War by non-military means

Understanding Russian information warfare

Ulrik Franke

FOI-R--4065--SE

March 2015

Ulrik Franke

War by non-military means

Understanding Russian information warfare

Bild/Cover: AP Photo/ Misha Japaridze

Titel	Krig med icke-militära medel: Att förstå rysk informationskrigföring
Title	War by non-military means: Understanding Russian information warfare
Rapportnr/Report no	FOI-R--4065--SE
Månad/Month	Mars/March
Utgivningsår/Year	2015
Antal sidor/Pages	60
ISSN	1650-1942
Kund/Customer	Försvarsdepartementet/ Ministry of Defence
Forskningsområde	8. Säkerhetspolitik
FoT-område	
Projektnr/Project no	A15101
Godkänd av/Approved by	Maria Lignell Jakobsson
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Rapporten utgör främst en genomgång av ryska officiella dokument och rysk militärteoretisk litteratur avseende informationskrigföring. Den rymmer också några fallstudier, i syfte att belysa hur teorin omsätts i praktik. En slutsats är att informationskrigföring inte bara ses som en fråga för de väpnade styrkorna, utan snarare som en strategisk verksamhet som kräver samordning av många myndigheter. En annan slutsats är att informationskrigföringen enligt doktrin och teori bedrivs kontinuerligt i såväl fred som i krig. Informationskrigföringen är politiserad och de ryska intellektuella som deltar i den militärteoretiska debatten ansluter sig nu till en syn på informationskrigföring där regimsäkerhet är det överordnade målet. Bland drivkrafterna återfinns en syn på världen som ett nollsummespel, där globaliseringen försämrar Rysslands säkerhet och där Ryssland släpar efter västerländska länder avseende teknik.

Nyckelord: Ryssland, informationsoperationer, informationskrigföring, påverkansoperationer, telekrig, cyberkrigföring, strategi, operationskonst

Summary

This report is first and foremost a review of Russian official documents and Russian literature on military theory with regard to information warfare. It also offers a few case studies, to shed light on how the theory is applied in practice. One conclusion is that information warfare is not considered to be just a matter for the Armed Forces, but rather a strategic matter that requires the coordination of many government agencies. Another conclusion is that information warfare, according to doctrine and theory, is conducted continuously in peacetime and wartime alike. Information warfare is also highly politicised, and the Russian intellectuals taking part in the military theory debate now embrace a view of information warfare where regime security is paramount. Among the driving forces for this is a view of the world as a zero-sum game, where globalisation is reducing Russian security, and where Russia lags behind Western countries in terms of technology.

Keywords: Russia, information warfare, information operations, influence operations, electronic warfare, cyber warfare, strategy, operational art

Preface

This report was produced within the framework of the Russia Studies Programme (Russian Foreign, Defence and Security Policy, RUFS) at the Swedish Defence Research Agency (FOI), which provides analyses for the Swedish Ministry of Defence. It is also a continuation of a collaboration that was initiated with the project National Security in the Information Society, which aimed to explore the relationship between politics and information technology in different countries and regions.

The report has benefited from the comments of Keir Giles, who acted as opponent at a public seminar on December 15, 2014. Gudrun Persson, who chaired the seminar, also offered a number of very useful remarks that substantially improved the manuscript. A preliminary draft was also presented at a discussion seminar on hybrid warfare arranged by the International Centre for Defence and Security (ICDS) in Tallinn on November 24, 2014.

Carolina Vendil Pallin

The Russia Studies Programme at FOI

18 February 2015

Table of contents

1 Introduction

In the Russian view of modern war, information warfare is given a lot of weight. Not least recent events in Ukraine have sparked a renewed interest in these aspects. This report aims to explore the intellectual foundations and practical use of information warfare as seen by Russian military theorists and expressed in official doctrine and documents, as well as by examining a handful of case studies.

Why is this important? Because information warfare is rapidly becoming an integral part of modern conflicts. The modern, increasingly digital, media landscape and the rapid development of information and communication technologies have created a new playing field. This needs to be understood by everyone – political decision makers, military officers, and the public alike.

Information warfare is about achieving goals that used to require serious military force and a lot of bloodshed, e.g. annexing a part of another country, by other means. Victory and defeat take place in the minds of the belligerents. Sometimes a message needs to be hammered home by destroying military hardware, civilian infrastructure and innocent life – but sometimes just the message, if cleverly crafted and credibly supported, is enough. The traditional military component need not be removed, but it can take on another role. The illegal annexation of Crimea is an excellent example.

This report does not aim to cover the field of Russian information warfare exhaustively. The aim is more modest: to serve as a foundation and an intellectual tool for further analysis. By focusing on recent developments in Russian official documents and theory of information war, it is hoped that the reader will gain an understanding of its intellectual underpinnings. These, in turn, can be a potent framework for understanding the concrete actions and measures taken. To the untrained eye, traditional military operations look like a bunch of vehicles and people in uniforms moving around. However, to the properly trained observer, seemingly scant observations of tanks, artillery and armoured personnel carriers can not only reveal the bigger picture of what is going on at the moment, but even form the basis of a projection of what will probably happen in the near future. In much the same way, this report is intended to be an aid for seeing the wood rather than the individual trees of Russian information warfare.

The main part of the report, therefore, focuses on describing information warfare as expressed in Russian official documents and military theory. In terms of official documents, its coverage should be reasonably comprehensive. In terms of military theory, coverage is more limited, and is mostly based on *Voennaia mysl*, the official military theory journal of the Ministry of Defence. A more thorough study of other sources would be welcome future work. Following this theory part, a few case studies and reflections are offered on how this intellectual framework can help us understand the practice. These examples are meant to be suggestive, not exhaustive.

1.1 A note on terminology

There is a plethora of terms on information warfare. In English, concepts such as information operations, command and control warfare, psychological operations, information security, cyberpower, influence operations, electronic warfare, military deception, cybersecurity, strategic communication, public diplomacy, cyber espionage, cyberwar etc. abound. To the professional, some of them have precise and well-defined meanings, some of them have become *non grata*, and some are just vague. (For a thought-provoking analysis of the problematic introduction of the “strategic communication” concept in NATO, see Johnsson, 2011.) To the layman, the intricacies of these terms are even less transparent.

In Russian, much the same is true. Many different terms are used, sometimes in purportedly precise ways, more often not. The translations in the report are those of the author, and could undoubtedly be further improved. However, to be as transparent as possible, and to try and avoid misunderstandings, this report often gives original Russian (transliterated) terms within brackets. Unfortunately, “official” English translations are for the most part lacking. A good exception is the joint initiative of the EastWest Institute and the Information Security Institute at the Moscow State University to sort out and align English and Russian cyber terminology (Godwin III et al., 2014).

The phrase “information warfare”, used in the title and throughout the report as the catch-all term of choice, has been deliberately chosen as a straightforward translation of the Russian “informatsionnoe protivoborstvo” (most commonly used) and “informatsionnaia voina” concepts. “Information warfare” is also a term used by other recent English-language studies on the subject, e.g. Thomas, 2014, or Darczewska, 2014. Furthermore, since it is nowadays rarely used within the US, NATO, or Sweden, it has a suitably foreign ring, reminding the reader that the subject is Russian information warfare. (Reserving different terms for different countries might seem uneconomical, but is actually the practice in other areas as well, e.g. when we speak of Western mechanised but Russian motorised infantry [motostrelkovyi], although the units are similar.)

For an interesting account of how Russian cyber terminology differs from Western usage, see Giles and Hagestad (2013).

2 Information warfare in Russian official documents

The following sections shed light on Russian concepts and views related to information war from several complementary perspectives, starting with government and military official documents.

The national security strategy is the most important official document. Indeed, its § 4 defines it as the very foundation of the national security system. Other important official documents such as the military doctrine are developed under the auspices of the National Security Council, which coordinates the large number of government agencies involved. The National Security Council itself is a powerful institution, chaired by the president. Its 13 permanent members, including the prime minister, the minister of defence, the minister for foreign affairs, and the heads of the security service the Federal Security Service (Federalnaia sluzhba bezopasnosti, FSB) and the Foreign Intelligence Service (Sluzhba vneshnei razedki Rossiiskoi Federatsii, SVR) meet on a weekly basis. Official documents not coordinated at this level, but released by single government agencies such as the Armed Forces, carry less weight. For a more thorough discussion on the hierarchy of official documents in the area of security policy, see Persson (2013b).

2.1 The national security strategy

The “Strategy for the national security of the Russian Federation up to 2020”, published in 2009, sets the stage for the Russian view on information war. It offers a grim outlook on world events (Government of Russia, 2009):

> Global information warfare [informatsionnoe protivoborstvo] is intensifying and the threats to the industrialised and developing world, their socio-economic development and their democratic institutions are growing (§ 10).

It is also made clear in the strategy that information is a tool, among others, that states can employ to improve their national security:

> Strategic deterrence involves the development and implementation of a complex system of interrelated political, diplomatic, military, economic, informational, and other measures aiming to pre-empt or reduce the threat of destructive actions from an attacking state (or coalition of states) (§ 26).

The measures thus enumerated in the strategy are very similar to the Western DIME, spelled out as Diplomatic, Information, Military and Economic power.

Furthermore, the strategy expresses concern that other countries are ahead of Russia in important respects, including information warfare:

> The threats to military security are: the policy of a number of leading foreign countries aiming to achieve overwhelming superiority in the military sphere, primarily in strategic nuclear forces, through the development of high-precision, information and other high-tech means of warfare […] (§ 30).

Importantly, however, not only military or technical threats are outlined in the strategy. To understand the Russian view of information warfare, it is also instructive to consider the wordings on "threats to national security in the cultural sphere":

> National security in the cultural sphere is negatively affected by attempts to revise the interpretation of the history of Russia, her role and place in world history, and lifestyle propaganda based on anything-goes attitudes and violence, and racial, national and religious intolerance (§ 81).

Culture and history are thus matters of national security, and are to be dealt with not only in Russia, but also abroad by

> creating a system of spiritual and patriotic education of Russian citizens, and by developing a common humanitarian and information and telecommunications environment in the Commonwealth of Independent States and its neighbouring regions (§ 84).

Towards the end of the strategy, a few more technical information security threats and responses are outlined:

> The information security threats to the implementation of this strategy are prevented by improving the security functions of information and telecommunications systems in critical infrastructure and high-risk facilities in the Russian Federation, by improving the protection of corporate and individual information systems, and by creating a unified support system for the information and telecommunications systems of importance for national security (§ 109).

These wordings clearly show that cyber issues are a key part of the Russian view of information warfare.

2.2 The military doctrine

The "Military doctrine of the Russian Federation", published in December 2014, also embraces the view of information as a national security tool among others, and information warfare features prominently in several sections. For example, one of the main external military dangers [osnovnye vneshnie voennye opasnosti] identified is (Government of Russia, 2014):

> the use of information and communication technologies for military-political purposes in order to act, against international law, against the sovereignty, political independence, and territorial integrity of states and to threaten international peace, security, and global and regional stability (§ 12.m).

How could such far-reaching effects be achieved by using information? The discussion about the characteristics of modern wars and conflicts offers a number of examples, stressing

> combined use of military force and political, economic, information, and other non-military means that are realised by extensive use of the protest potential of the population [protestnogo potentsiala naseleniia] and special forces (§ 15.a).

This particular scenario – where the population turns against the political leadership – is a recurring theme in the Russian view of information warfare, clearly inspired by recent events such as the “colour” revolutions in former Soviet republics and the Arab spring. Understanding this scenario also makes it easier to understand why the doctrine enumerates other information-related threats, such as influencing young people to abandon historical, spiritual, and patriotic traditions (§ 13.v) or to disrupt government agencies and information infrastructure (§ 13.a).

The emphasis on information warfare is not new. The previous military doctrine, from February 2010, observed that “the role of information warfare is increasing” (§ 12.g) (Government of Russia, 2010) and the task of the Armed Forces and other troops to “develop forces and means for information warfare” is identical in the 2010 (§ 41.v) and 2014 (§ 46.b) doctrines. However, whether any dedicated information warfare units will appear in the Armed Forces’ order of battle is still an open question. In the wake of the war with Georgia in 2008, some experts called for the creation of dedicated “Information Troops” within the Armed Forces. However, it seems that this impetus disappeared around 2011 or 2012, possibly due to institutional competition against the FSB (Giles, 2011).

2.3 The conceptual views

In the official documents discussed so far, information warfare, though acknowledged to be important, is one topic among many. However, in 2011, the Ministry of Defence released the “Conceptual views on the activities of the Armed Forces of the Russian Federation in the information space”, which deals specifically with information warfare from a military perspective (Ministry of Defence of the Russian Federation, 2011).

It is important to understand that the conceptual views are a document on the military strategic level, describing information warfare on an abstract level, linked to the law of armed conflict, to Russian national law, to the military doctrine, and to some extent to Russian foreign policy. The conceptual views are *not* a handbook for operational planning or tactical execution, nor do they describe organisations of staffs or units or say anything about specific capabilities.

A few important observations from the document are the following. The increasing use of information technology (IT) in military and civilian life has made information warfare more important over the past decade (introduction). Information warfare is not a service or branch of its own, but includes elements from intelligence, deception on the operational level [operativnaia maskirovka], electronic warfare, communications, protected and automated command and control, information management among staffs, and also the defence of information systems from electronic warfare and computer network operations (§ 2.3). When engaged in information warfare, the Ministry of Defence is to coordinate its actions with other federal government agencies (§ 2.4). For a more thorough discussion on the cyber aspects of the conceptual views and how the Russian Armed Forces see their role in cyberspace, see Giles (2012).

The conceptual views also offer a number of important definitions, some of which are worth quoting in extenso (Ministry of Defence of the Russian Federation, 2011) (all from § 1):

> Military conflict in the information space [voennyi konflikt v informatsionnom prostranstve] is a way to resolve conflicts between or within states by the use of information weapons.
>
> An information weapon [informatsionnoe oruzhie] is information technology, means and methods that are used in order to wage information war.
>
> Information war [informatsionnaia voina] is a struggle between two or more states in the information space with the goal to damage information systems, processes or resources, critical or other infrastructure, to undermine political, economic and social systems, to destabilise a society and a state by massive psychological influence on the population, and also putting pressure on a state to make decisions that are in the interest of the opponent.
>
> The information space [informatsionnoe prostranstvo] is the sphere of activity related to forming, creating, converting, transmitting, using and storing information to influence both individuals and society, information infrastructure, and information itself.

Again, a few important observations can be made. First, information weapons are not restricted to (cyber) technology – they can also encompass means and methods (though it is vague exactly what this means). Second, information war similarly ranges from action against information systems, to undermining society and broad psychological operations against a populace, to very narrow effects on particular decision makers. Third, the information space – where information war takes place – is very broad, literally including everything that touches information. Thus, the picture of information war painted in the conceptual views is very extensive. It is notable that it covers the entire range from cyber tools to influence.

2.4 The concept for the security of society

Based on these observations from the military documents, it seems clear that to fully grasp the Russian concept of information war, it is necessary to look also at strategy documents outside the military realm. Formally, the reasons for this are twofold: first, the definition of information war quoted above includes civilian aspects, and, second, it is noted that in matters of information war, military forces must be coordinated with other federal government agencies.

Concerning the influence aspects of information war, it is thus worth looking at some wordings in the "Concept for the security of the society of the Russian Federation", published in 2013 (Government of Russia, 2013):

> One of the main sources of threats to the security of society is the extremist activities of nationalist, religious, ethnic and other organisations and structures aiming to ruin the unity and territorial integrity of the Russian Federation, and to destabilise the domestic political and social situation in the country. The spread of extremist sentiments among the youth is of particular concern. Members of extremist organisations actively employ modern technologies, including the information and telecommunications network the Internet, to spread extremist material, to attract new members into their ranks, and to coordinate illegal activity (§ 11).

It is noteworthy that these wordings appeared after the events of the Russian 2011–2012 election cycle, with its large-scale popular protests against the rigging of elections and the corruption of those in power, and the corresponding government crackdown against the opposition after Putin was reinstated as president. For a further analysis of these events, see Franke and Vendil Pallin (2012).

2.5 The information security doctrine

Concerning the technical aspects of information war, the “Information security doctrine of the Russian Federation”, published in 2000, remains the cornerstone. A number of newer documents have appeared in recent years that supplement it, but it is still valid and has not been replaced. It counts information warfare by other countries as one of the external sources of threats to the information security of the Russian Federation (Government of Russia, 2000):

> The development in a number of states of information warfare concepts that are expected to result in means of taking dangerous action in the information spheres of other countries in the world, to interrupt the normal functioning of information and telecommunications systems and obtain unauthorised access to stored information resources (section 3).

The doctrine extensively catalogues threats to information security, and countermeasures to these threats, in many areas of society. In the military area, it is interesting to note that technical measures, such as certification, intrusion detection systems and high-reliability designs coexist with more traditional military measures to counter adversarial information warfare:

> Measures and means to conduct strategic and operational deception [maskirovka], intelligence and electronic warfare, methods and means to actively counter propagandistic information and psychological operations from a probable enemy (section 6).

Thus, the holistic view of information warfare as an integrated whole of technology and influence holds true also when it comes to defence. In this context, it is also interesting to note that the doctrine outlines a number of dangers to information security in the spiritual [dukhovnyi] area:

> Deformation of the mass media system as by monopolisation and uncontrolled expansion of the foreign media sector within the national information space (section 6).
>
> Mass media use by foreign special services, operating on the territory of the Russian Federation, to decrease the defence capabilities of the country and the security of the state, and the spreading of disinformation (section 6).

The spiritual area should also be assessed in the light of the increasing role of the Russian Orthodox Church as a tool for influence and soft power (see Persson, 2013b).

Though these wordings are from 2000, the perspective they represent has only become more prominent in Russian thinking on information warfare since then. As we observed above, the colour revolutions in former Soviet republics and the Arab spring have focused attention on scenarios where the population turns against the political leadership, and this is reflected for instance in the current military doctrine (Government of Russia, 2014). This will also be discussed further in the next chapter.

2.6 Policy documents on international information security

Another area that has received a lot of attention in Russian official documents is the international diplomatic arena. Since 1998, Russia has sponsored a series of resolutions in the United Nations General Assembly, called "Developments in the field of information and telecommunications in the context of international security" (UN GA, 2014). The fact that Russia has chosen the United Nations General Assembly First Committee, which deals with disarmament, as the forum in which to push these questions is interesting. It reveals Russia's strictly military perspective on information war (between sovereign states) that is to be avoided by UN conventions (between sovereign states).

As part of this work, a draft "Convention on international information security", intended for widespread adoption by the countries of the world, is being promoted by the Russian Ministry for Foreign Affairs (Ministry of Foreign Affairs of the Russian Federation, a). The Russian-language version is available on the website of the Russian Federation National Security Council (Ministry of Foreign Affairs of the Russian Federation, b). This draft convention was originally made public in Yekaterinburg in September 2011. The draft contains a section (article 2) listing terms and definitions, largely overlapping with those cited above from the conceptual views. However, in the diplomatic context, it is worth quoting two additional definitions (Ministry of Foreign Affairs of the Russian Federation, a):

> 'information security' [informatsionnaia bezopasnost] is a state in which personal interests, society, and the government are protected against the threat of destructive actions and other negative actions in the information space;
>
> 'international information security' [mezhdunarodnaia informatsionnaia bezopasnost] is a state of international relations that excludes the possibility of breaks in global stability or the creation of threats to the security of governments and the global community in the information space.

This proposed definition of information security differs significantly from the more technically oriented "confidentiality, integrity, availability of data" definition that is commonly used in the West. Whereas the latter definition judges a message to be secure if it reaches its intended recipient, unaltered and without being read by a non-authorised party, the former is so wide-ranging –

requiring protection against negative and destructive action – that it becomes close to being useless in practice. The key to understanding the difference becomes evident when the definition of international information security is taken into consideration. Here, it becomes clearer what negative and destructive actions mean – they relate to the stability and security of governments. This reflects the Russian state-centred, realist view of the world: only state actors matter. This is also why these initiatives are being pushed in the UN General Assembly First Committee. Clearly, the definitions by far transcend the boundaries of technology, and venture into politics, international relations and the law on armed conflict.

As part of its activities to promote its definitions and wider policy stance in this area, Russia has arranged seminars on international information security in a number of capitals around the world. In Sweden, the Russian Embassy hosted such an event on April 2, 2013, inviting academics, politicians, civil servants and representatives from the private sector. The draft convention was presented for almost one and a half hours.

In the context of information operations, it is instructive to consider “the main threats in the information space that could damage international peace and stability” enumerated in the draft convention (Ministry of Foreign Affairs of the Russian Federation, a) (all from article 4):

> 1) the use of information technology and means of storing and transferring information to engage in hostile activity and acts of aggression;
>
> 2) purposefully destructive behaviour in the information space aimed against critically important structures of the government of another State;
>
> 3) the illegal use of the information resources of another government without the permission of that government, in the information space where those resources are located;
>
> 4) actions in the information space aimed at undermining the political, economic, and social system of another government, and psychological campaigns carried out against the population of a State with the intent of destabilizing society;
>
> 5) the use of the international information space by governmental and non-governmental structures, organizations, groups, and individuals for terrorist, extremist, or other criminal purposes;
>
> 6) the dissemination of information across national borders, in a manner opposed to the principles and norms of international law, as well as the national legislation of the government involved;
>
> 7) the use of an information infrastructure to disseminate information intended to inflame national, ethnic, or religious conflict, racist and

> xenophobic written materials, images or any other type of presenting ideas or theories that promote, enable, or incite hatred, discrimination, or violence against any individual or group, if the supporting reasons are based on race, skin colour, national or ethnic origin, or religion;
>
> 8) the manipulation of the flow of information in the information space of other governments, disinformation or the concealment of information with the goal of adversely affecting the psychological or spiritual state of society, or eroding traditional cultural, moral, ethical, and aesthetic values;
>
> 9) the use, carried out in the information space, of information and communication technology and means to the detriment of fundamental human rights and freedoms;
>
> 10) the denial of access to new information and communication technologies, the creation of a state of technological dependence in the sphere of informatization [informatizatsiia], to the detriment of another State;
>
> 11) information expansion, gaining control over the national information resources of another State.

As expected, several of these threats are the same as (or very similar to) those enumerated in the other official documents. Threats 3, 4, and 6 are very reminiscent of the military doctrine's description of how military force can be combined with the "protest potential of the population", emphasising the regime stability aspect (notably in threat 4). Threat 6 again underlines the state-centred realist Russian view on information security. Threats 8, 10, and 11 are similar to the threat of foreign information superiority described in the national security doctrine. Threat 8 also touches upon the spiritual threats outlined in the information security doctrine and should be viewed in the light of the growing role of the Russian Orthodox Church as a soft power tool (Persson, 2013b), whereas threats 4, 5, and 7 closely resemble the threat description given in the concept for the security of society.

The draft convention does not only list threats, but also suggests solutions. Indeed, its second chapter (article 6) outlines "measures for averting military conflict in the information space". Essentially, these measures all hark back to the idea that states have sovereign information spaces, which may not be breached by other states, again stressing the state-centred view. Thus states should, inter alia (Ministry of Foreign Affairs of the Russian Federation, a):

> 4) refrain from any actions aimed at a complete or partial breach of the integrity of the information space of another State;
>
> 5) refrain from using information and communication technology to interfere with the internal affairs of another State; […]

> 8) refrain from slander as well as from using insulting or hostile propaganda to intervene into or interfere in the internal affairs of other States;
>
> 9) have the right and duty to take action against the proliferation of untruthful or distorted messages which could be considered as a means of interfering in the internal affairs of other States or as damaging world peace and security.

While theoretically it might be interesting to ponder the compatibility of these tenets with freedom of speech online, in practice it is quite clear that they collide (Franke, 2013). For example, it is instructive to compare with the wording of the EU cybersecurity strategy put forward by European Commission and the high representative of the European Union for foreign affairs and security policy in 2013 (European Commission and EEAS, 2013, 2.5):

> One of the major elements of the EU international cyber policy will be to promote cyberspace as an area of freedom and fundamental rights. Expanding access to the Internet should advance democratic reform and its promotion worldwide. Increased global connectivity should not be accompanied by censorship or mass surveillance.

The tension between these fundamentally different ways of addressing the role of free information flow on the Internet is obvious, and understanding it explains a lot of the diplomatic frictions over Internet governance in recent years.

2.7 The concept for a Russian cybersecurity strategy

Finally, it is worth mentioning the concept for a Russian cybersecurity strategy (The Federation Council, 2014) that is being developed under the auspices of the Federation Council, the upper chamber of the Russian Parliament. Though it has not (yet) been approved and officially adopted, this document is interesting for several reasons.

First, it notes that other official Russian documents do not differentiate the term cybersecurity [kiberbezopasnost] from information security [informatsionnaia bezopasnost]. As explained in the cybersecurity strategy concept, Russian use of the term “cybersecurity” has mostly been a way to participate in the international dialogue and normative development on cybersecurity. The cybersecurity strategy concept itself, however, offers a definition of cybersecurity that differs from information security (quoting the definition from the draft convention on international information security above, also building on a corresponding notion of information space, quoting the definition from the Ministry of Defence conceptual views above):

> cyberspace is the sphere of activity in information space that is formed by all communication channels of the Internet and other telecommunications networks, the technical infrastructure that ensures their functionality, and all forms of human activity (individual, organisation, state) realised through them;
>
> cybersecurity is the entire set of conditions in which all the components of cyberspace are protected from the maximum number of threats and influences with undesirable consequences.

Notably, cyberspace is explicitly considered a subset of a wider information space. Under this definition, the cognitive domain is fully subsumed into cyberspace.

Second, the cybersecurity strategy concept is considerably less militarised than it is in the other official documents. Admittedly, this is not surprising in the case of the military documents – but the difference between the cybersecurity strategy concept and for instance the information security strategy is striking. This is clearly reflected in the first section of the strategy, which sets the stage for the rest of the discussion. Whereas most other documents focus exclusively on vulnerabilities and risks, the cybersecurity strategy concept acknowledges the positive impact of information and communications technology (ICT) on Russia and the rest of the world in a way that is common in Western official documents, but rarely seen in Russia: “The Internet and other defining parts of cyberspace have been established as shaping factors of Russian economic development and modernisation. Bringing ICT into government processes will be the basis for building an efficient and socially responsible democratic state in the 21st century” (section I). Only then are the threats outlined (section I):

> suffering losses in terms of rights, interests, and livelihood for individuals, organisations, and government agencies;
>
> cyberattacks against protected information resources from cybercriminals and cyberterrorists;
>
> use of cyberweapons as part of special operations and cyberwar, including accompanying traditional military actions.

Here, cyberwar is merely one threat out of many, not featuring as prominently as in the other official documents. Wordings and language also differ: the cybersecurity strategy concept speaks of public-private partnership [chastno-gosudarstvennoe partnerstvo], repeatedly embraces a multi-stakeholder approach to security where government, civil society and business each has its role to play, and invokes as a principle “the balance between establishing responsibility for not observing cybersecurity requirements on the one hand, and introducing too great restrictions on the other hand” (section V). This is quite different from most of the other Russian strategies, which do not concern themselves with the downsides of trying to impose security on society (e.g. costs or unintended adverse consequences). However, given recent developments, it seems unlikely that this cybersecurity initiative will ever be officially adopted.

2.8 Summary

To summarise, the Russian official documents all paint a rather dark picture of the world – a place where information warfare against Russia is commonplace. They also unanimously subscribe to a very broad concept of information warfare, ranging from psychological operations targeting individuals or entire populations, to computer network attacks and the treacherous influence of foreign mass media. The one dissenting voice here is the cybersecurity strategy concept, which stresses the positive aspects of modern information society and sets out to protect them.

In keeping with tradition, the focus of the official documents is defensive – explicitly, they reveal little information about how Russia goes about waging information war against other countries, though a lot can be read between the lines.

Finally, though the media landscape and the public sphere of discourse have evolved a lot over the past decade, there is no obvious trend over time in the Russian official documents.

3 Information warfare in Russian military theory

In official documents, policy is just established, without supporting arguments. Therefore, it is useful to also study the Russian military theory discourse where more profound reasoning can be found. In Russia, the Ministry of Defence publishes *Voennaia mysl*, an official military theory journal, and funds research at the Military University. Though the opinions expressed in the resulting research articles and theses are those of the authors, it is clear that the lines of thought thus expressed say something important about what is deemed worthy of attention in the Russian military establishment. As we shall see, the Russian two-pronged approach to information warfare – taking it into the information-technical and the information-psychological areas (Thomas, 2014) – remains highly relevant. Both aspects must be considered lest we misunderstand and underestimate Russian information warfare capabilities.

3.1 Information warfare in general

A good introduction to the Russian military view of information warfare is an article by retired Major General Ivan Vorobev, published in 2007 (Vorobev, 2007). Vorobev is a grand old man of Russian military theory, who has taught and researched tactics and operational art for decades, following a distinguished military career. In conjunction with his 90th birthday, his contributions to military theory were praised at length by his peers in *Voennaia mysl* (No. 6, 2012). It is safe to say that the perspective advanced by Vorobev carries a lot of weight in the Russian military community.

Characterising modern information war, Vorobev turns to the Gulf war of 1991 to argue the importance of “a thorough assessment in advance of the enemy’s command and control and weapon systems” in order to find weaknesses that can be attacked either kinetically or using electronic warfare resources. Vorobev is a proponent of a very traditional and strictly military mindset, who does not factor civilian actors or economic and social aspects into the military equation. To Vorobev, the new and important aspect is that the enemy can be fought not only by kinetic attack and spatial manoeuvre, but also by means of denying him access to correct information.

To do this, Vorobev defines a three-pronged concept of information attack or information shock [informatsionnyi udar]: (i) information-psychological attack, misinforming and deceiving the enemy; (ii) psychotropic attack, affecting the psyche of the enemy using special means; and (iii) computer attack, affecting the computers in the command and control system of the enemy.

It is instructive to observe here that the view proposed by Vorobev is strikingly similar to that proposed within NATO some 20 years ago, when concepts such as the Revolution in Military Affairs and Command and Control Warfare (C2W) were introduced. Since then, the NATO view has evolved and care is now taken to distinguish the current "information operations" concept from C2W: "Info Ops is neither a continuation of Command and Control Warfare (C2W), nor does it replace C2W. […] C2W is a specific type of operation – Info Ops is a staff function" (NATO, 2009, pp. 10–11).

Vorobev also stresses the importance of coordination when conducting information warfare: "Since there are a lot of forces of different kinds involved when conducting information warfare, an organisation for precise coordination is required". More precisely, this is mostly achieved by coordinating counter-intelligence, electronic warfare, precision strikes on enemy command and control nodes, command posts, intelligence collection assets and radars, as well as computer network operations against enemy command and control systems and the use of deception [maskirovka]. Again, it is evident that what Vorobev has in mind is a conventional symmetric war between state actors. Indeed, the "Information Troops" concept advanced by some experts in the wake of the Georgian war in 2008 (Giles, 2011) was probably geared towards precisely this kind of information warfare.

In this context, it is also interesting to note that the view put forward by Vorobev represents the "standard view" regularly disseminated to the wider Russian military audience. For example, the more hands-on periodical *Armeiiskii Sbornik*, issued by the Ministry of Defence and widely read in the Russian army, featured an article reusing Vorobev's very title "The information shock operation" in March 2011 (Chibisov and Vodkin, 2011). Here, again, the traditional C2W view is promulgated, stressing the coordination of electronic warfare (EW) with intelligence, target acquisition and joint fires, complete with examples from the first Gulf war (which took place almost to the date 20 years before the article was published).

In July 2014 retired Major General Charis Saifetdinov published an article investigating information warfare in the military realm (Saifetdinov, 2014). Following his career as an artillery officer, Saifetdinov served at the Military Academy of the General Staff and directed the 27th Central Research and Development Institute of the Ministry of Defence, overseeing research efforts on command and control systems and computer-aided military exercises.

Saifetdinov observes that in the modern world, information can be used to achieve political, economic, military, and other goals, and he broadly agrees with the official documents (e.g. the 2010 military doctrine) that the use of information warfare alongside traditional military operations is becoming more common. As examples, he cites not only the Gulf war of 1991 and Operation Iraqi Freedom in 2003, but also the events in Ukraine in 2014. Listing the effects that can be achieved by information warfare, Saifetdinov again starts out very traditionally, with two tenets. First, command and control systems can be degraded, disrupting the ability of the political and military leadership to work together, and their sensors can be deceived so that they are unable to function as decision makers. Second, psychological operations can be conducted against the population at large or against individual decision makers. Based on these observations, he concludes not only that conscious and goal-driven information warfare is a deciding factor for who wins or loses a military conflict, but also, and perhaps more interestingly, that the use of information warfare can be a way to avoid open military conflict. This observation, of course, is highly relevant in the light of the events in Ukraine, but is not new. In the Russian context, the frozen conflicts in Abkhazia and Nagorno-Karabakh following the fall of the Soviet Union spring to mind.

Based on the disheartening experience from the operations in Chechnya, Saifetdinov also argues that information warfare has not received enough attention in Russia. He argues that Russia should be eager to learn from how others have conducted information warfare, particularly the American experiences from Iraq and Afghanistan. Indeed, he lists a few important areas where research and subsequent command decisions are needed: the terminology of information warfare needs to be set, the goals that are to be achieved must be made explicit, principles for how to achieve the goals set need to be established, and the appropriate units and resources must be identified. Only then can efficient forms and measures to wage information war be found.

Saifetdinov's laments are typical of a newly established field. Much of his wish list applies equally to NATO. Noting that these issues have indeed received more attention in recent years (as is evident from the official documents analysed in the previous section), Saifetdinov goes on to make some remarks on solutions. First, he argues, the goal of military information warfare should be to establish information superiority [informatsionnoe prevoskhodstvo]. This is interesting, as this concept is not explicitly listed in the Russian official documents, but is very frequently used in the NATO context. Saifetdinov has clearly borrowed this concept from the West. Saifetdinov's next tenet is more interesting, and indeed worth quoting at length (p. 39):

> Information warfare needs to be continuously conducted in peacetime, in periods of escalating threats, and in wartime with all available forces and as a way to act against the information objects of the opposing side and to defend one's own from similar action.

This is important for two reasons. First, the fact that information warfare should be conducted continuously from peace to war. This is interesting in the light of "Conceptual views on the activities of the Armed Forces of the Russian Federation in the information space", discussed earlier (Ministry of Defence of the Russian Federation, 2011), because the conceptual views discuss at length how to contain, prevent and resolve conflicts (chapter 3), as well as confidence-building measures (chapter 4). The focus on international humanitarian law in the conceptual views draws a very distinct line between war and peace. However, as we shall see, it fits very well with the view advanced by Chief of the General Staff Valerii Gerasimov in 2013. Second, the use of all available forces and means emphasises the fact that information warfare is not exclusively in the purview of the military, but rather requires an all-of-government approach.

Indeed, the need for close coordination is at the heart of Saifetdinov's view on the principles for how to achieve information warfare goals. In peacetime, Saifetdinov argues, information warfare must support goals set by the political level, and be conducted to "increase the effectiveness of political, diplomatic, economic, legal and military means to ensure the national security of the Russian Federation, primary to solve the task of strategic deterrence" (p. 40). Here, of course, there is a need for close cooperation between the military and other government agencies with information warfare capabilities. (Unfortunately, Saifetdinov does not enumerate these agencies explicitly.) As a consequence, command and control must be high-level: the General Staff or the central political leadership. The newly established National Defence Control Centre of the Russian Federation [Natsionalnyi tsentr upravleniia oboronoi Rossiiskoi Federatsii], once it starts functioning, probably also has a role to play. The need for coordination applies in war and peace alike, though the particular goals differ.

As for information warfare tasks, Saifetdinov argues – explicitly in line with the military doctrine – that modern war is characterised by an increasing tempo. Today there is an almost real-time requirement on the commander to assess the situation, make decisions, take action and evaluate the effects. This tempo leads to a greater vulnerability to enemy information warfare that affects the C2 systems used for civilian and military command and control at the top level. In addition, Saifetdinov adds, there are the psychological aspects of information warfare. Therefore, protecting C2 systems is a top (defensive) priority of information warfare.

In his conclusion, Saifetdinov argues that it is critically important to find the proper place of information warfare within the unified system of government and military command and control (thus again underlining the importance of looking at the domain not only from a military perspective, but as a whole-of-government approach). A unified system for information warfare should include sub-systems for (i) information assurance, (ii) computer network operations, (iii) intelligence, including signals intelligence, (iv) electronic warfare, and (v) psychological operations including cohesive measures to ensure the morale of one's own troops.

It is useful to contrast the primarily military operational perspective of Vorobev and Saifetdinov with the larger strategic perspective offered by Aleksandr Gorbenko in 2009 in his PhD thesis from the Military University (Gorbenko, 2009). His topic is information warfare in the politics of modern states, and he identifies five areas where both attack and defence are possible on the information arena: (i) systems for making and executing government decisions; (ii) the information resources of government agencies and mass media; (iii) the moral and psychological status of the population in general, and those serving in the security sector in particular; (iv) information infrastructure (networks, communication nodes etc.); and (v) information, communication and control systems (e.g. in industrial plants). Again, this is reminiscent of the view expressed in the official documents.

Another perspective is offered by colonels Sergei Bazylev, Igor Dylevskii, Sergei Komov and Aleksandr Petrunin (Bazylev et al., 2012). Whereas Bazylev works in the Main Operations Directorate of the General Staff, Dylevskii, Komov and Petrunin are experts assigned to the Ministry of Defence, working in the area of international information security (cf. above, Section 2.6). The authors adhere very closely to the (at the time) recently published “Conceptual views on the activities of the Armed Forces of the Russian Federation in the information space”. Their article is essentially a shortened version of the conceptual views, and the authors most probably played an important part in preparing the official document.

Bazylev et al. identify two main effects of information warfare. First, attacks on critical infrastructure systems for industry, finance, energy and transport can have huge consequences in themselves, as well as leading to financial collapses or system-wide economic crises. Second, attacks can be used to disrupt the top political and military leadership, demoralise and mislead the population, and create widespread panic. Again, this is very similar to the doctrinal documents analysed in the previous chapter. One interesting point, though, is the authors’ point on weapons of mass destruction. It is not surprising, claim Bazylev et al., that the heads of state of the Shanghai Cooperation Organization have declared that the use of information weapons can have consequences on a par with the use of weapons of mass destruction. This claim is often referred to in the analysis of Russia’s policy on the use of nuclear weapons, but is frequently misrepresented to say either that Russia puts information warfare on a par with the use of weapons of mass destruction (rather than putting their *consequences* on a par) or, even stronger, that Russia would respond to information warfare using weapons of mass destruction. The latter interpretation is clearly not warranted by doctrine. Rather, the military doctrine states that Russia reserves the right to use nuclear weapons either as a response to use of nuclear weapons or other weapons of mass destruction, or when the very existence of the state is threatened by means of conventional weapons (§ 18) (Government of Russia, 2010).

Whereas Vorobev, Saifetdinov and Bazylev et al. all discuss information warfare within a military context, retired Colonel Anatolii Streltsov adopts a wider strategic scope, including other branches of government, and indeed the political leadership (Streltsov, 2011). Streltsov is a very important player in this context. Not only has he been attached to the Russian National Security Council since 1995, but he is also the author of several authoritative books on government information security strategy and an advisor at the Institute for Information Security Issues at the Moscow State University. As such, Streltsov is very influential with regard to how the Russian national security establishment looks upon information warfare.

Streltsov’s 2011 article is a comprehensive and self-contained statement of the Russian view of strategic information warfare and well worth reading given the prominence of the author. While adhering closely to official documents – policy products the production of which he no doubt has overseen – Streltsov not only reiterates those positions, but also attempts to offer legal, philosophical and social science foundations for them. It is thus worth summarising his article at some length.

The starting point is the same grim world view that is expressed in the national security strategy (Government of Russia, 2009), which is indeed cited. In a world of increasing tensions, widening economic inequalities between countries, and increasing use of information technology, argues Streltsov, global information warfare [globalnoe informatsionnoe protivoborstvo] becomes one of the most important phenomena of international affairs.

More precisely, politics in every country is a battle ground where both legitimate and illegitimate actors participate, the former within the legal framework of the country, and the latter outside that framework. Thus, claims Streltsov, there is a tension between on the one hand the national interest of countries to try and affect the political decision-making processes of other countries in a way favourable to themselves and on the other hand the principles of independence and sovereignty embodied in the United Nations Charter. Whenever one country tries to interfere in the internal affairs of another, it becomes an illegitimate actor in the political processes of that country – often, claims Streltsov, associated with social and individual coercion. Unsurprisingly, the so-called colour revolutions in a number of former Soviet republics are mentioned as examples of such illegitimate meddling by outside forces in the affairs of other countries (the outsiders are not explicitly named, but it is allegedly “not hard to see external political actors interested in these illegitimate, coercive solutions”). From this starting point, Streltsov sets out to determine the main tasks for government policy in information warfare as part of national security, “based on generalisations from political science and practical experience”.

The main government task in information warfare, argues Streltsov, is to thwart the attempts of illegitimate actors to use the information environment [informatsionnaia sfera] to affect national politics in an illegal way. More specifically, this happens in two ways: information warfare *without* the forcible use of technology, i.e. in the area of political ideology, and information warfare *with* the forcible use of technology, i.e. in the area of information technology. These two ways are realised through three sub-tasks delineated in the article: (i) political information warfare, (ii) technical information warfare, and (iii) information provisioning about government policy.

Streltsov defines the first of these sub-tasks as follows (p. 20):

> Political information warfare [politicheskoe informatsionnoe protivoborstvo] involves first and foremost neutralising or reducing the danger that harmful ideological or religious teachings will be spread or that there will be disinformation about state policy in the national or international public sphere.

Danger [opasnost] and threat [ugroza] are somewhat technical terms in this context, used in the national security strategy (Government of Russia, 2009). A danger, according to this terminology, is not currently a threat, but can develop into one.

Political information warfare, according to Streltsov, is wielded within the framework of so-called *soft power* [miagkaia sila]. In the international context, this term was originally coined by Nye (1990), but the Russian use of the term is clearly different and more aggressive. It is noteworthy that the *miagkaia sila* term could equally well translate into *soft force*, a term that might more accurately reflect the Russian perception. A more thorough discussion of the Russian view of soft power is found in Persson, 2014.

The aim of political information warfare is to prevent outside actors from having undue influence on political decisions. Streltsov offers two actual examples: first, international terrorist organisations acting on Russian territory, spreading their ideas; and, second, that Russia is being defamed in foreign countries. Thus, within political information warfare, there are three main tasks: (i) identifying and stopping harmful ideological propaganda, (ii) stimulating civil society to counter harmful ideological propaganda, and (iii) stopping disinformation about state policy.

As for technical information warfare, Streltsov notes that its main goal is to force illegitimate political actors to adhere to international law (i.e. non-interference). More precisely (p. 22):

> Technical information war [tekhnicheskoe informatsionnoe protivoborstvo] is waged by special information and communication technology (called ‘information weapons’ [informatsionnoe oruzhie]), designed to breach the robustness and security of the information infrastructure objects on the opposing side.

These “information weapons” are what would probably be called cyber capabilities in a Western discourse.

Adhering as ever to official documents, Streltsov claims that there is an ongoing global arms race in information weapons. Within technical information warfare, there are three main areas to attend to: (i) preparations in order to be able to act forcibly against the ICT systems of potentially hostile or unfriendly states; (ii) maintaining the security of one's own critical infrastructure ICT systems in order to eliminate or diminish the consequences of attacks from hostile or unfriendly states; and (iii) making sure that sufficient intelligence on military-political, social and economic conditions is gathered through the collection of signals and computer intelligence [kompiuternaia razvedka].

As for information provisioning about government policy, it is defined as follows (p. 22):

> Information support to government policy [informatsionnoe obespechenie gosudarstvennoi politiki] involves attaining support from domestic society and from the international community for the activities within that policy, and cooperation in implementing it.

Streltsov breaks this task down into two sub-tasks: (i) maintaining a positive image of the state [obespechenie pozitivnogo imidzha gosudarstva], and (ii) making sure that the community is informed about the actions taken as part of state policy. Important aspects of maintaining a positive image internally include the image of its leaders, what is taught in schools, not least with regard to history, and the shape of the public debate. There is also the matter of how the state is perceived externally, abroad, which again depends on the opinions of influential individuals in other countries, on how history and other subjects within the humanities are taught, and on how the state is treated in foreign media.

Keeping the community informed about the actions taken (again) includes building a positive image of national history, but also showing how the political leadership has actually solved specific problems. If this task is successfully resolved, argues Streltsov, the positive sentiments of the national and international community will help maintain social stability within the population (this wording is by now familiar from the official documents) and also create a positive environment in which citizens, companies and investors will be attracted to take part in the successful realisation of government policies. In order to successfully spread the word of successful government policies, of course, government agencies and officials will have to closely "cooperate" with mass media and civil society.

Streltsov concludes his article by reiterating that the tasks thus delineated are necessary for national independence and sovereignty in modern global information society. To carry out these tasks successfully, he also notes, there is a need for close coordination between the federal agencies and other organisations involved.

To summarise, it is clear that there are several perspectives on information warfare among Russian military theorists. Vorobev, for example, adopts a traditional and strictly military perspective, whereas Streltsov offers a more strategic and politically oriented outlook. Whereas the former perspective is similar to the C2W view held within NATO 20 years ago, the latter is probably influenced by the evolution of an increasingly international media landscape and the experience of the so-called colour revolutions in former Soviet republics. Indeed, a colour revolution in Russia seems to be Streltsov's worst fear. It is worth stressing that the perspectives we have seen represent different parts of a whole – the Russian view of information warfare has both military and non-military components.

3.2 Influence operations

Rustam Bagirov, in his PhD thesis from the Military University, addresses the issue of political communication to safeguard Russian military security (Bagirov, 2009). In the foreign policy context, he advocates a system to counteract hostile information influencing senior civilian and military decision makers, as well as the population at large. As an example, he explains how the Russian senior political leadership and the mass media coordinated their efforts during the 2008 war against Georgia in order to counter negative reporting abroad. Internally in Russia, Bagirov calls for "coordination of the information activities of government agencies". If government communication is not improved, it will not be possible to manage the threats to the military security of the country, claims Bagirov. He suggests developing a "concept for military information politics, corresponding to the organisation of the Armed forces", and proposes that inspiration can be found in modern marketing.

Aleksandr Priakhin, in his PhD thesis from the Military University, addresses the "moral spirit" of the Russian army, how it is affected and changed in modern information society, and how information warfare [informatsionnoe protivoborstvo] can be used to ensure a high fighting spirit (Priakhin, 2009). Among other things, Priakhin recommends active government work to improve the status of soldiers in society and to raise their material, social and moral status. In particular, the ministries for culture and education are encouraged to promulgate national values, the proud history of Russia and Russian traditions. To facilitate this, Priakhin also recommends government control of important mass media.

It is interesting to note that both Bagirov and Priakhin discuss influence operations on a strategic level, proposing policies that need to come into effect well before a conflict. This underlines the fact that information warfare requires thorough planning before the shooting starts.

3.3 Electronic warfare

One important aspect of information warfare is its relation to other, closely related, disciplines. Retired Lieutenant General Viktor Kuznetsov, retired Colonel Yurii Donskov and Colonel Andrei Korobeinikov attempt to sort out the relation between electronic warfare (EW) [radio-elektronnaia borba] and information warfare (IW) [informatsionnaia borba], tracing this question back to the discussion in the 1980s and 1990s on network-centric warfare (Kuznetsov et al., 2013). To understand their perspective, it is worth noting that the authors all represent the EW community, having served as officers in the EW branch and made their scientific careers in EW research institutes.

Looking historically at EW, the authors describe how it first arose in the early 20th century, when military units began to use radio devices for communications, and that it was at its apex in the late 20th century, when radio had become ubiquitous. EW systems and units can now be found from the strategic to the tactical level, and they cooperate closely with other functions such as joint fires, signals and intelligence. However, the late 20th century also saw the rapid development of C2 systems based on modern information and communications technology (ICT), leading to widespread discussions on C2 warfare as a means to attain information superiority. To explain this concept, Kuznetsov et al. explain that military decision making comprised four processes: (i) obtaining information, (ii) processing it, and (iii) communicating decisions to subordinates, thus (iv) controlling units and weapon systems. This is the military context in which, according to Kuznetsov et al., the EW and IW concepts have become increasingly intertwined. There is also a technological context of automation, robotisation and developments in artificial intelligence for military decision support, where the authors lament the fact that Russia is more than 15 years behind the most advanced countries.

In order to analyse the future impact of information warfare, Kuznetsov et al. describe how it differs from EW. First, EW is only concerned with the electromagnetic spectrum, whereas IW potentially uses all possible ways to mediate communications. Second, EW units have traditionally been geared towards electronic attack such as jamming, whereas in the future IW context there will probably be a need for more symmetric efforts in attack and defence. The rest of the article is concerned with how the EW service needs to change in order to fit within modern IW. Here one can read, between the lines, a concern with the survival and thriving of the EW service at least as great as the concern for effective military operations. The suggestions are both technological – highlighting the need for new jamming equipment aboard new platforms – and conceptual – stressing that EW should be seen through the broader IW lens, where jamming is supplemented with deception and information flooding, and EW efforts might be led by an assistant chief of staff for IW.

Colonel Vladimir Balybin, retired Colonel Yurii Donskov and Major Aleksei Boiko address the issue of EW in the context of information warfare in general, and cyberwarfare in particular (Balybin et al., 2013). Again, the authors all represent the EW community. Basically, they authors argue that EW terminology needs to be updated with new concepts if it is to match the rapid development of information technology and its role in modern information warfare.

At the heart of their analysis is the following definition of cyberspace [kiberprostranstvo], where it should be noted that the cognitive aspects are still left out (p. 30):

> the totality of the information and the information infrastructure that is designed to develop, create, convert, transmit, use and store this information using computers and computer networks.

In war, cyberspace is used in order to supply information and for effective command and control of forces and weapon systems. Now, in modern network-centric warfare [setetsentricheskie boevye deistvie], EW is used to achieve information superiority [informatsionnoe prevoskhodstvo] over the enemy. However, this can be done in many ways, and the use of various kinds of software to affect enemy systems is growing, argue Balybin et al.

The main problem, according to the authors, is that EW is centred on the concept of radio-electronic objects [radioelektronnye obiekty], basically technical objects that emit radio waves. However, there is an increasingly poor correspondence between these objects and key objects in modern, computerised command and control systems. A lot of equipment highly relevant to the task of achieving information superiority is left out.

To set this straight, Balybin et al. propose a relatively simple change: to replace radio-electronic objects with information technology objects [informatsionno-tekhnicheskie obiekty]. If this larger class of objects were to become the centre of attention of EW in the future, EW would be in a much better position to help achieving information superiority.

Interestingly, the authors explicitly warn that failure to address this problem might be detrimental to the development of the EW service, and make it harder to develop forces capable of specialised military operations in cyberspace. In contrast, by adopting the proposed change, there will be a "new, extra impulse of justification to develop the EW service", which will allow Russia to increase its information warfare capabilities to reach international standards. Again, it is quite clear that the authors are concerned that the EW service will not get its fair share of attention as new information warfare capabilities are developed.

To summarise, it is interesting to note that the articles written by representatives of the EW service apparently reflect a fear of being left out as a new landscape of information warfare matures. Following the demise in 2011–2012 of the

"Information Troops" concept (Giles, 2011), based on the EW service, the articles, published in 2013, seem to reflect a concern and disappointment with this development. Whereas EW traditionally has played a very important role in battlefield information superiority, it clearly risks becoming less important in a more strategically oriented information warfare context as proposed e.g. by Streltsov.

3.4 Cyberwarfare

"Cyber" issues and their role in information warfare are another important topic that has received a lot of attention in Russian military theory discussions.

In a 2011 article, Colonel Pavel Antonovich sets out to capture the "essence and contents of cyberwar" (Antonovich, 2011). Antonovich has a background in EW and currently serves at the Military Academy of the General Staff. Noting that information security issues are becoming more important in international affairs, and observing that there is a plethora of "cyber" terms floating around, he attempts to reach reasonable definitions of key terms. Doing so, he takes account of etymology, but importantly also looks to US terms and definitions, in particular the 2009 acknowledgement of cyberspace as a domain for military operations.

Antonovich also identifies some important characteristics of cyberspace. The near-absence of national borders in cyberspace makes the legality of many acts difficult to determine. Though many countries have legislation outlawing various forms of cybercrime, there is no single and unified international legal regime. The best attempt so far to create one, the Budapest convention on cybercrime that Russia fervently opposes, is conveniently left out of the discussion. It is thus possible, argues Antonovich, to speak of a range of adversarial, criminal and destructive ways to use networked resources.

Investigating US terminology, Antonovich argues that the computer network attack (CNA) concept is not synonymous to the cyberattack concept, because it refers only to networks, not to cyberspace at large. Instead, he proposes the following definition (p. 42):

> A cyberattack [kiberataka] is a form of adversarial (illegal) acts in cyberspace; acts that are directed against cybernetic systems, information resources or information infrastructure to reach some kind of objective, and are carried out with the help of special computer equipment and means (ways) to reach effects.

Furthermore, in cyberspace, attacks are closely related to vulnerabilities. If there are no vulnerabilities, it is useless to attack, argues Antonovich. He therefore offers two additional definitions (p. 43):

> A cyber vulnerability [kiberuiazvimost] is a weakness (deficiency) in a cybernetic system, in relation to which there exists one or more cyberthreats, and which could be used to realise a cyberattack.
>
> A cyberthreat [kiberugroza] is the combined conditions and factors that could be realised in relation to a cyber vulnerability to raise the risk of damage to a cybernetic system or its owner.

Following these two definitions, a cyberweapon can be said to be in use whenever a threat, related to a vulnerability, is actually realised (or in defending against this).

Having offered these definitions, Antonovich goes on to discuss cyberwar and cyberconflict. He observes that many actors, in principle, have the resources and incentives to take part in such conflicts, and therefore offers a broad definition of cyberwar, including non-state actors (p. 45):

> Cybernetic war [kiberneticheskaia voina] is the systematic struggle [sistematicheskaia borba] in cybernetic space between states (or groups of states), political groups, or extremist, terrorist etc. groups that is carried out in the form of attack and defence.

The main targets (of attack and for defence), Antonovich notes, are information resources, which are threatened in terms of the standard information security aspects of confidentiality, integrity and availability. Here it is worth noticing that Antonovich's definition of cyberwar is considerably wider than the definitions of military conflict in the information space or information war from the conceptual views, as it includes non-state actors (Ministry of Defence of the Russian Federation, 2011). However, extremist, terrorist, and criminal non-state actors are included among the threats enumerated in the draft convention on international information security (Ministry of Foreign Affairs of the Russian Federation, a).

Relating to official documents, Antonovich quotes the national security strategy (Government of Russia, 2009), but observes that the documents published so far have not discussed cyberwar to the extent he deems necessary. He concludes that more discussion, studies and development are needed.

The issue of non-state actors in cyberspace is at the heart of an article by Anton Varfolomeev, who conducts an analysis of the relation between (government-sponsored) cybersabotage and (non-government) cyberterrorism (Varfolomeev, 2012). Varfolomeev has served as a diplomat, working with terrorism issues in the Council of Europe and the G8, and now teaches at the Lobachevskii State University of Nizhni Novgorod. Using the Stuxnet cyberattack on the uranium enrichment plant in Natanz, Iran, as a case study, he argues that there are striking similarities between cybersabotage and cyberterrorism. For example, while the Russian legal definition of sabotage is written with foreign military or intelligence service teams striking at the economy or military capability of Russia in mind, similar actions could be carried out by non-state actors as well. The point is that this is becoming easier using cyber means than with conventional means. While terrorism is illegal everywhere, government-sponsored sabotage resides in some kind of legal grey area: Varfolomeev argues that (in any country) “our guys” are always intelligence officers working within the legal limits of our jurisdiction, whereas “their guys” are always spies, working outside the laws that we recognise. Of course, this is not the whole truth. Varfolomeev conveniently overlooks cases such as Watergate, the Iran-Contra affair or the Swedish IB affair – public opinion in free countries has not always been so forgiving to their own intelligence agencies and governments.

The key concern voiced by Varfolomeev is the following: how big is the risk that government-developed capabilities for cybersabotage will fall into the wrong hands and become generally available to would-be cyberterrorists, to the detriment of every government? Though, unsurprisingly, he is asymmetric in basing his analysis solely on the cybersabotage capabilities of “leading Western countries” (p. 7).

To answer this question, Varfolomeev identifies three kinds of limitations on cyberterrorist capability. First, there is scarcity of resources. Terrorist groups, at present, cannot devote as much human resources and man-hours as governments to developing sophisticated tools for cyberattack. This limitation has been a key assumption in the analyses deeming Stuxnet to be the work of one or more governments. However, even if people and know-how are bottlenecks, it would be theoretically possible for terrorist organisations to recruit people who have experience from government-sponsored cyberattack development programmes, thus inheriting knowledge. Some kinds of technology can also be hard to obtain, though it can be stolen from companies. Varfolomeev recommends public-private partnerships to protect sensitive industries from such illegitimate technology transfer. Second, there are limitations on the possibilities for carrying out cross-border operations. However, globalisation in general and worldwide markets for ICT in particular have certainly lowered the thresholds for the would-be cyberterrorist. Third, terrorist groups have less analytical and data-processing capabilities than governments. However, this difference can be expected to decrease in the future.

Retired Lieutenant General Viktor Kuznetsov, retired Colonel Yurii Donskov and Lieutenant Colonel Oleg Nikitin have tried to delineate the role of cyberspace in modern military operations (Kuznetsov et al., 2014). Again, given their background, these authors approach the issue from an EW perspective. Observing that there is a confusion of terminology, they propose a three-pronged understanding of the modern battle space. First, there is the physical battle space in the traditional limited sense [boevoe prostranstvo (v uzkom smysle)]. For a mechanised company within a battalion, they argue, this is a few square kilometres, with perhaps 30 important objects. However, in modern conflicts, this needs to be expanded to cover cyberspace [kiberprostranstvo], defined by Kuznetsov et al., following Balybin et al. (op. cit.), as the totality of the information and the information infrastructure that is used in combat to manage information and make decisions. They give the example of a US brigade that was equipped with 2 500 work stations mounted in 900 armoured personnel carriers and connected into a single network. Such modern ICT systems enable improved situational awareness and also allow modern high-precision weapons systems to reach their full potential. Kuznetsov et al. note that Russia is also moving towards similar, fully computerised, C2 systems. However, cyberspace thus defined is also the physical basis of an even wider concept, namely the information space [informatsionnoe prostranstvo].

This space, the widest of them all, also includes information that is not stored in any technical infrastructure, but rather in the minds of decision makers. The information space, thus defined, goes beyond technology, and also includes the psychological aspects of information warfare. Thus, whereas cyberwarfare might be about going after databases and communications links, other forms of information warfare, including tactical and operational deception [maskirovka], occur not (only) in cyberspace but in the wider information space. According to the authors, the physical battle space is thus a part of cyberspace, which is in turn a part of the information space.

Kuznetsov et al. observe that cyberwarfare is still in its infancy. However, many countries, including Russia, are developing their capabilities in this area, and are creating specialised military cyber units. Unfortunately, the authors do not elaborate on the nature of the Russian efforts.

Attempting to draw conclusions from their analysis, Kuznetsov et al. contrast the situations of the individual soldier or junior officer with that of a more senior officer commanding a larger unit. The individual soldier or platoon leader mostly makes decisions on a minute-by-minute basis, in a battle space that is usually more or less within visual range. Therefore, it is difficult to affect these decisions by cyber means. The commander of a brigade, in contrast, makes decisions on a 30–40-minute time scale, aided by a staff, and acts in a battle space that encompasses hundreds of square kilometres. His battle space also contains hundreds of servers, work stations, and communications lines – and cyberattacks against these have the potential of significantly affecting the ability of the brigade to carry out its assigned tasks. To the extent that the commander uses advanced decision-support systems, attacks on these are another potential vulnerability.

In conclusion, Kuznetsov et al. observe that the advent of modern ICT both enables new ways of affecting the enemy (cyberattacks) and new ways of leading subordinates (modern C2 systems).

To summarise, Russian military thinking about cyberwar seems to be at a formative stage. This is evident both from the vivid discussion about conceptual definitions and from the fact that there is no agreement on the military implications. However, it is still an open question whether military thinking will ever really catch up with the pace of technological developments in the realm of information and communication technology.

3.5 Information warfare in modern war

Though most authors in the Russian military debate agree that information warfare is becoming increasingly important, it is not the only aspect of modern wars that has received attention. It is instructive to consider how information warfare can be placed within a wider context.

Retired Colonel Sergei Chekinov and retired Lieutenant General Sergei Bogdanov address information warfare in the context of war by non-military means [nevoennye sredstva] and war by indirect approach [nepriamye deistviia] (Chekinov and Bogdanov, 2011). The authors are both affiliated with the Centre for Military Strategic Studies of the General Staff, which is directed by Chekinov. As such, their analysis should be given considerable weight when attempting to understand the Russian perspective on information warfare.

In the analysis of Chekinov and Bogdanov, which proceeds from the same ominous outlook on the world as do the official documents, the indirect approach is becoming increasingly important in the modern world. Indeed, they argue, whereas the indirect approach has historically been second to the direct one of overpowering manpower and weapons, in the present world the indirect approach is increasingly becoming the first and foremost tool of the master strategist. Unsurprisingly, their prime example is the policy of the US and other countries, described as “aggressive goals being masked behind the pretence of spreading ‘democracy’, ‘protecting the weak’ or the war on terror”.

The indirect approach in warfare can roughly be described as follows. Do not attack the enemy where he is strongest, but where he is weakest. Do this by surprise and quick manoeuvring, and by continuously looking for unexpected opportunities for attack. Chekinov and Bogdanov describe the idea referring to Sun Tzu and Napoleon, but first and foremost they cite British General Liddell Hart, who is usually credited with the modern idea of the indirect approach (as well as the English terminology). Liddell Hart argued that successful manoeuvre warfare and unexpected attacks on enemy weaknesses would eventually lead to *dislocation* of the enemy’s preparations – psychological and physical – thus in effect winning the battle before it starts (Widén and Ångström, 2005, cf. in particular pp. 92–93 and pp. 183–184).

Chekinov and Bogdanov argue that, while deception has always been used in war, in the modern world, the means of influence by information [sredstva informatsionnogo vozdeistviia] (a kind of indirect approach) have developed to the level where they can actually perform strategic tasks on their own. Indeed, whereas Liddell Hart investigates indirect action primarily within the traditional military context, Chekinov and Bogdanov thus explore its use in the wider context of international relations more broadly. Echoing the wording of official documents, they argue the importance of information warfare (p. 6):

> Experience from local wars and armed conflicts of the past decades shows that strategic information warfare [strategicheskoe informatsionnoe protivoborstvo] plays an important role in disrupting military and government leadership and air and space defence systems, misleading the enemy, forming desirable public opinions, organising anti-government activities, and conducting other measures in order to decrease the will of the opponent to resist.

In order to ensure the military security of the Russian Federation, they argue, system-wide measures need to be taken, including political, diplomatic, information, economic, military, and non-military means.

In particular, Chekinov and Bogdanov argue that the combined factors of globalisation and the advent of modern information technology have created closely integrated economic ties – including the global flows of resources, technology, money, information, etc. – between different countries. Whereas this interdependence is often taken as a factor favouring peace and stability, Chekinov and Bogdanov see it rather as a threat. Globalisation and IT, they argue, open new avenues for influence. This view is, by now, familiar from the official documents – recall the “uncontrolled expansion of the foreign media sector” from the information security doctrine – and also fits well with the repressive domestic Internet policy (cf. also below, Section 4.5). Unsurprisingly, Chekinov and Bogdanov criticise US policy to uphold the globalised economic system, and cite the fall of the Soviet Union and the “system of world socialism” as a cautionary example of the fact that “today states that are unable to ensure their information security risk losing their political sovereignty and economic independence, and cannot aspire to be global or even regional leaders”.

Having thus summarised the thinking of Chekinov and Bogdanov on information warfare in the context of the indirect approach, it is also worth mentioning that the authors, in order to strengthen their thesis about the importance of non-military means in current world affairs, promulgate a number of far-fetched conspiracy theories towards the end of their article. Thus, according to Chekinov and Bogdanov, not only were the colour revolutions in former Soviet republics the work of the US intelligence services, but furthermore Roosevelt and Churchill incited Hitler to attack the Soviet Union in 1941, and the 2004 Indian Ocean earthquake and tsunami were the work of a US super-weapon. (Such "climate weapons" serve as an example of the indirect approach.) The fact that these claims are advanced by the Centre for Military Strategic Studies of the General Staff is disconcerting in its own right.

Another perspective on information warfare is given by Colonel Yurii Starodubtsev and Lieutenant Colonels Vladimir Bukharin and Sergei Semenov, who offer a critique of the "information war" [informatsionnaia voina] and "network-centric war" [setetsentricheskaia voina] concepts, as part of their introduction to the "technospheric war" or "war in the technological realm" [tekhnosfernaia voina] concept (Starodubtsev et al., 2012). The three authors all have a background in the EW service.

Starodubtsev et al. differentiate between two meanings of information war. First, it is to influence the civilian population or military personnel of another country by spreading certain information. This basically reflects the psychological operations aspect, and the authors note that such operations can target both broad groups and specific individual decision makers, such as "a president, a prime minister, a minister for foreign affairs, diplomatic representatives, commanders of military forces etc.". Second, information warfare is activities aiming to achieve information superiority [informatsionnoe prevoskhodstvo] over the enemy, by means of inflicting damage on his information, information processes and information systems while at the same time protecting one's own. These observations lead Starodubtsev et al. to offer their own definition of information war (p. 24):

> Information war [informatsionnaia voina] *is the complex impact (of the whole set of information operations* [*informatsionnye operatsii*]*) on the system of government and military command and control and on the military-political leadership of the opposing party*, that already in peacetime can lead to decisions in the interest of the initiating party, and that throughout the conflict can completely paralyse the command and control infrastructure of the enemy.
> [Emphasis in original]

As we have seen above (e.g. Saifetdinov), this definition offers a view of information warfare that is continuous through peace and war. However, the authors criticise both "information war" and "network-centric war" for being terms used without proper substantial contents, thus hindering the proper development of the field. Instead, they propose their own concept (p. 27):

> War in the technological realm [tekhnosfernaia voina] is a system of information acts, coordinated in terms of goal, place, and time, aiming to take control (partially or fully) of selected automated enemy command and control systems, or to set them into a destructive state.

This concept is considerably more limited than the whole of information war. In fact, it resembles a definition of what might be called cyberwar. The notions of psychological influence are excluded, leaving only a technological core. Indeed, the authors note that war in the technological realm will only be subject to known laws of technology and technological uncertainties, whereas the probabilistic nature of traditional war (allowing for weather, the fighting spirit of the troops etc.) is eliminated.

To understand why Starodubtsev et al. find “war in the technological realm” to be a more useful concept than either information war or network-centric war, it helps to recall their EW background. It stands to reason that they find a purely technology-oriented concept of warfare more attractive, and easier to square with traditional EW operations.

Another perspective on information warfare as part of modern war was given by the Chief of the General Staff, Valerii Gerasimov, in a speech to the Russian Academy of Military Science in January 2013, later reworked and published as an article (Gerasimov, 2013). In particular, he discussed the role of non-military methods in modern conflicts.

He notes that the role of non-military means has increased, and that they can now be far more effective than traditional weapons. As usual, the Arab spring is invoked as an example (p. 2):

> Experience from military conflicts, including from the so-called colour revolutions in North Africa and the Middle East, confirms that a relatively flourishing state in just months or even days can become an arena for vicious armed conflict, a victim of foreign intervention, and descend into chaos, humanitarian catastrophe and civil war.

The difference, compared to the standard Western interpretation of these events, is striking, but not surprising.

According to Gerasimov’s model, information warfare [informatsionnoe protivoborstvo] is conducted continuously throughout the conflict – long before there is an open military conflict. Indeed, the military means are but a small part of war – the largest part by far is played by non-military means.

Much has been made of Gerasimov’s speech, and in particular of the diagrammatic illustration accompanying it. When assessing his message, it is important to bear in mind that it was delivered in an address to his fellow generals in the Russian Academy of Military Science. It does not represent a turning point in the Russian view of modern war or information warfare – on the contrary, it continues the official documents and military theory reviewed above. However, the message of the decreasing role of traditional military means was certainly provocative to some of the (retired) military establishment – and it was certainly meant to be. In this sense, the Gerasimov address should be seen as part of the effort to reform and modernise the Russian Armed Forces. See also the analysis of Gerasimov’s speech in Persson (2013b).

3.6 Summary

Summarising the Russian debate about information warfare in the larger context of modern war, a few observations can be made. First, from a military perspective, there is a striking pessimism: non-military measures outweigh military measures by four to one, argues Gerasimov, but he suggests no remedy for how to make the military tool more powerful. This is startling, coming from the chief of the general staff. Chekinov and Bogdanov fear the globalised and economically integrated world, but offer no way out of it. Second, it is clear that there is a lively debate about information warfare in the larger scheme of things, drawing both on classic theories such as Liddell Hart’s and on more modern ones such as “war in the technological realm”.

One important observation is that most theorists perceive information warfare as continuous between peace and war. The implication is clear: we are at the receiving end of Russian information warfare at this very moment.

Looking at the Russian military theory debate at large, several trends coexist. Information warfare is sometimes construed as a narrow battlefield activity, but most often it is seen as a larger strategic matter. Some services, such as EW, contemplate their role in such a larger context, sometimes from a rent-seeking perspective. While many authors closely follow the international debate on information and cyber operations, the implications and conclusions drawn still seem largely influenced by the Soviet legacy. The overall perspective is defensive and pessimistic. Nevertheless, keeping this defensive perspective in mind can be useful also when analysing situations where Russia is on the attacking rather than the defending side.

4 Case studies and reflections

Having thus acquainted ourselves with Russian official documents and military theory, it is time to turn to some practical examples and see how they connect to the theory. The aim of the intellectual framework is to better understand the practice. The examples are only meant to be suggestive, not exhaustive.

4.1 History education

As noted above, the national security strategy worries about attempts to “revise the interpretation of the history of Russia, her role and place in world history” (Government of Russia, 2009). Streltsov argues along similar lines, making the building of a positive image of national history an important part of what he calls “information provisioning about government policy” (Streltsov, 2011). Priakhin, earlier, argued the same case (Priakhin, 2009).

This particular aspect of the Russian theory of information warfare is now being put into practice. In February 2013, President Putin ordered the Ministry of Education to create new history textbooks for schools, containing a single and unified interpretation of Russian history. There should be no room for “contradictions or double interpretations”. According to the time plan, the textbooks will be ready in 2015. In Russia, history is a matter of national security (Persson, 2013a).

In other countries, such attempts would not necessarily be categorised as information warfare. But theorists such as Streltsov and Priakhin explicitly mention history, and how it is taught, as matters of information warfare [informatsionnoe protivoborstvo]. Indeed the Armed Forces have had a unit combating the “falsifications of history” since July 2013 (Persson, 2013a).

4.2 The campaign to discredit Carl Bildt

Throughout the escalating crisis in and subsequent Russian aggression against Ukraine from late 2013 onwards, Swedish Minister for Foreign Affairs Carl Bildt was an outspoken supporter of Ukraine and a critic of Russia until his term in office ended following election defeat in September 2014. Therefore it is not surprising that he was regularly smeared in Russian state-controlled media such as RT (formerly known as *Russia Today*).

For the domestic Russian-speaking audience, Bildt was discredited in the popular *Vesti Nedeli* [News of the Week] show on the state-owned TV channel Rossiia 1 on December 1, 2013 (Kiselev, 2013). Bildt was called a CIA agent and a Poltava revanchist, and this was followed by smearing of degenerate Swedish child-rearing and children’s culture (Ennis, 2013b). A week later, *Vesti Nedeli* host Dmitrii Kiselyov was appointed head of the new Russian international news agency Rossiia Segodnia, formed by merging state-owned news agency RIA Novosti and the official international radio station, Voice of Russia (Ennis, 2013a).

In the wake of the Malaysian Airlines flight MH17 tragedy, Bildt and Polish Minister for Foreign Affairs Radek Sikorski were dubbed “the principal perpetrators of this madness”, having schemed to break “the ties between Russia and Ukraine that had taken centuries to build” (Lozansky, 2014). In August, an RT columnist celebrated Bildt’s predicted electoral defeat: “If any single European politician has blood on his hands in Ukraine this year, it’s Stockholm’s resident neo-con fanatic” (MacDonald, 2014).

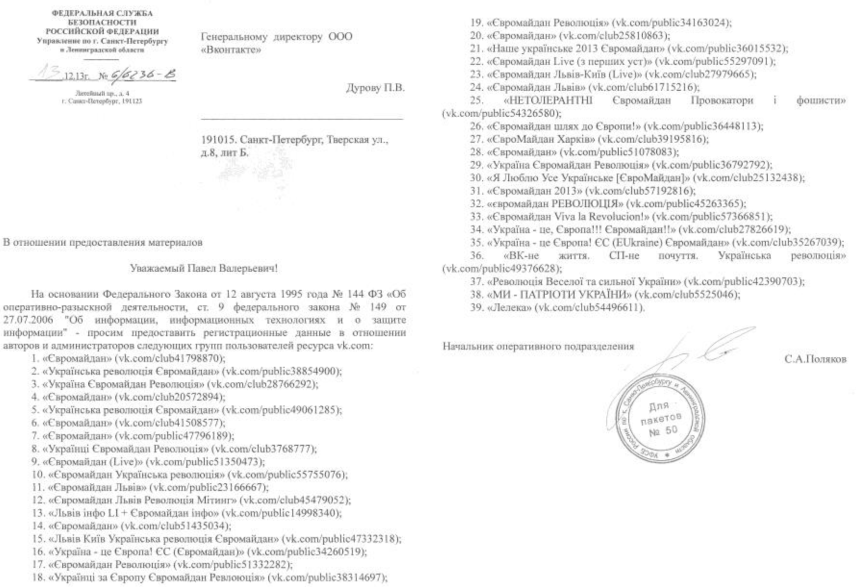
The significance of the anti-Bildt campaign should not be overstated. What is interesting in this context is how the denigration of Bildt relates closely to Streltsov’s political aspects of information warfare (Streltsov, 2011). Streltsov argues that the state must maintain a positive image of its political leaders (p. 23), and he explicitly states that (defensive) political information warfare should identify and stop harmful propaganda and disinformation, in the national and international public spheres. The discrediting of Bildt is an excellent example of how such political information warfare looks when it is not defensive, but attacking.

4.3 The illegal annexation of Crimea

The use of information warfare in conjunction with the illegal annexation of Crimea in early 2014 has received a lot of attention. The following exposition builds on the analysis of the military operation, including its information warfare aspects, given in Norberg et al. (2014), but additionally factors in the perspective of official documents and military theory.

The Crimea operation was not merely a military operation. At the time, Russia used the Armed Forces in four different ways, none of which involved traditional combat: to threaten Ukraine; for diversions; to facilitate local forces taking power; and to actually take and hold Crimea, i.e. to enable an illegal annexation. After the Crimea operation, however, the Armed Forces have been involved in combat in eastern Ukraine. Indeed, these uses of the military tool in concert with other branches of government to achieve the intended effect are a good illustration of the principles suggested by Saifetdinov and Streltsov. Therefore, the new and surprising aspect of the Crimea operation was not the capabilities of the Armed Forces, but rather the capability to coordinate military and non-military means, including the information warfare aspects.

The centre of gravity was not territory, but Ukraine’s will to resist. That will was deliberately diminished through the information environment. One key aim was



ФЕДЕРАЛЬНАЯ СЛУЖБА
БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Управление по г. Санкт-Петербургу
и Ленинградской области

13.12.13г. № 6/6236-В

Литейный пр., д. 4
г. Санкт-Петербург, 191123

Генеральному директору ООО
«Вконтакте»

Дурову П.В.

191015. Санкт-Петербург, Тверская ул.,
д.8, лит Б.

В отношении предоставления материалов

Уважаемый Павел Валерьевич!

На основании Федерального Закона от 12 августа 1995 года № 144 ФЗ «Об оперативно-разыскной деятельности, ст. 9 федерального закона № 149 от 27.07.2006 "Об информации, информационных технологиях и о защите информации" - просим предоставить регистрационные данные в отношении авторов и администраторов следующих групп пользователей ресурса vk.com:

1. «Євромайдан» (vk.com/club41798870);
2. «Українська революція Євромайдан» (vk.com/public38854900);
3. «Україна Євромайдан Революція» (vk.com/club28766292);
4. «Євромайдан» (vk.com/club20572894);
5. «Українська революція Євромайдан» (vk.com/public49061285);
6. «Євромайдан» (vk.com/club41508577);
7. «Євромайдан» (vk.com/public47796189);
8. «Українці Євромайдан Революція» (vk.com/club3768777);
9. «Євромайдан (Live)» (vk.com/public51350473);
10. «Євромайдан Українська революція» (vk.com/public55755076);
11. «Євромайдан Львів» (vk.com/public23166667);
12. «Євромайдан Львів Революція Мітинг» (vk.com/club45479052);
13. «Львів інфо LI + Євромайдан інфо» (vk.com/public14998340);
14. «Євромайдан» (vk.com/club51435034);
15. «Львів Київ Українська революція Євромайдан» (vk.com/public47332318);
16. «Україна - це Європа! ЄС (Євромайдан)» (vk.com/public34260519);
17. «Євромайдан Революція» (vk.com/public51332282);
18. «Українці за Європу Євромайдан Ревлююція» (vk.com/public38314697);
19. «Євромайдан Революція» (vk.com/public34163024);
20. «Євромайдан» (vk.com/club25810863);
21. «Наше українське 2013 Євромайдан» (vk.com/public36015532);
22. «Євромайдан Live (з перших уст)» (vk.com/public55297091);
23. «Євромайдан Львів-Київ (Live)» (vk.com/club27979665);
24. «Євромайдан Львів» (vk.com/club61715216);
25. «НЕТОЛЕРАНТНІ Євромайдан Провокатори і фошисти» (vk.com/public54326580);
26. «Євромайдан шлях до Європи!» (vk.com/public36448113);
27. «ЄвроМайдан Харків» (vk.com/club39195816);
28. «Євромайдан» (vk.com/public51078083);
29. «Україна Євромайдан Революція» (vk.com/public36792792);
30. «Я Люблю Усе Українське [ЄвроМайдан]» (vk.com/club25132438);
31. «Євромайдан 2013» (vk.com/club57192816);
32. «євромайдан РЕВОЛЮЦІЯ» (vk.com/public45263365);
33. «Євромайдан Viva la Revolucion!» (vk.com/public57366851);
34. «Україна - це, Європа!!! Євромайдан!!» (vk.com/club27826619);
35. «Україна - це Європа! ЄС (EUkraine) Євромайдан» (vk.com/club35267039);
36. «ВК-не життя. СП-не почуття. Українська революція» (vk.com/public49376628);
37. «Революція Веселої та сильної України» (vk.com/public42390703);
38. «МИ - ПАТРІОТИ УКРАЇНИ» (vk.com/club5525046);
39. «Лелека» (vk.com/club54496611).

Начальник оперативного подразделения С.А.Поляков

УФСБ России по г. Санкт-Петербургу и Ленинградской области
Для пакетов № 50

Figure 1. The leaked FSB order to VKontakte CEO Pavel Durov to hand over information about pro-Ukrainian groups

to control the transmission infrastructure in Crimea. Russian soldiers – famously having removed nationality and rank insignia from their uniforms – secured infrastructure, such as TV and radio stations, as well as mobile phone operators (Ukrtelekom, 2014). Information content was equally important. The Maidan movement and the new Kiev government were demonised, for example by the publication of allegedly authentic e-mails showing that the new Ukrainian leaders were puppets of the West. Whoever was behind the publications (*Anonymous Ukraine* could be anyone), the stories were covered prominently in Russian state-controlled media (The Voice of Russia, 2014). In the area of operations, journalists were harassed. Non-military Russian government agencies also actively sought to control the information environment, e.g. the social network *VKontakte*. In December 2013, the FSB ordered it to deliver intelligence on pro-Ukrainian groups. *VKontakte* CEO and founder Pavel Durov claims to have refused, and later posted the orders online, as depicted in Figure 1. He later resigned and left Russia, accusing the government of a hostile takeover of *VKontakte*. All these measures are in line with the idea of a sovereign Russian information space (compare the draft “Convention on international information security”) that has to be defended.

In March 2014, the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) blocked the Internet resources of pro-Ukrainian groups (Roskomnadzor, 2014b). Similar blockings also befell the websites of prominent Russian opposition leaders such as Aleksei Navalnyi, already under house arrest, and Garry Kasparov (Roskomnadzor, 2014a).

However, the most striking feature remains the coordination between different activities. For example, the messages sent by the Russian political leadership, through diplomatic channels and through Russian state-controlled international media such as RT, were supported by leaked phone calls allegedly featuring American (BBC, 2014) and Estonian (Reuters, 2014) diplomats. The interception of such calls suggest that competent signals intelligence capabilities were used to gain media coverage and sow doubt and uncertainty in the West. Sometimes information distributed by Russia was spread on social media and subsequently picked up by traditional media. For example, a map of alleged protests against the Ukrainian government posted by the Russian diplomatic mission to NATO was reprinted in Swedish newspaper *Svenska Dagbladet* along with the observation that there was a propaganda war ongoing. All of these actions correspond quite closely to the ideas of mass media war expressed in the "Concept for the security of the society of the Russian Federation" (Government of Russia, 2013) and the information security doctrine (Government of Russia, 2000).

One useful perspective on the information warfare aspect of the illegal annexation of Crimea is the OODA – Observe, Orient, Decide, Act – loop, often used to describe the elements of military command and control. This is a key concept in manoeuvre warfare, where the two opposing sides each go through the OODA loop over and over again. If one of them is slower than the other, he will fall further and further behind, making his decisions increasingly obsolete and eventually rendering his command and control capability useless (Widén and Ångström, 2005, p. 189). On this interpretation, information warfare is largely about decelerating the opponent's progression through the OODA loop (and accelerating one's own).

In the *observe* phase, measures were deliberately taken to make it difficult for outside spectators to see what was going on. Time was wasted trying to understand blatant lies, such as the denial of the "little green men" being Russian forces.

Considering the *orient* phase, the large-scale military exercise close to the Ukrainian border served as a diversion that attracted attention away from Crimea and made it more difficult to understand what was going to happen. Another factor that made orientation harder (later broadly employed in eastern Ukraine) was the use of proxies and new actors to sow confusion. Russia did not annex

Crimea directly, but had the regional parliament elect a new prime minister at gunpoint, who could then apply for membership in the Russian Federation.

As for the *decide* phase, it is interesting to note how the use of fait accompli can force an opponent to start over again in the OODA loop. Russia projected the image of the annexation of Crimea as being irreversible both militarily and politically. Another interesting aspect is how unexpected or unconventional methods were used to raise the threshold for making certain decisions. Russian special forces managed to take key terrain and objects in Crimea without (much) bloodshed. This made it much harder for the Ukrainian government to respond with decisive military force (as happened later, in eastern Ukraine). By acting unconventionally, Russia managed to shift the potential burden of proof and raise the threshold for all-out military defensive action.

Arguably, the *act* phase is the most difficult to affect using information warfare. Perhaps the communications and control phases of Kuznetsov et al. are more appropriate because communications and control can be severed, for example by taking control of key communications nodes, as was quickly done in Crimea.

To summarise, information warfare broadly construed played an important part in the success of the Crimean operation. Communications nodes were taken over, Crimea was cut off from the rest of the world, and a massive campaign was directed towards the international community to legitimise the annexation (Søgard and Hagen, 2014). Indeed, the Russian pattern of action during the illegal annexation of Crimea adheres quite closely to the official characterisations of information warfare:

> The early use of information warfare to achieve political goals without using military force, and its later use to create a positive reaction within the international community to the use of military force (Government of Russia, 2010, § 13.g)
>
> to undermine political, economic and social systems, to destabilise a society and a state by massive psychological influence on the population, and also putting pressure on a state to make decisions that are in the interest of the opponent (Ministry of Defence of the Russian Federation, 2011, § 1)
>
> Mass media use by foreign special services, operating on the territory of the Russian Federation, to decrease the defence capabilities of the country and the security of the state, and the spreading of disinformation (Government of Russia, 2000, section 6).

The measures taken internally in Russia and externally towards Ukraine and Western countries are best understood as a single, unified information warfare campaign.

4.4 The messages sent by military flights

In the analysis of the annexation of Crimea above, four different uses of the Armed Forces were identified. However, yet another way of using military means is strategic messaging or signalling. This is particularly evident in peacetime, when there is, so to speak, no tactical situation, but all military posturing can be assumed to be a matter of delivering strategic messages.

Though not explicitly articulated, this can be seen in Gerasimov's discussion of the role of non-military methods in modern conflicts (Gerasimov, 2013). According to his model, strategic deterrence is a military measure, but for such measures to be effective they need to be converted into political and diplomatic pressure. The way to do this, of course, is to make sure to deliver the message to those that are to be pressured. Information warfare is the unifying strand that connects the military and non-military means.

To take a concrete example, consider recent exercise patterns of Russian military aircraft. To name but a few events, Russian Tu-95 Bear-H bombers exercised off the coasts of Alaska and California in June 2014 (Lendon, 2014), and again off Alaska and Canada in September 2014, this time entering the US Air Defense Identification Zone (Brusk and Ellis, 2014). In late October 2014, NATO tracked Russian strategic bombers over the Atlantic, the Black Sea and the Baltic, noting that they represented an unusual level of air activity (Macdonald, 2014). The list goes on – and it is a long one. In November 2014, the European Leadership Network released a policy brief listing almost 40 close military encounters between Russia and the West in 2014 (Frear et al., 2014).

In Sweden, the Armed Forces and the National Defence Radio Establishment (FRA) stated in early October 2014 that for the past six months Russian fighters had been acting in a much more aggressive way, flying very close to Swedish signals intelligence aircraft in international airspace (Swedish National Defence Radio Establishment (FRA) and Swedish Armed Forces, 2014). Figure 2 shows a photograph released from such an encounter.

From an information warfare point of view, it is worth stressing that this kind of activity in the air is not carried out in a vacuum. In planning and conducting these exercises, the Russian political and military leadership are well aware that they will be observed and interpreted by political and military leaders of other countries, as well as reported on and analysed in the media. These activities send messages of Russian strength, resolve and military capability – not necessarily on their own, but certainly when combined with other means, such as tough diplomatic talk, into an integrated whole. Such messaging is yet another way of using military measures – in operations other than (traditional) war – for information warfare.

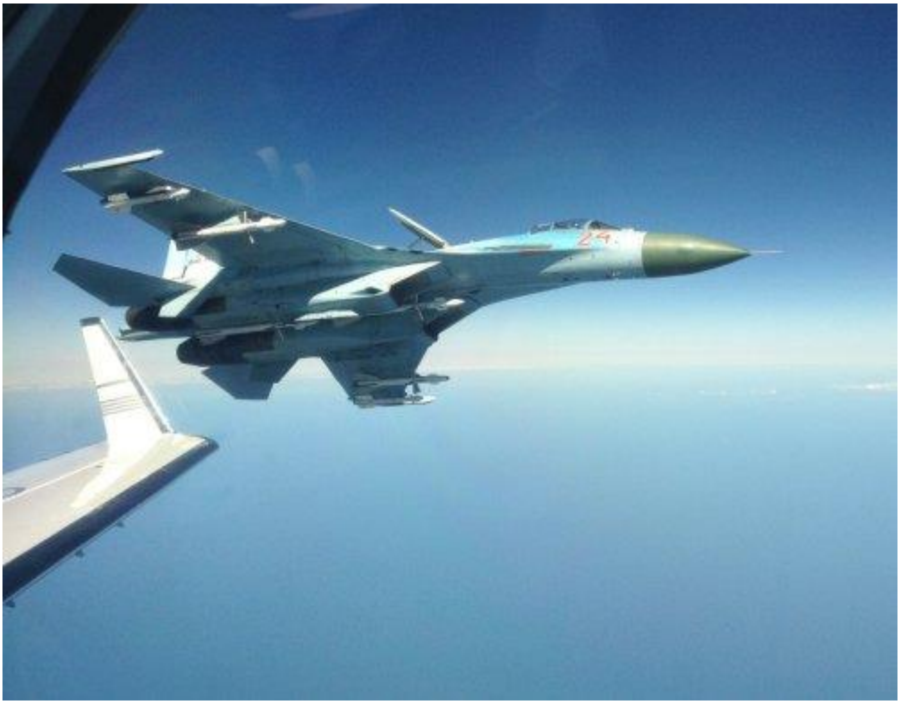


Figure 2. A photograph released by the Swedish National Defence Radio Establishment (FRA), showing a Russian Su-27 fighter aggressively close to a Swedish signals intelligence aircraft in international airspace

4.5 Internet control and censorship

The elections in 2011–2012 in Russia sparked waves of protests – the largest since the fall of the Soviet Union – where a lot of political usage of the Internet could be observed (Franke and Vendil Pallin, 2012). Following Putin's re-election as president in 2012, however, the political system has become more authoritarian, and a number of measures have been taken to ensure that similar protests and domestic upheaval do not occur again. A number of laws clearly aimed at stifling dissent on the Internet have been enacted, ranging from mandatory warnings with age limits on web pages, a "blacklist" of forbidden Internet resources maintained by Roskomnadzor and harsher laws on libel in 2012 (Franke and Vendil Pallin, 2012) to registration requirements for bloggers with a readership above a certain size in 2014 (Persson and Vendil Pallin, 2014), thus removing the possibility of anonymity. Freedom House, in their annual report on Internet freedom, note an increase in the number of criminal prosecutions of online users, as well as increased legal and extra-legal harassment of regular users and activists, driving Internet activists to flee Russia for other countries (Kelly et al., 2013). A few additional aspects were discussed above in the context of the annexation of Crimea.

This development is unsurprising, given the emphasis on maintaining social stability and regime security found for instance in the draft Convention on international information security (Ministry of Foreign Affairs of the Russian Federation, a) and in Streltsov (2011), as well as the fear of extremist use of the Internet expressed by Antonovich (2011) and in the "Concept for the security of the society of the Russian Federation" (Government of Russia, 2013) as well as Priakhin's call for government control of important mass media (Priakhin, 2009). That these measures are indeed considered part of an ongoing information war of "massive psychological influence on the population" is also evident from the conceptual views of the Ministry of Defence (Ministry of Defence of the Russian Federation, 2011). The perceived enemy is identified in the information security doctrine (Government of Russia, 2000, section 6): expansion of the foreign media in Russia and mass media being used by foreign special services to spread disinformation and to decrease Russian defence capabilities and state security.

In such a war, freedom of expression or of the media carries little weight. Freedom House has rated Russia "non-free" in terms of press freedom ever since 2003 (Deutsch Karlekar and Dunham, 2014).

In the realm of the Internet, Russia seems bent on pursuing a sovereign information space, wherein no outside actors can disseminate any kind of information to the Russian population without the approval of the authorities, i.e. the incumbent political leadership.

5 Conclusions

Based on the review of official documents and military theory, as well as the case studies, we now proceed to make some important observations and draw some tentative conclusions.

Initially, it is worth remarking that everyone is struggling with information operations terminology. The Russian debate on information warfare is filled with attempts to offer conclusive and enlightening definitions, but the fact that this has gone on for years suggests that it is less than successful. The Russian debate is also fuelled by the Western debate – *Voennaia mysl* is full of articles analysing the doctrinal developments of US and NATO information operations doctrines (a recent example is Goncharov and Artamonov, 2014).

One important observation is that information warfare is not only a matter for the Armed Forces, or the Ministry of Defence. Rather, it is repeatedly stressed in official documents, as well as in military theory, that the resources of many different government agencies need to come together to wage successful information war. But, while many authors stress the coordination of all available state resources, they are not as forthcoming with describing the relevant agencies. However, it stands to reason that some key players are the Federal Security Service (FSB), the Foreign Intelligence Service (SVR), the Armed Forces, the Military Intelligence Service (GRU), the IT and mass media supervision service Roskomnadzor, the Federal Protection Service (FSO), and the Ministry for Foreign Affairs. If this is indeed the case, then coordination of these agencies must come from the highest political level, i.e. through the Russian National Security Council (which is part of the Presidential Administration). A reasonable hypothesis is that the National Security Council has the mandate to decide whether a particular operation is to be conducted, but then delegates operational lead to one of the agencies, probably most often the FSB. As for the role of the Armed Forces, it remains to be seen what division of labour will be established between the new National Defence Control Centre and the other parts of the General Staff.

Another key observation is that information warfare, according to doctrine and theory, is conducted continuously in peacetime and wartime alike. For example, in peacetime, foreign political leaders can be discredited, messages can be sent by aggressive use of military flights, and the Russian outlook on world events can be projected outwards using dedicated media outlets in foreign languages.

Another observation that can be made from the official documents is that the influence and the technical aspects (e.g. cyberwarfare) are almost always considered as part of a greater unified whole of information warfare.

However, these observations about the close coordination of different resources and the integrated approach come with caveats. It is clear that the traditional military electronic warfare (EW) service feels left out, and fears that it will not play an important role in future information warfare capabilities. Russian information warfare capabilities should thus not be considered monolithic – clearly there are vested interests working to favour certain solutions.

It is also interesting to note how politicised information warfare has become. Though there are military theorists who deliberately delimit themselves to the battlefield in a way that is reminiscent of the Western Command and Control Warfare (C2W) and Revolution in Military Affairs (RMA) concepts, the Russian intellectuals taking part in the military theory debate now embrace a view of information warfare where regime security is paramount. Indeed, one might say that state security and regime security have fused. Streltsov probably offers the best articulation of this position. Whereas in a democracy it is not a matter of national security that the incumbent leadership has high approval ratings or is re-elected, in Russia this is precisely the case. Streltsov explicitly argues that maintaining a positive image of the state and its leaders is a key information warfare task (p. 23). As a very rough slogan, one might say that traditional military theorists speak of information warfare as a means to attain information superiority over the enemy, whereas official documents and theorists like Streltsov focus more explicitly on regime security. A tendency for the military establishment increasingly to be adopting the latter perspective can be perceived in the new military doctrine (Government of Russia, 2014), in its description of how traditional military operations can be combined with the “protest potential of the population”.

Having made these observations about the Russian view of information warfare, it is natural to ask why it looks the way it does. Though these kinds of questions are notoriously hard to answer in a definite manner, a few tentative observations can still be made. First, it seems that one important driver is a persistent view of international relations as a zero-sum game, in which a security gain for someone is necessarily a security loss for someone else. Second, there seems to be a perception among the Russian intellectuals who have influenced the view of information warfare that Russia is lagging behind other countries in terms of technology. Hence the concern with “leading foreign countries aiming to achieve overwhelming superiority in the military sphere” in the national security strategy. In other words, everything is defined in terms of threats, whereas opportunities are rarely seen. Third, there is distrust of economic globalisation and interdependence as means to foster peace and prosperity (Chekinov and Bogdanov, 2011). Fourth, there is a belief – undoubtedly forced upon anyone who acts within the increasingly authoritarian Russian state apparatus – that the incumbent political leaders and systems are always the best. Fifth, the Soviet legacy is distinctly visible in the way the domestic media have been curbed, and in the barrage of new measures to control the Internet (Franke and Vendil Pallin, 2012, Kelly et al., 2013). This increasingly isolationist and authoritarian strategy might also create an unwanted feedback loop in which Russia falls ever further behind technologically and economically (the second observation above), which then motivates even harsher measures.

It is tempting to polemicise against many of these beliefs, pointing out that free trade in telecommunications fosters growth and prosperity (Mattoo et al., 2006), that attempts to maintain social stability by force might in the end lead to massive blowups making everyone worse off (Taleb and Blyth, 2011) or even that too much nationalism diminishes government effectiveness (Ahlerup and Hansson, 2011). However, it is important to realise that in the shaping of policy perceptions and threat assessments matter as much as facts. If the Russian political leadership firmly believes that the world is a zero-sum game where everyone is out to get them, they will act accordingly – and to some extent *make* the world such a game.

6 References

Ahlerup, P. and Hansson, G. (2011). Nationalism and government effectiveness. *Journal of Comparative Economics*, 39(3):431–451.

Antonovich, P. I. (2011). O sushchnosti i soderzhanii kibervoiny [On the essence and contents of cyberwar]. *Voennaia mysl*, (7):39–46.

Bagirov, R. Z. (2009). *Politicheskaia kommunikatsiia v obespechenii voennoi bezopasnosti Rossiiskoi federatsii [Political communication in the safeguarding of the military security of the Russian Federation]*. PhD thesis. Military University, Moscow.

Balybin, V. A., Donskov, Y. Y., and Boiko, A. A. (2013). O terminologii v oblasti radioelektronnoi borby v usloviiakh sovremennogo informatsionnogo protivoborstvo [On the terminology of electronic warfare in modern information warfare]. *Voennaia mysl*, (9):28–32.

Bazylev, S. I., Dylevskii, I. N., Komov, S. A., and Petrunin, A. N. (2012). Deiatelnost Vooruzhennykh Sil Rossiiskoi Federatsii v informatsionnom prostranstve: printsipy, pravila, mery doveriia [The activities of the Armed Forces of the Russian Federation in the information space: Principles, rules, confidence-building measures]. *Voennaia mysl*, (6):25–28.

BBC (2014). Ukraine crisis: Transcript of leaked Nuland-Pyatt call. http://-www.bbc.com/news/world-europe-26079957 (accessed October 14, 2014).

Brusk, S. and Ellis, R. (2014). Russian planes intercepted near U.S., Canadian airspace. CNN, http://edition.cnn.com/2014/09/19/us/russian-plane-incidents/ (accessed October 30, 2014).

Chekinov, S. G. and Bogdanov, S. A. (2011). Vliianie nepriamykh deistvii na kharakter sovremennoi voiny [The influence of indirect actions on the character of modern war]. *Voennaia mysl*, (6):3–13.

Chibisov, I. N. and Vodkin, V. A. (2011). Informatsionno-udarnaia operatsiia [The information shock operation]. *Armeiskii sbornik*, (3):46–49.

Darczewska, J. (2014). *The anatomy of Russian information warfare. The Crimean operation, a case study*. Centre for Eastern Studies, Warsaw. Point of View No. 42.

Deutsch Karlekar, K. and Dunham, J., editors (2014). *Freedom of the Press 2014*. Freedom House.

Ennis, S. (2013a). Putin’s RIA Novosti revamp prompts propaganda fears. BBC, http://www.bbc.com/news/world-europe-25309139 (accessed October 30, 2014).

Ennis, S. (2013b). Russia: Children’s toilet TV show drawn into Ukraine-EU row. BBC, http://www.bbc.com/news/blogs-news-from-elsewhere-25198264 (accessed October 30, 2014).

European Commission and EEAS (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, High representative of the European Union for foreign affairs and security policy. Joint communication to the European parliament, the Council, The European Economic and Social committee and the Committee of the Regions, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed October 13 2014).

Franke, U. (2013). On the cyber-reputation of governments. *International Review of Information Ethics*, 19:66–71.

Franke, U. and Vendil Pallin, C. (2012). *Russian Politics and the Internet in 2012*. FOI, the Swedish Defence Research Agency, Stockholm. FOI-R--3590--SE.

Frear, T., Kulesa, L., and Kearns, I. (2014). *Dangerous Brinkmanship: Close Military Encounters Between Russia and the West in 2014*. European Leadership Network.

Gerasimov, V. V. (2013). Tsennost nauki v predvidenii [The value of science in forecasting]. *Voenno-Promyshlennyi Kurer*, (8):2–3.

Giles, K. (2011). “Information Troops” – A Russian Cyber Command? In *Cyber Conflict (ICCC), 2011 3rd International Conference on*, pp. 45–60. IEEE.

Giles, K. (2012). Russia’s public stance on cyberspace issues. In *Cyber Conflict (CYCON), 2012 4th International Conference on*, pp. 63–75. IEEE.

Giles, K. and Hagestad, W. (2013). Divided by a common language: Cyber definitions in Chinese, Russian and English. In *Cyber Conflict (CyCon), 2013 5th International Conference on*, pp. 413–429.

Godwin III, J. B., Kulpin, A., Rauscher, K. F., and Yaschenko, V., editors (2014). *Critical Terminology Foundations 2*. EastWest Institute and the Information Security Institute at the Moscow State University.

Goncharov, S. V. and Artamonov, N. F. (2014). Dostizhenie informatsionno-psikhologicheskogo prevoskhodstva v sovremennykh boevykh deistviiakh (po vzgliadam rukovodstva armii SShA) [Reaching information-psychological superiority in modern military operations (according to the views of the US military leadership)]. *Voennaia mysl*, (6):61–69.

Gorbenko, A. N. (2009). *Informatsionnoe protivoborstvo v politike sovremennykh gosudarstv [Information warfare in the politics of modern states]*. PhD thesis. Military University, Moscow.

Government of Russia (2000). Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii [Information security doctrine of the Russian Federation]. http://-www.scrf.gov.ru/documents/6/5.html (accessed August 19, 2014). Signed into effect by President Vladimir Putin.

Government of Russia (2009). Strategiia natsionalnoi bezopasnosti Rossiiskoi Federatsii do 2020 goda [National security strategy of the Russian Federation up to 2020]. http://www.scrf.gov.ru/documents/1/99.html (accessed February 21, 2013). Signed into effect by President Dmitrii Medvedev.

Government of Russia (2010). Voennaia doktrina Rossiiskoi Federatsii [Military doctrine of the Russian Federation]. http://www.scrf.gov.ru/documents/18/-129.html (accessed August 18, 2014). Signed into effect by President Dmitrii Medvedev.

Government of Russia (2013). Kontseptsiia obshchestvennoi bezopasnosti Rossiiskoi Federatsii [Concept for the security of the society of the Russian Federation]. http://www.scrf.gov.ru/documents/16/117.html (accessed August 19, 2014). Signed into effect by President Vladimir Putin.

Government of Russia (2014). Voennaia doktrina Rossiiskoi Federatsii [Military doctrine of the Russian Federation]. http://www.scrf.gov.ru/documents/18/-129.html (accessed February 5, 2015). Signed into effect by President Vladimir Putin.

Johnsson, M. (2011). NATO and the challenge of strategic communication. Research paper produced under the NDC Fellowship Programme, NATO Defence College, Italy.

Kelly, S., Truong, M., Earp, M., Reed, L., Shahbaz, A., and Greco-Stoner, A., editors (2013). *Freedom on the net 2013: a global assessment of internet and digital media*. Freedom House.

Kiselev, D. (2013). Sammit “Vostochnoe partnerstvo” [The summit of the “Eastern partnership”]. *Vesti Nedeli*, Rossiia 1, http://vesti7.ru/news?id=41805 (accessed October 30, 2014).

Kuznetsov, V. I., Donskov, Y. Y., and Korobeinikov, A. S. (2013). O sootnoshenii kategorii “radioelektronnaia borba” i “informatsionnaia borba” [On the relation between “electronic warfare” and “information warfare”]. *Voennaia mysl*, (3):14–20.

Kuznetsov, V. I., Donskov, Y. Y., and Nikitin, O. G. (2014). K voprosu o roli i meste kiberprostranstva v sovremennykh boevykh deistviiakh [On the question of the role and place of cyberspace in modern military operations]. *Voennaia mysl*, (3):13–17.

Lendon, B. (2014). Russian bombers fly near California. CNN, http://-edition.cnn.com/2014/06/13/us/u-s-russia-military-flights/ (accessed October 30, 2014).

Lozansky, E. (2014). ‘Slam dunk journalism’ or propaganda warfare? RT, http://-rt.com/op-edge/175548-foreign-policy-us-russia-journalism/ (accessed October 30, 2014).

Macdonald, A. (2014). NATO jets track ‘unusual’ Russian bomber sorties. Reuters, http://www.reuters.com/article/2014/10/29/us-nato-russia-exercises-idUSKBN0II27S20141029 (accessed October 30, 2014).

MacDonald, B. (2014). Goodbye to Carl Bildt, out of line and out of time. RT, http://rt.com/op-edge/182600-bildt-swiss-far-right-ukraine/ (accessed October 30, 2014).

Mattoo, A., Rathindran, R., and Subramanian, A. (2006). Measuring services trade liberalization and its impact on economic growth: An illustration. *Journal of Economic Integration*, 21(1):64–98.

Ministry of Defence of the Russian Federation (2011). Kontseptualnye vzgliady na deiatelnost vooruzhennykh sil Rossiiskoi Federatsii v informatsionnom prostranstve [Conceptual views on the activities of the Armed Forces of the Russian Federation in the information space]. http://ens.mil.ru/science/-publications/more.htm?id=10845074cmsArticle (accessed February 20, 2014).

Ministry of Foreign Affairs of the Russian Federation (a). Convention on international information security (Concept). http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/-7b17ead7244e2064c3257925003bcbcc!OpenDocument (accessed September 25, 2014).

Ministry of Foreign Affairs of the Russian Federation (b). Konventsiia ob obespechenii mezhdunarodnoi informatsionnoi bezopasnosti (kontseptsiia) [Convention on international information security (Concept)]. http://-www.scrf.gov.ru/documents/6/112.html (accessed September 25, 2014).

NATO (2009). *NATO Bi-SC Information Operations Reference Book, version 1.3*. NATO.

Norberg, J., Franke, U., and Westerlund, F. (2014). The Crimea Operation: Implications for Future Russian Military Interventions. In Granholm, N., Malminen, J., and Persson, G., editors, *A Rude Awakening. Ramifications of Russian Aggression Towards Ukraine*. FOI, the Swedish Defence Research Agency, Stockholm. FOI-R--3892--SE.

Nye, J. S. (1990). *Bound to lead: The changing nature of American power*. Basic Books.

Persson, G. (2013a). *Russian History – A Matter of National Security*. FOI, the Swedish Defence Research Agency, Stockholm. RUFS Briefing No. 19, August.

Persson, G. (2013b). Security Policy and Military Strategic Thinking. In Hedenskog, J. and Vendil Pallin, C., editors, *Russian Military Capability in a Ten-Year Perspective – 2013*. FOI, the Swedish Defence Research Agency, Stockholm. FOI-R--3734--SE.

Persson, G. (2014). Russian Influence and Soft Power in the Baltic States: the View from Moscow. In Winnerstig, M., editor, *Tools of Destabilization – Russian Soft Power and Non-military Influence in the Baltic States*. FOI, the Swedish Defence Research Agency, Stockholm. FOI-R--3990--SE.

Persson, G. and Vendil Pallin, C. (2014). The View From Russia. In Granholm, N., Malminen, J., and Persson, G., editors, *A Rude Awakening. Ramifications of Russian Aggression Towards Ukraine*. FOI, the Swedish Defence Research Agency, Stockholm. FOI-R--3892--SE.

Priakhin, A. M. (2009). *Moralnyi dukh possiiskoi armii kak obiekt Informatsionnogo protivoborstva [The moral spirit of the Russian army as an object of information war]*. PhD thesis. Military University, Moscow.

Reuters (2014). Estonia denies leaked call implicates Ukraine protesters in killings. http://www.reuters.com/article/2014/03/05/us-estonia-eu-ukraine-idUSBREA2423O20140305 (accessed October 14, 2014).

Roskomnadzor (2014a). Ogranichen dostup k riadu internet-resursov, rassprostraniavshikh prizyvy k nesanktsionirovannym massovym meropriiatiiam [Limited access to a number of Internet resources that have called for illegal mass action]. http://rkn.gov.ru/news/rsoc/news24447.htm (accessed October 14, 2014).

Roskomnadzor (2014b). Po trebovaniu Generalnoi prokuratory RF prekrachen dostup k soobshchestvam ukrainskikh natsionalisticheskikh organizatsii v sotsialnoi seti “VKontakte” [Following a request from the prosecutor general of the Russian Federation, access has been limited to the communities of Ukrainian nationalist organisations on the social network “VKontakte”]. http://rkn.gov.ru/-news/rsoc/news24185.htm (accessed October 29, 2014).

Saifetdinov, K. I. (2014). Informatsionnoe protivoborstvo v voennoi sfere [Information warfare in the military realm]. *Voennaia mysl*, (7):38–41.

Søgard, H. A. and Hagen, J. M. (2014). *FFI-fokus: Kampen om sannheten [The fight for truth]*. Forsvarets forskningsinstitutt, Oslo.

Starodubtsev, Y. I., Bukharin, V. V., and Semenov, S. S. (2012). Tekhnosfernaia voina [War in the technological realm]. *Voennaia mysl*, (7):22–31.

Streltsov, A. A. (2011). Osnovnye zadachi gosudarstvennoi politiki v oblasti informatsionnogo protivoborstvo [The main tasks for government policy in information warfare]. *Voennaia mysl*, (5):18–25.

Swedish National Defence Radio Establishment (FRA) and Swedish Armed Forces (2014). FRA och Försvarsmakten bekräftar närgånget uppträdande av ryskt flyg [FRA and the Armed Forces confirm obtrusive behaviour from Russian aircraft]. http://www.fra.se/snabblankar/nyheterochpress/nyhetsarkiv/-nyheter/-fraochforsvarsmaktenbekraftarnargangetupptradandeavrysktflyg.235.html (accessed October 30, 2014).

Taleb, N. N. and Blyth, M. (2011). The Black Swan of Cairo: How Suppressing Volatility Makes the World Less Predictable and More Dangerous. *Foreign Affairs*, 90:33.

The Federation Council (2014). Kontseptsiia strategii kiberbezopasnosti Rossiiskoi Federatsii [Concept for a Cybersecurity Strategy for the Russian Federation]. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (accessed January 20, 2014).

The Voice of Russia (2014). Anonymous Ukraine releases Klitschko e-mails showing treason. http://voiceofrussia.com/news/2014_02_23/Anonymous-Ukraine-releases-Klitschko-e-mails-showing-treason-3581/ (accessed October 14, 2014).

Thomas, T. (2014). Russia’s information warfare strategy: Can the nation cope in future conflicts? *The Journal of Slavic Military Studies*, 27(1):101–130.

Ukrtelekom (2014). V AR Krym nevidomimi u viiskovii formi povtorno zablokovano dekilka vuzliv zviazku [In the Autonomous Republic of Crimea, unknown uniformed men have repeatedly blocked several communications nodes]. http://www.ukrtelecom.ua/presscenter/news/official?id=120389 (accessed October 14, 2014).

UN GA (2014). Developments in the field of information and telecommunications in the context of international security. http://www.un.org/-disarmament/topics/informationsecurity/ (accessed September 25, 2014).

Varfolomeev, A. A. (2012). Kiberdiversiia i kiberterrorizm: predely vozmozhnostei negosudarstvennykh subiektov na sovremennom etape [Cyber sabotage and cyber terrorism: limits of non-government actors at the present stage]. *Voennaia mysl*, (12):3–11.

Vorobev, I. N. (2007). Informatsionno-udarnaia operatsiia [The information shock operation]. *Voennaia mysl*, (6):14–21.

Widén, J. and Ångström, J. (2005). *Militärteorins grunder [Foundations of military theory]*. Försvarsmakten [Swedish Armed Forces], Stockholm.

7 Acronyms and abbreviations

C2	command and control
C2W	command and control warfare
EW	electronic warfare
FOI	Swedish Defence Research Agency (Totalförsvarets forskningsinstitut)
FRA	National Defence Radio Establishment (Försvarets radioanstalt)
FSB	Federal Security Service (Federalnaia sluzhba bezopasnosti)
FSO	Federal Protection Service (Federalnaia sluzhba okhrany)
GRU	Military Intelligence Service (Glavnoe Razvedovatelnoe Upravlenie)
ICT	information and communications technology
IT	information technology
IW	information warfare
NATO	North Atlantic Treaty Organization
OODA	Observe, Orient, Decide, Act
RUFS	Russian Foreign, Defence and Security Policy (FOI)
SVR	Foreign Intelligence Service (Sluzhba vneshnei razedki Rossiiskoi Federatsii)
UN	United Nations

War by non-military means

In the Russian view of modern war, information warfare is given a lot of weight. The modern, increasingly digital, media landscape and the rapid development of information and communication technologies have created a new playing field. Information warfare is rapidly becoming an integral part of modern conflicts, as recent events in Ukraine illustrate.

This report aims to explore the intellectual foundations and practical use of information warfare as seen by Russian military theorists and expressed in official doctrine and documents, as well as by examining a handful of case studies.

One conclusion is that information warfare is not considered to be just a matter for the Armed Forces, but rather a strategic matter that requires the coordination of many government agencies. Another conclusion is that information warfare, according to doctrine and theory, is conducted continuously in peacetime and wartime alike. Information warfare is also highly politicised, and the Russian intellectuals taking part in the military theory debate now embrace a view of information warfare where regime security is paramount. Among the driving forces for this is a view of the world as a zero-sum game, where globalisation is reducing Russian security, and where Russia lags behind Western countries in terms of technology.

The report and other FOI publications on Russia are available on the Russia studies' website: www.foi.se/russia

FOI

ISSN1650-1942

www.foi.se