real intentions are more clearly visible in those parts of the documents which discuss Russia's perception of threats (with information threats considered to be the most important, as their existence is seen as evidence that the West, i.e. mainly the United States and NATO, is interfering in Russia's internal affairs and targeting the country's vital interests), or the provisions on the use of force to counter threats. The latter element seems to be key: in successive editions of the documents the range of situations in which Russia reserves the right to use force has been expanded, initially by including the regional security context (protecting Russian-speaking citizens), and subsequently the pursuit of international policy objectives. In this, information threats were presented as a direct source of a conflict that could be resolved using 'all necessary means'.

The Russian strategists are particularly concerned about the military and technological advantage of the United States and its allies, including in the information space, to use the Russian terminology. This concern is expressed in the document published on 24 July 2013 and titled **Basic principles for the Russian Federation's state policy in the field of international information security to 2020,**[23] which Russia formulated as a reaction to a similar strategy adopted by the United States. By presenting its own approach, Russia is raising a *votum separatum* against the US vision (which, as the document emphasised, is also shared by Europe). The document outlines the main objectives of Russia's international activity, which are to build an international information security

[23] See Основы государственной политики Российской Федерации в области международной информационной безопасности…, *op. cit.*

system, develop mechanisms for international co-operation in this area, and assemble a wide front of support for Russia's initiatives aimed at internationalising the management of the Internet and the International Telecommunication Union (ITU)[24]. The document also states that Russia will co-operate closely with its allies, especially the members of the Shanghai Co-operation Organisation, the Collective Security Treaty Organisation, the CIS and BRICS (Brazil, Russia, India, China and South Africa).

The language of the document clearly echoes the rhetoric of the Cold War: like the USSR in the old days, Russia today is fighting for the demilitarisation of outer space and a stop to the arms race, and is also championing efforts to internationalise the global information space, ensure the non-proliferation of information weapons and preserve the information sovereignty of states, both with regard to information technology (reaching technological parity and overcoming technological disparities between developed and developing countries), and political sovereignty (the phrase "acts of information aggression aimed at discrediting the sovereignty of states" is used several times in the document).

The actions taken in connection with this document can be seen as an example of how Russia operationalises its strategic objectives. The 'strategic initiative' outlined in the document has been reinforced institutionally, as the Ministry of Foreign Affairs has assumed the task of co-ordinating all the activities aimed at fostering international information security. A position of presidential plenipotentiary for international information security has been created within the Kremlin administration, and the diplomat Andrei Krutskikh has been appointed to do the job. As reported by *Kommersant*, "the Security Council and the relevant ministries were asked to present concrete proposals for

[24] Russia had already launched a diplomatic offensive to revise the existing system for managing the world wide web at the United Nations in the previous decade. It then stepped up its efforts in the run-up to and during the World Conference on International Communications in Dubai (December 2012). In coalition with China, Russia has also sought regulation of the Internet under international law, arguing the web should be managed by the International Telecommunication Union (ITU – a specialised UN agency for the standardisation and regulation of the global telecommunications market). Russia's key demand is to for the management of domain registries to be taken away from the ICANN (the Internet Corporation for Assigned Names and Numbers, an international non-profit organisation based in Los Angeles, set up in 1998 to take over the management of the Internet from the US government administration) and entrusted to national governments. Under the Russian proposal, member states of ITU should have a sovereign right to manage the internet on their respective territories and exercise more control over it, while the ITU should oversee measures concerning cyberspace security and the combatting of cybercrime.

measures to implement the *Basic Principles* to the president".[25] The document itself reads: "the state's policy in this area will be implemented by the federal executive bodies, within their respective remits, (...), and also through public-private partnerships".

The fact that the document was published at that time did not in any way mean that the implementation of its objectives started then; in practice it has been underway at least since the year 2000. It seems, therefore, that the intention behind the *Basic Principles* was to keep up the momentum of the information campaign and expand it into the region. The organised activity of the expert and analytic community testifies to this, with numerous publications (including some addressed to audiences outside Russia),[26] as well as conferences devoted to the subject at the Moscow State Institute of International Relations (MGIMO), the Russian Institute for Strategic Studies (RISI) and other institutions. Similar information campaigns accompanied the publication of the draft **UN Convention on International Information Security** (2011) and the draft **Code of Conduct for International Information Security** (2011), which were put forward at the UN by Russia and China with the backing of Tajikistan and Kyrgyzstan. The contents of these documents are no different from what is stipulated in the *Basic Principles*: what the documents have in common is the idea that information war is a crime against global peace and international security. The drafts tabled at the UN broadly outline the threats present in the information space (mentioning disrespect for the cultures, history and social systems of individual countries, the proliferation of information weapons, and impeding access to the newest IT technologies, alongside cyberterrorism and cybercrime), and propose a set of principles that should govern international information security (including a levelling of the differences in information technology advancement between states, the right of states to establish sovereign legal norms and manage the information space on their own territories, the principle of territorial jurisdiction with regard to the penalisation of information crimes, the principle of non-interference in the information space of states, etc.).

[25] Елена Черненко, Мир домену твоему. Россия определилась с информационной безопасностью, *Коммерсант*, 1.08.2013; http://www.kommersant.ru/doc/2245463

[26] The propaganda campaign accompanying the release of the document juxtaposed Russia's position to the confrontational approach of the United States, whose objective, according to the campaign, is to "ensure its own supremacy and global dominance in the cyberspace (...). Russia's aim is not to dominate cyberspace. Instead, it insists that some general principles should be adopted for this sphere in order to avoid cybercrime and cyberthreats". http://pl.sputniknews.com/polish.ruvr.ru/2013_08_02/Rosja-okreslila-koncepcje-cyberbezpieczenstwa/

Experts from the Russian Ministry of Defence contributed to formulating these principles. They had long called for the cyberspace to be regulated under international law, including the international law of war,[27] arguing that the absence of regulations on the use of 'information weapons' encouraged countries to use them. Officials from the Ministry have also taken in various conferences in Russia and abroad, such as the annual conference on international information security in Garmisch-Partenkirchen in Bavaria, which Russia co-organises.[28] There are also some scarce reports that the Centre of Military-Strategic Studies of the General Staff of the Russian Armed Forces participates in the drafting of strategic documents.[29]

The West did not back Russia's initiatives at the UN, seeing them as an instrument to take a more hard-line course in its internal affairs by restricting the freedom of speech and limiting access to the world wide web. Meanwhile, domestic and foreign public opinion has been constantly fed the message that Russia is an informational global power which comes up with initiatives for global solutions to stop the information arms race. During the Infoforum-Eurasia in Sevastopol in July 2015, Andrei Krutskikh, the Russian president's plenipotentiary for international information security, said that the Russian-proposed basic

[27] See for instance, S.A. Komov, S.V. Korotkov, S.N. Rodionov, International Information Security: Military Aspects, *Military Thought*, volume 12, number 4, 2003, p.1-5; I.N. Dylevsky, S.A. Komov, S.V. Korotkov, Military Aspects of Ensuring International Information Security in the Context of Elaborating Universally Acknowledged Principles of International Law, *Disarmament Forum, ICTs and international Security*, number 3, 2007, p. 35-43; S.M. Boyko, I.N. Dylevsky, S.A. Komov, S.V. Korotkov, S.N. Rodionov, On International Legal Qualifications of Information Operations, *Military Thought*, volume 17, number 1, 2008, p.15-25; *International Information Security: Problems And Decisions*, chapter 3, 'Military-Political Aspects For Provision of International Information Security', edited by S.A. Komov, Moscow, 2011.

[28] Представители МО РФ о применимости норм и принципов международного права к военной деятельности в информационном пространстве, https://digital.report/predstaviteli-mo-rf-o-primenimosti-norm-i-printsipov-mezhdunarodnogo-prava-k-voennoy-deyatelnosti-v-informatsionnom-prostranstve/; Анатолий Стрельцов о проблемах адаптации международного права к информационным конфликтам, https://digital.report/problemyi-adaptatsii-mezhdunarodnogo-prava-k-informatsionnyim-konfliktam/

[29] See for instance, Александр Пинчук, Центр военно-стратегической мысли, 26 January 2010, http://old.redstar.ru/2010/01/26_01/2_02.html. See also С.Г. Чекинов, Центр военно-стратегических исследований Генерального Штаба Вооруженных Сил Российской Федерации: история и современность, *Военная Мысль,* № 1/2010, стр. 3-5. Colonel Chekinov, the Centre's chief, links its establishment in 1985 to the fundamentally altered situation after the process of reducing of strategic nuclear potentials started. "It went hand in hand with the implementation of high-precision conventional weapons systems, militarisation of space and active information warfare (...) because as the Cold War transformed into new forms, the contradictions between states did not subside, but became even more pronounced."

principles of conduct in global networks had been approved by UN experts. Krutskikh also argued that the co-operation agreements on international information security signed during the most recent BRICS summit and previously by the members of the Shanghai Co-operation Organisation and the Collective Security Treaty Organisation were evidence of Russia's success in this field. This led him to conclude that "Russia has united two-thirds of the world over a shared concept of preventing information wars."[30]

However, a more in-depth analysis of the initiatives in question shows that Russia's efforts were less about international co-operation and more about calling the existing international legal order into question. Instead of promoting co-operation as declared, Russian strategists have been instigating extreme distrust in the United States in an effort to define Russia's position in the new global order and assert the Russian Federation's right to co-decide on global security issues. Such intentions are also evident if one looks at the symbolic layer of the Russian strategic documents, understood as a set of arguments, narratives and stereotypes. Doctrinal constructs such as 'information war', 'information weapons', 'US global dominance' or 'arms race', 'technological parity' and 'demilitarisation of the information space' are hardly a basis for constructive dialogue, as is the entire terminology qualified by the 'information' adjective, which renders it difficult to align the Western and Russian approaches. This language reveals that as Russia escalates its unconstructive actions, it does not actually have any positive programme for co-operation, because such a programme should be built on some shared objectives.

2. The regional level: back to Soviet models?

The current trends in the security environment of the post-Soviet area are unfavourable to Russia, which has to compete for influence in the region with the United States, the EU, China, Turkey, Iran and other actors. Most countries in the region do not consider themselves to be under external military threat, and so calls for unity in the strategic defence area mainly serve Russia's interests.

[30] Евразийские форумы «Инфофорум-Евразия», http://infoforum.ru/main/evraziiskie-fory-my-infoforym-evraziia. It has been reported that the most recent Eurasian Forum was organised by the State Duma Committee on Security and the National Forum of Information Security (Infoforum) with the support of the apparatus of the Russian president's plenipotentiary for international information security, the Security Council of the Russian Federation, the Ministry of the Interior, the FSB, the Ministry of Foreign Affairs, the Collective Security Treaty Organisation, and the administration of Sevastopol and the Republic of Crimea.

Moreover, the CIS area today does not constitute a geopolitical or civilisational community. In the South Caucasus, Russia has been losing its civilisational influence to Turkey, and in Eastern Europe to the European Union. Russia's economic, and also partly its military influence in the entire area has been eroding in favour of China, whose strategic initiatives such as the Silk Road make China an attractive centre of gravity. Yet Russia continues to view control of the region as a hallmark of its status as a world power and a mechanism to impede attempts by the countries in the region to pursue multi-vector policies and integrate with structures that are beyond Moscow's control. This is why all the documents discussed here emphasise the prime importance of Russia's policy towards the CIS and its close military co-operation with regional organisations.

Russia defined the strategic objectives of its policy in the region shortly after the collapse of the Soviet Union. These include:

- preserving the common defence space,
- maintaining a single civilisational and cultural space,
- defending the rights of Russian-speaking people,
- controlling the extraction and transport of energy resources,
- protecting the external borders of the CIS, and
- countering the influence of other states.

In the sphere of defence, the main focus is on:

- maintaining control of former Soviet military installations and retaining a military presence in key locations,
- managing regional conflicts, and
- guaranteeing Russia's monopoly on the possession of nuclear weapons (for its allies, nuclear guarantees are the main argument for military co-operation with the Russian Federation).

This co-operation is organised on multiple platforms: within the CIS, the Collective Security Treaty Organisation and the Shanghai Co-operation Organisation, as well as under bilateral agreements which set up a range of consultation and executive mechanisms that are often redundant (one wonders, for instance, what the purpose is of the Agreement on co-operation in the field of international information security signed with Belarus in 2013, if similar documents have already been signed within the CSTO and the CIS). Apart from military measures (the permitted scope of which Russia unilaterally extended in 2008 and 2014 by claiming the right to use force to protect Russian-speaking people in Georgia and Ukraine), Russia employs a wide range of political and economic measures in the pursuit of its objectives, and the strategic offensive proceeds on many fronts, including the information front.

The Infoforum-Eurasia mentioned above should be seen as one of the initiatives undertaken by Russia to address the **civilisational aspect of the information front**. It is one of Russia's numerous informational platforms for integration in the post-Soviet area, many more of which have been established in recent years. A Centre for Military-Political Studies was set up at the MGIMO in 2012 and runs two online portals on 'Eurasian defence'.[31] A column named New Eurasia has been created in the *National Strategy Issues* quarterly published by the Kremlin's Russian Institute for Strategic Studies (RISI)[32]. In 2013, the eurasiancenter.ru portal was created at the *Rossiya Segodnya* Agency, and in 2015 the Eurasia Daily news agency was founded.[33]

As part of the so-called public-private partnership, these new platforms have been supplemented by a number of 'social' initiatives. The CSTO Institute recently set up the CSTO Analytic Society and the CSTO Youth School.[34] The purpose of the projects is to co-ordinate the activity of researchers, political scientists, experts and leaders of political and social youth organisations from the member states in order to foster a common information policy, lobby for Russia's interests and take part in anti-Western campaigns. Professor Igor Panarin, a noted information war theorist and practitioner, has been appointed the Society's co-ordinator.

[31] http://eurasian-defence.ru/ and http://eurasian-oborona.ru/

[32] http://riss.ru/bookstore/journal/

[33] https://eadaily.com/ru/ These agencies take part in information campaigns and mobilise and discipline the allies. See for instance Лукашенко должен понять, что его единственный союзник — Россия, *Eadaily*, 8.02.2016; https://eadaily.com/ru/news/2016/02/08/lukashenko-dolzhen-ponyat-chto-ego-edinstvennyy-soyuznik-rossiya

[34] The CSTO Institute (http://www.odkb-csto.org/institute/) was set up in 2009 by transforming the Moscow Institute for Integration Studies. Branches were set up at the same time in Kyiv and Yerevan. In Armenia, the conditions for the activity of the branch were appropriate and it continues to function today, while the branch in Kyiv has since closed. The CSTO Analytic Society and the CSTO Youth School are both dominated by Russians. For instance, Kazakhstan is represented in the CSTO Analytic Society by two think-tanks, and Russia by more than twenty. In the Society's closed meeting on 16 December 2015 the allies were represented by experts from Kyrgyzstan and Armenia, and the communiqué issued afterwards suggests that Russian experts (from RISI, MGIMO and the Institute of Oriental Studies of the Russian Academy of Sciences) were overrepresented.

The legal basis for these activities comprises a large number of official documents signed at various points in time, including the **Concept for the Formation of the Commonwealth of Independent States' Information Zone** (1996), the **Concept for cooperation among the participating states of the Commonwealth of Independent States in the sphere of ensuring information security** (2008), and the **Concept for cooperation on combating crimes committed with the use of information technologies** (2013). A multitude of executive mechanisms have been established to implement them, including the CIS Council of News Agency Chiefs, the CIS Association of National News Agencies, the Regional Telecommunications Community, the Information Technology Coordination Council, the CIS Information Security Commission, and others.

The informational and psychological operations in the region are based on the concept of Eurasia, which is a modification of the 'near abroad' doctrine, with Russia as the leader of a centre-periphery integration model. The periphery is treated as a market for uncompetitive products and a strategic foreground in which Russian bases are located. The concept of Eurasia is contrasted with the Euro-Atlantic concept, and the polemic between the two serves to build and maintain tension in domestic and foreign public opinion, while also providing a broader conceptual basis for action, including military action. Regardless of the particular arguments used (the struggle for the national interest and sovereignty of the countries in the region), Russia's aim is invariably to strictly delimit the spheres of influence and responsibility. Since the 'Orange Revolution' in Ukraine in 2003/4, Russia has been exploiting ever more intensively the threats stemming from the 'export of Western democracy', and today it insists on presenting its armed interventions in Crimea and Donbas as a kind of liberation mission aimed at freeing Ukraine from US dominance.

While the Russian integration initiatives are many and varied, they have not been particularly effective, as even the Kremlin's experts admit.[35] It is in this context that one should consider the objective, as formulated in the National Security

[35] See Г. Тищенко, И. Николайчук, Л. Абаев, В. Карякин, Проблемы национальной безопасности России в военно-политической и оборонной сферах: современное состояние. „Доклады РИСИ" in *Проблемы национальной стратегии,* № 6 (33) 2015. In the conclusions of this report, entitled 'Issues of Russia's national security in the political-military and defence spheres. The current situation' the military experts of the Kremlin's Russian Institute for Strategic Studies are pessimistic about Russia's ability to create a 'new' military bloc modelled on NATO and, seeing no potential for deeper military co-operation between Russia and China (within the framework of the Shanghai Co-operation Organisation, which was established for consultation purposes), they suggest more dynamic activity within the CSTO.

Strategy of the Russian Federation (point 90), of "[converting the CSTO] into a universal international organisation capable of confronting regional challenges and military-political and military-strategic threats [...] as well as threats in the information sphere". This provision marks yet another attempt at revitalising the CSTO; the organisation was first given a new identity and the propaganda status of 'the Eastern NATO' in 2002, when the Tashkent Treaty was renamed as the CSTO and officially presented as an organisation capable of countering new threats such as extremism, terrorism, illicit arms trade, illegal migration, and organised drug smuggling. The novelty now is that the catalogue of the CSTO's tasks has been expanded to include countering information threats, and that the body has been given the status of a 'universal organisation' (whatever that may mean).

Yet it is unlikely that the 'new' CSTO will be able to solve the old problems. The allies treat the organisation as an instrument to pursue their specific objectives, which on top of that are often contradictory.[36] The efficacy of military alliances is measured in joint tasks accomplished, and not in the number of agreements signed. Meanwhile, the CSTO has not been able to attract any new members, and Uzbekistan has quit the organisation. The allies are waging a kind of propaganda war among themselves: in November 2015 Belarus suggested that Tajikistan could leave the CSTO, arguing that the Organisation had failed to act on its decision taken in September 2013 to provide military and technical assistance to reinforce Tajikistan's border forces. Apart from some Belarusian equipment and several army surplus vehicles from Armenia, Tajikistan got no assistance, and complained about it on several occasions.[37] Meanwhile the Russian Ministry of Defence continued to claim on various occasions that the Russian bases in Tajikistan and Kyrgyzstan were in constant readiness, and that the Afghan-Tajik border was being reinforced within the CSTO framework. According to the Russian deputy defence minister, General Anatoly Antonov, Russia has been actively supporting the modernisation of its allies' armed forces, training their troops and providing arms and military equipment.[38]

[36] The allies have also sent out mutually contradictory signals. The Belarusian president Alyaksandr Lukashenka, who emphasised in 2011 that the CSTO Collective Response Force could be used to counter coups, is currently highlighting the importance of military co-operation between Belarus and China (see Сергей Острына, Враг у ворот – ОДКБ созерцает и молчит; http://www.belvpo.com/ru/61214.html; Белорусско-китайские заслуги в ликвидации «ЕвроПРО», *РСЗО «Полонез»*, http://www.belvpo.com/ru/52976.html).

[37] http://www.belvpo.com/ru/61214.html

[38] Владимир Богданов, ОДКБ проведет спецоперации по пресечению нелегальной миграции, *Российская Газета,* 5 February 2016; http://www.rg.ru/2016/02/05/strany-odkb-provedut-specoperacii-po-presecheniiu-nelegalnoj-migracii.html

General Nikolai Bordyuzha, secretary-general of the CSTO headquarters in Moscow, has also made frequent statements about strengthening the CSTO's military component. In 2014 he announced the creation of a CSTO Consultation Co-ordination Centre for Responding to Cyber Incidents and a Crisis Response Centre.[39] During the Russian-Ukrainian conflict, Bordyuzha stated several times that CSTO peacekeeping troops were ready to act outside the territory of the CSTO member states, i.e. also in Ukraine. In June 2015 the CSTO Council of Defence Ministers decided to introduce new methods for organising military drills, which would now take the form of unannounced combat-readiness tests modelled on those conducted by Russia.

Meanwhile, it has been announced that work is underway to create a CIS cybersecurity centre (there is no information as yet about its name, function or the division of competences among its individual members). As usual, Moscow presents this initiative as a manifestation of its altruistic assistance to its allies; however, there are many indications that the projected centre will follow the tried and tested patterns of the past, of which Russia's failed strategic initiative to stop the degradation of the former USSR Combined Air Defence System may serve as an example. That project was undertaken within the CIS in 1992, but not all states were interested in the specific undertakings as they believed that rebuilding the system, and especially its missile attack early-warning capacity, would mainly serve the interests of Russia. As a result, Moscow was forced to build regional air defence systems within the CSTO. In order to sustain and expand the system, Russia had to equip Kazakhstan, Armenia and Belarus with state-of-the-art S-300 systems (even though it generally does not provide modern weapons to its allies, preferring to deploy its own equipment and troops on the allies' territories, thus deepening the asymmetry of relations).

[39] http://redstar.ru/index.php/nekrolog/item/26173-odkb-gotova-k-lyubym-vyzovam. The CSTO centre being set up by the Russian Ministry of Defence is to be integrated with the Russian Federation's defence management system, according to a statement by Vladimir Putin that was reported accurately, although somewhat awkwardly from the propaganda point of view, by Sputnik.pl: "In Russia a new National Centre for the Management of Defence of the Russian Federation has been opened. It is based entirely on Russian technology and state-of-the-art software which as yet has no equivalent in the world. Today the secretary of our organisation said that all the CSTO countries would be involved in the operation of the Centre. I am convinced that this will make the national defence systems more manageable by our military, and improve the co-ordination of our work", Putin said at a meeting of the CSTO Collective Security Council (http://pl.sputniknews.com/polish.ruvr.ru/2014_12_23/Kraje-OUBZ-wezma-udzial-w-pracy-narodowego-centrum-zarzadzania-obrona-FR-5017).

While Russia needs to strengthen its capacity of information and psychological impact to conduct its anti-US and anti-NATO campaigns and to sustain the integration processes (it never misses an opportunity to remind the allies of impending information threats and the need to repulse information aggression), the projected cybersecurity centres should be regarded mainly in economic terms. The countries in the region, especially Azerbaijan and Kazakhstan, are an important market for Russian arms and military equipment, and for IT, telecom and communication services, also for the military. The internet and new telecom technologies represent a lucrative domain and a constantly growing market. Needless to say, it is Russia which defines the shape of the regional cybersecurity and cyberdefence projects. To this end, Russia has set up a system of so-called base organisations. The All-Russian Research Institute for Computational and Information Technology Issues has been granted the status of the CIS countries' base organisation in charge of providing methodology, training and organisational services for the implementation of IT technology.[40] A training facility for CSTO specialists in cybersecurity and psychological warfare has been created within Russia's MIFI.[41] Using its military advantage, Russia has been building a single cyberspace in the region, while at the same time strengthening its instruments for political, economic and technological domination in the CIS area.

Time is putting the Russian strategic initiatives to a test. Russia continues to implement the economic, civilisational, cultural, political and military measures in the countries of the region, subordinating them to its own interests, even though the results have been disappointing, and some of the measures have turned out to be counterproductive. Russia's partners in the CSTO were shocked by its policy towards Ukraine. Despite this, the CSTO state leaders have continued to sign joint declarations, but at the same time none of them have recognised the sovereignty of the self-proclaimed states of South Ossetia and Abkhazia, which Russia counts among its allies in its latest documents (the 2014 Military Doctrine and the 2015 National Security Strategy). None of the CSTO members supported the annexation of Crimea or the Russian intervention in Donbas.

[40] Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации» (ФГУП ВНИИПВТИ) in Russian. See www.pvti.ru

[41] MIFI (the Moscow Engineering and Physics Institute) is the transformed research institute of the Russian arms industry. In 2011 an Information Security Chair was established within its Faculty of Cybernetics. It offers four specialisations: computer system protection technologies, critical infrastructure management systems, security of automated management systems and information security analytics.

Neither have the allies joined Russia's sanctions against Turkey and Ukraine. They did not condemn Turkey after the shooting down of the Russian Su-24 on the Turkish-Syrian border in November 2015. Contrary to claims of a possible allied intervention mandated by the UN in September 2015, the CSTO's position on the Russian intervention in Syria, adopted on 21 December 2015, was limited to condemning terrorism and supporting the UN Security Council resolution calling for a political resolution of the conflict. The CSTO declaration resembled the familiar Soviet newspeak: the allies noted "rising tensions in the Eurasian space, the CSTO's sphere of responsibility" and pledged to "strengthen the organisation's military potential and continue co-operating in the fight against terrorism at the political level and at the levels of security services, ministries and departments".

3. The national level: military organisation of society

While the results of Russia's military information strategy at the international and regional levels are unimpressive, the strategy has clearly been a success internally in Russia. Its long- and short-term objectives are convergent, and are also in line with the Kremlin's aim of mobilising and consolidating the public in support of the regime, an intention that is clearly visible in statements such as Vladimir Putin's words of thanks to the Russian army for "defending Russia's interests in Syria", which the President expressed on the occasion of Defenders of the Fatherland Day on 21 February 2016, once again implying there is a 'Western conspiracy against the interests of Russia'.

The success of the militarist propaganda is also reflected in public opinion polls, in which the numbers of respondents declaring negative attitudes towards the West are soaring. The Russians consider the United States to be the main potential enemy of Russia: this opinion has been expressed by 53% of respondents in a poll by VCIOM conducted in October 2015 (compared to 19% in 1990). 48% of respondents fear a military attack on Russia (13% in 1990). Views of the army's combat capabilities have also changed; today one in three persons in Russia believe that the Russian army is the best in the world, and 49% think it is one of the best (21% in 1990).

Interestingly, these trends were even more pronounced in a February 2016 poll by the Levada Centre, which is considered to be an independent polling institution. Two-thirds of respondents in that survey (65%) believe that Russia faces a real military threat, and a massive majority (81%) are convinced that the army would be able to protect them in case this threat materialised. A growing proportion of Russians (according to the same Levada poll) are in favour of maintaining universal conscription (58% in 2016 compared to 40% in 2014).

This situation is the outcome of many years of systemic action, especially the programme for training information security specialists launched in 2000 and the large-scale programme named 'Patriotic education of the Russian Federation's citizens' which has been in place since 2001. The latter initiative is coordinated by the Russian Military Historical Centre,[42] a Russian government agency led by Admiral Vyacheslav Fetisov. Initially its main focus was on military historical policy, as the Centre sought to highlight the combat traditions and the heroic deeds of the Russian army and demystify Russia's military history (which they alleged had been distorted by some Russian historians and the West), while also supporting veterans and preserving monuments and memorial sites commemorating soldiers fallen defending the homeland. However, the current, third edition of the programme for the years 2016–2020[43] focuses on cooperation between the army and the public, as well as the military and patriotic education of children and young people. The programme is being implemented by the Ministries of Defence, Education, Culture and Sports, with the support of many other government bodies including the Ministry of Foreign Affairs, the Ministry of Emergency Situations, the Federal Security Service, the Federal Drug Control Service, the Federal Penitentiary Service and the Agency for Youth Affairs and others, as well as social organisations such as the Volunteer Society for Cooperation with the Army, Aviation, and Fleet (DOSAAF), the All-Russian Organisation for Veterans of War, Labour, Armed Forces and Law Enforcement Agencies, All-Russian Public Organisation of Disabled Veterans of Afghanistan, the Russian Union of Veterans, the Merit-Code-Memory-Honour Foundation of Military Graduates, the Russian Union of Youth, and the Inter-Regional Youth World Foundation, and religious organisations (mainly the Moscow Patriarchate) and other actors. Local administration bodies mandatorily participate in the programme's implementation, having set up separate structures in charge of the patriotic, military and civil education of young people.

The projects scheduled for the years 2016–2020 usually follow the tried formulas of earlier undertakings: apart from the monitoring and efficacy assessments of regional programmes, they are focused on setting up patriotic clubs

[42] Росвоенцентр in Russian.

[43] Мероприятия по реализации государственной программы «Патриотическое воспитание граждан Российской Федерации на 2016-2020 годы», http://www.rosvoencentr-rf.ru/obobshchennye-doklady/gosprogramma-pvg-rf-2016-2020/meropriyatiya-po-realizatsii.php

and associations within education, culture and sports institutions.[44] Within the framework of the programme, methodology recommendations and teaching aids (such as 'Heroes of the Russian Soil' or 'The History of the Homeland in the Songs of the Alexandrov Choir') are developed, and regional conferences on 'Patriotism as the Unifying Idea of Russia in the Twenty-first Century' are organised. One of the stated objectives is to ensure mass participation by young people in the celebrations of the 75th anniversary of the end of the 'Great Patriotic War' in 2020. The young generation has been assigned a symbolic role as the 'guardians of memory', 'continuators of the historic mission of victory', and 'heirs to the common victory of the nations of Russia' (runs, outdoor games, seminars and round-table discussions will be held under such slogans in 2020). The programme also follows the established customs of organised tours to sites related to the 'liberating mission of the Russian Empire's army, the Red Army and the Soviet Army' at various historical junctures and the 'restoration of the memory of those fallen in the years 1941–1945 during the liberation of Crimea and Sevastopol as well as Poland and Germany'.

The Academy of Military Sciences (AVN) is one of the main actors in charge of the military segment of the information system.[45] Contrary to what the name suggests, it is not an academic institution: it was established by Boris Yeltsin's decree of 1995 as a 'centre of independent defence research' and has since been chaired by General Makhmut Gareyev.[46] Its founding bodies included the Russian Institute of Strategic Studies (which at that time operated as part of the Foreign Intelligence Service), the Committee of Researchers for Global Security, the League to Support Defence Industry Enterprises, the Russian Union of Industrialists and Entrepreneurs, the Centre for International and Military-Strategic Studies, the Foundation for Social-Economic and Political Research, and others. In the first half of the 1990s the Academy took in staff members from disbanded research and science institutions and military political and technology experts who had been moved to the reserves. Today this prestigious name stands for an association of think tanks and research institutions of the armed

[44] This year the trend has gained momentum, with the establishment under the patronage of the Ministry of Defence of an all-Russian movement called 'Young Army' (the first 'Young Army' clubs were set up in 2008 at the initiative of teachers of 'basic security in life activities'). See for instance, Минобороны создает молодежную организацию „Юнармия", *Коммерсант*, 5 April 2016, http://www.kommersant.ru/doc/2956367

[45] www.avnrf.ru/

[46] Gareyev is 93 years old and, as his biographic notes often emphasise, has been awarded 18 military orders and 27 medals; as the deputy chief of the General Staff of the Soviet Union's Armed Forces he was one of the authors of the **Defence Concept of the Warsaw Pact** in 1987.

forces, the Ministry of the Interior, the Border Service, the FSB, the Ministry of Emergency Situations, as well as civilian experts and journalists specialising in defence topics.

The Academy conducts research, conceptual and methodology work as well as organisational activities: it has been building up its capacity to implement the military information measures and carry out systemic projects. The results of the research carried out by the Academy members are published in the quarterly *Vestnik AVN,*[47] available at the Academy's official portal. Its flagship social and educational project include the Academy of Information Self-Defence,[48] which has been issuing the *Information Wars* quarterly since 2008[49] and participating in the state programme of patriotic education by organising an annual military and historical visual arts contest for children and young people, running the Alpha military and sports youth centre (which promotes martial arts), organising mass events (such as '*Спасибо деду за победу*': "Thanks to grandpa for the victory") and drafting schoolbooks for the subject 'Basic security in life activities' for grades 5 to 11 (the subject is an equivalent of civil defence plus survival skills, camouflage, basic geopolitics and worldview formation).[50] The objective of all these projects has been to promote the ideas of patriotism and pride in the Russian army, instil a commitment to defending the homeland, develop interest in defence, and foster 'counterintelligence attitudes' among the public.

The Academy closely co-operates with the Ministry of Defence and the General Staff of the Russian Armed Forces (its presidium and the editorial office of *Vestnik AVN* are headquartered in the offices of the Chair of Military History of the Military Academy of the General Staff, Universitetsky Prospekt 14 in Moscow). The symbiosis between the active and retired segments of the military information system is visible in their regular contacts and the fact that they speak with one voice. Take for instance the lecture by the Chief of Staff, General Valery Gerasimov, during the annual meeting of the Academy members in late February 2016. Speaking about 'new' military threats to Russia, the general

[47] http://www.avnrf.ru/index.php/zhurnal-qvoennyj-vestnikq/arkhiv-nomerov?layout=blog

[48] The institution self-defines as a "social, voluntary association of specialists researching the impact of information on the human mind and the techniques and methods of information self-defence".

[49] http://www.iwars.su/

[50] The subject 'Basic security in life activities' was introduced into the general education curriculum under the Law on education in the Russian Federation of 29 December 2012. It includes both classroom lessons and out-of-school activities such as rescue training at centres of the Ministry of Emergency Situations and the Ministry of Defence.

mentioned the so-called 'colour movements' and the negative impact of external information on the minds of people in Russia, which in his view destroy the nation's historical, spiritual and patriotic defence traditions. He called on military researchers to reflect more deeply and propose new ideas about the strategic directions of the Armed Forces' activities in outer space and in the information sphere, taking into account the operational experiences in Ukraine and Syria.[51]

Speaking about the need to equip the army adequately for the information wars, he reiterated the strategic objectives signalled in point 46 of the Military Doctrine of December 2014, emphasising the importance of channels to exchange information with other bodies and services, and of close co-operation among the military formations operating under the different government departments, as well as the military and non-military components of territorial defence in the event of a crisis situation. Highlighting the importance of the National Defence Centre in this context, he emphasised the need to enhance the information management systems and integrate them with the automated control systems at the strategic, operational and tactical levels.

The Academy's activities lift some of the financial burdens from the defence budget. The projects it implements are mainly financed by arms industry companies, as well as the Security Council, the Federation Council, the State Duma and individual government departments which award the AVN contracts for research, expert and executive projects. The quarterlies published by the academy are financed by the Military Insurance Society, and the Suvorov and Svechin prizes for young researchers – by the 'Science-21st Century' Foundation for National Security Research, which also partners with the AVN in the implementation of the 'Army and Society' project.[52] The sponsors, donors and patrons of these projects are invited to join the AVN as honorary members. According to its 2015 activities report, the Academy currently has 839 real members, 432 correspondent-members and 91 honorary members (of which 30% are active officers and 70% reserve and retired generals and researchers). The system of titles used by the Academy members, which resembles the titles used within the Russian Academy of Sciences, is intended to emphasise the social prestige of this gathering of Russian military researchers (in order to join the Academy, one needs to be a national of the Russian Federation or another state [which in practice means Belarus, as there is a Regional Branch of the AVN in Belarus],

[51] See the text of the address at Валерий Герасимов, По опыту Сирии, *Военно-промышленный Курьер*, 9 March 2016, http://www.vpk-news.ru/articles/29579

[52] http://www.arm-ob.ru/

be over 18 years old and hold a PhD title (кандидат наук)). The lecturers title themselves 'professors of the Academy of Military Sciences'.

The stated purpose of this kind of projects and undertakings is to pool the efforts of the government, the society and the army with a view to shaping a system of civilisational values, in which the history and tradition of the Russian army's victories would play an important role. The ultimate objective is to boost the prestige of and respect for military service, and eliminate the negative tendencies that emerged from the ideological and spiritual vacuum of the 1990s, leading to a weakening of the foundations of the Russian state. The revival of the state, announced at the beginning of Vladimir Putin's first term as president, and the programmes launched at that time (including the programme of military patriotic education) were intended to deliver a cohesive state system and foster a strong identification with the state built on a particular vision of common history and shared civilisational values, imposed from above (because like the USSR, Russia is a multi-nationality and multi-cultural state, and one can hardly speak of a community of origins or common cultural heritage in its case; nor can the history of the nations of Russia serve as a connecting factor). This approach has not encountered any major psychological or mentality barriers. While in the 1990s the public was outraged at the pathologies in the Russian army (the so-called *дедовщина* or hazing; ethnic cleansing during the operations in Chechnya, plundering and violence against civilians), today it admires the 'patriots of Crimea', the 'little green men' or 'polite people', Russian weapons and the successes of the operation in Syria, and gladly participates in mass events serving the purposes of militarist propaganda. On such occasions, it manifests its pro-state patriotism and pride in the all-powerful, centralised state and its leader.

The strengthening of the state's military structures and its potential for mobilisation has been accompanied by a process of organising society according to a military logic, which continues today. It is an extensive process, managed from the top, and is intended to yield results in the long term, as evidenced by the fact that it includes projects addressed to children. The art and song contests organised to mark the 70th anniversary of victory in 2015 involved the participation of children from the 5- to 7-year age bracket, and the Voyentorg chain of army stores has recently expanded its range to include 'militarised' teddy bears (tank driver, airman, marine, etc.). Underlying this kind of military-educational undertakings is the myth of the invincible Russian army. The omnipresence of military symbols and the 'khaki patriotism' have already accomplished the militarisation of the people's minds in Russia. This, in turn, demonstrates that the concept of the army's activities in the information space is not only about blurring the divide between war and peace and close co-operation between the military and non-military segments of the system, but also about legitimising Putin's regime. In the Armed Forces' narrative, an attack on the regime constitutes a military threat because it undermines the very existence of Russia as a cohesive, internally homogenous political, economic, social and information space. This vision or perception of the world and the external military threats is construed from the point of view of the Kremlin's interests. In this regard, the short- and long-term strategic objectives of the Kremlin and the military are aligned. It is also clear that power in Russia is founded primarily on force, and that efforts to consolidate the public around the Kremlin always rely on the use of the concept of an enemy who is invariably defeated by the Russian army. Thus, it should come as no surprise that the toys on offer at Voyentorg include a *judoka* teddy bear and a hockey-player teddy bear, alongside the airman teddy bear and the teddy bear on an Arctic mission.[53] It is through this kind of accessible propaganda that the image of the Armed Forces' commander and the guarantor of the stability of Russia's regime is promoted among the youngest Russians.

[53] http://rusnews2015.ru/mishki-nanosyat-otvetnyj-udar/

IV. CONCLUSION: THE ARMY IN THE SERVICE OF POLITICS

The activities of the Armed Forces of the Russian Federation in the information space are subordinated to Russia's wider, long-term information security strategy. The army thus performs strictly military (non-public) functions alongside non-military, public tasks: in keeping with the Russian strategic culture, the factor of force serves to justify Russia's status as a global power and the internal and external policies of its leadership. Seeking to build a multi-polar world, the Kremlin has been exploiting this approach in order to maintain and expand its influence in its immediate neighbourhood and beyond. The US army and its NATO allies are the main point of reference here and are seen as the Russian army's main enemy. The military information policy seeks to highlight the capabilities of the Russian Armed Forces, while at the same time undercutting the positions of its potential opponents.

An analysis of the Russian strategic documents, taking into account the involvement of the army in the pursuit of political-military objectives, leads to the conclusion that the Russian strategists' views on the question of the use of force have been evolving towards more radical positions. The functions of nuclear deterrence, which initially served to prevent a nuclear attack, have been expanded to include the prevention of a conventional attack and (most recently) an information attack (as defined in Russian terminology). The expanded scope of psychological deterrence stems from the need to step up pressure on the potential aggressors and allies in Russia's immediate neighbourhood. This is the purpose of the adjustments made in successive editions of Russia's doctrines, which serve to spread fear and deepen distrust of the West.

The significance of information deterrence (and more broadly, of the military factor) will increase. Apart from the use of force and diplomacy (one of the main instruments in information wars) Russia does not have many powerful arguments in international politics. These two constitute the main pillar of Russia's status as a regional power. As it gradually loses its global influence, Russia will use all means and measures at its disposal to stop this process. At this stage, it has the potential for destruction, which it has been concealing by emphasising its aspiration to preserve a global balance of power and ensure parity in various spheres, including 'information parity'.

To conclude, it is worth noting that the objectives of the Russian Armed Forces' information activities at the strategic level have been defined in a very general way. They include measures to develop cyberpower, cyberdefence and cyberoffence. A full recognition of these objectives requires not only a thorough knowledge of the decision-making processes in Russia, but also knowledge of the Russian state's technological and organisational capabilities.

At the operational level, the implementation of these objectives will involve co-ordinating the activities of various actors in charge of different tasks. An analysis of those activities shows that the Russians have not been particularly inventive, invariably relying on the same tried and tested methods. And those methods, which are perfectly comprehensible to the countries of the region, are also increasingly well recognised in the West.

APPENDIX 1

List of source documents

Military Doctrine of the Russian Federation, 2014 (http://rusemb.org.uk/press/2029)

Information Security Doctrine of the Russian Federation, 2000 (http://www.scrf.gov.ru/documents/6/5.html)

Draft Information Security Doctrine of the Russian Federation, 2015 (http://infosystems.ru/assets/files/files/doktrina_IB.pdf)

National Security Strategy of the Russian Federation to 2020, 2015 (http://www.scrf.gov.ru/documents/99.html)

Basic principles for the Russian Federation's state policy in the field of international information security to 2020, 2013 (http://www.scrf.gov.ru/documents/6/114.html; unofficial English translation at https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf)

Russian Federation Armed Forces' Information Space Activities Concept (http://function.mil.ru/news_page/country/more.htm?id=10845074@cmsArticle)

Fragment of the Concept paper on the state system for monitoring, preventing and eliminating the consequences of computer attacks against the information resources of the Russian Federation (http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf)

APPENDIX 2

Russian Federation Armed Forces' Information Space Activities Concept: an overview

Published in 2012, the Russian Federation Armed Forces' Information Space Activities Concept is the only strategic ministerial document that has been made public. The military vision presented therein, which on the one hand emphasises a systemic approach to the security and defence of the Russian Federation's information space, and on the other highlights the global reach of information actions, does not significantly differ from the vision discussed in Part I of this paper. The document also serves the purposes of the specific kind of political-military marketing, clearly intended to produce a positive reaction at home and abroad (it has been published in both Russian and English).

The document consists of four parts:

1. basic terms and definitions,
2. principles,
3. rules,
4. confidence-building measures.

The document opens with an Introduction and closes with a Conclusion. Its preamble states that the information space is a new theatre of military operations (alongside the land, sea, air and outer space): "The fast development of various information systems, Internet-like computer networks and electronic mass media has led, at the turn of the millennium, to the creation of the new global information space. Along with the land, sea, air and outer space, the information space has been extensively used for a wide range of military tasks in the armies of the most developed countries." The definition of information space emphasises the impact that information has on individual and group awareness. Apart from psychological operations, the military activities in the information sphere include the technical aspect (equipment, hardware, software). In several instances, the document emphasises that the information space is integrated with the security and defence sphere ("Armed Forces cyberspace activities imply the use of military information resources to solve defence and security problems").

In the glossary of basic terms and definitions in part 1, the Defence Department identifies the Armed Forces as part of the information security potential of Russia, and defines the information security of the Armed Forces themselves as "the security of the information resources of the Armed Forces against attack using information weapons". The military definition of information war remains deeply embedded in the classic paradigm of war: "**the confrontation between two or more states** in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilise the state and society, as well as the coercion of the state to take decisions for the benefit of the opposing force." It omits the role of non-state combatants in information wars, but very clearly links the technical and psychological aspects of information war. The objective of an information attack is to destabilise the political, economic and social system of another state, and the targets include the state administration bodies, telecommunication systems and infrastructure, the public (including both civilians and troops), and the mass media (especially the electronic mass media). The information weapons used for this purpose ("information technologies, means and methods used to conduct the information warfare") are of a dual nature, addressing both the technological and the psychological aspects of information.

Part 2. (Principles) is the largest section of the document; it lays down the principles which guide the Armed Forces' activities in the information space. These include legitimacy, priority for information activities, complexity (the use of all available assets by the Armed Forces), interaction (co-operation) within the information security system of the Russian Federation, regional and global co-operation, and innovation. While the principles of legitimacy and international co-operation, especially at the regional level, are a constant element in all Russian strategic documents, serving to demonstrate the peaceful and defensive intentions of the Russian state and to emphasise that Russia has many allies who share its approach, the other three principles deserve a more careful analysis, because they reveal the mechanics of the military information warfare operations. Take for instance the **principle of priority for information** activities, in accordance with which the army has an obligation to seek as a matter of priority to collect relevant and reliable information on the threats, to process it rapidly, analyse it profoundly and develop protective measures in a timely manner. The document reads: "the need for adoption of such measures on a priority basis in the current context is due to (but not limited to) the fact that hundreds of millions of people (whole countries and continents) are involved in a single global information space formed by the Internet, electronic mass media and mobile communication systems".

The underlying assumptions that:

(1) today's world is one of information war;
(2) that war leads to catastrophic consequences;
(3) neutralising this threat requires the Russian Armed Forces to act globally;

are in keeping with the doctrinal perception of threats and the intention to respond to them using all available forces and means.

The principle of complexity, on the other hand, offers an insight into the nature and scale of operations. The document reads: "Operations in the information space are comprised of the staff and field intelligence efforts, operational deception, electronic warfare, communications, code and automated C2, information work of HQs, as well as protecting friendly information systems against electronic, cyber and other threats. [...] Commanders and staffs at all levels are directly involved in organising information space activity in peacetime, in wartime, in the preparation and execution phases of operations (warfare). Each of these command structures, with regard to their functions and authority, plans the subordinate troop activities linked by a single concept of action in the information space." Through this language, the Russian defence department confirms that the operations in both peacetime and wartime are planned and executed as part of a single concept. They include defensive and offensive activities, and passive and active measures, including special operations requiring camouflage. Possible operations also include electronic warfare (distortion, disabling communication channels) and computer attacks.

The principle of interaction requires that the department of defence co-ordinate its information space activities with the other federal executive organs (a euphemism standing primarily for the secret services). The interaction, as the document emphasises, takes place within the information security system of the Russian Federation under the 2000 Information Security Doctrine of the Russian Federation. Interoperability between the different services and bodies is also required under **the principle of innovation**, which provides that activities in the information space and training activities should rely on cutting-edge technologies and techniques, and that highly skilled staff should be involved in tackling the challenges of information security. "For this reason, the scientific and production potential of the leading Russian innovation centres can be applied to design and produce such means and technologies, and the design should be carried out in the framework of national and departmental programs and R&D." The document also states that information security specialists should be trained at the higher education institutions of the Ministry of Defence, although "in addition, specialists who have graduated from other educational institutions could legally be involved". The principles of complexity and co-operation stem from the systemic approach to information security, which requires the co-ordination of the activities of all the departments in charge of security in Russia, their resources, methods and modes of action, and calls on the individual actors to build up their capacity to work in a co-ordinated way.

Part 3. (Rules) deals with conflict deterrence, prevention and resolution. The rules are no different from the general rules of military policy as laid down in the Military Doctrine of the Russian Federation, which the document quotes ("The military policy of Russia is aimed at preventing an arms race, deterring and preventing military conflicts"). To this end, the document recommends that the actors concerned develop the information security system of the Russian Armed Forces; keep information security means and forces in constant readiness; use all available means for early detection of potential military conflicts in the cyberspace, and unmask the masterminds, instigators and accomplices; carefully analyse conflict causes and escalation factors; and **manage (exercise control of) conflicts** in order to prevent emergency situations. Of particular note is the last point (10) which establishes a rule to "explain a conflict's causes and background to the world community impartially, publicly and in proper time" and to shape public opinion through "appropriate orientation and mobilisation, [and make] it possible to create a climate in the global information space that will restrict options for escalation on the part of its masterminds". The provisions on conflict resolution clearly refer to the text of the US Strategy for Operating in Cyberspace: if conciliatory measures, referral to the UN Security Council and other non-violent means fail, Russia reserves the right to enforce its right to individual or collective self-defence using all available military means. The influence of US cyberstrategy is also visible in the provisions on the implementation of the conflict management concept, which recognise the information space as a theatre of operations, as well as in the innovation principle.

The deterrence strategy laid down in the document envisages the application of all necessary means (political, economic, diplomatic, information) needed for Russia to exert its pressure. In the sphere of information, this involves providing counter-information to the public opinion at different levels, including globally. To this end, the document stresses the need to develop 'information infrastructure' in foreign territory: "In the interest of individual and collective self-defence, to deploy necessary information security assets on the territory of foreign states in pursuance of the freewill agreements; (...) During the conflict, to inform at all times the domestic and foreign mass media about the development of the situation and promote conflict de-escalation and the consolidation of results with regard to the public opinion". Two points in this section emphasise the priority on co-operation in strengthening international information security, especially at the regional level within the framework of the Collective Security Treaty Organisation (comprising Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia and Tajikistan), the Commonwealth of Independent States (CIS), the Shanghai Co-operation Organisation (comprising China, Kazakhstan, Kyrgyzstan, Russia and Uzbekistan) and on efforts at the United Nations towards the adoption of a universally recognised code of international legal norms and principles applicable to the information space. In the practical dimension, such norms and principles would serve several strategic objectives, including military deterrence, the ability to project power, establishing an information-aggression 'immune system', information conflict management, and maintaining the constant readiness of the information warfare forces and means.

Part 4. (Confidence-building measures) is the shortest section of the document, and comes with a declaration to the effect that while conducting operations in the information space, the Armed Forces will strive to develop confidence-building measures. These include:

"1. The exchange of national information space security concepts,

2. Intensive exchanges of information on crises and threats in the information space, on measures taken with a view of their settlement and counteraction, and

3. Consultations on the information space issues that could invoke concern from the parties, and cooperation in military conflict management".

The **conclusion** emphasises that: "the Armed Forces of the Russian Federation will strive for the maximum exploitation of the information space potential in order to strengthen the defensive capacity of this country, to contain and prevent military conflicts, to develop military cooperation and shape an international information security system for the sake of the world community".