FOI, Swedish Defence Research Agency, is a mainly assignment-funded agency under the Ministry of Defence. The core activities are research, method and technology development, as well as studies conducted in the interests of Swedish defence and the safety and security of society. The organisation employs approximately 1000 personnel of whom about 800 are scientists. This makes FOI Sweden's largest research institute. FOI gives its customers access to leading-edge expertise in a large number of fields such as security policy studies, defence and security related analyses, the assessment of various types of threat, systems for control and management of crises, protection against and management of hazardous substances, IT security and the potential offered by new sensors.

FOI
Swedish Defence Research Agency
Defence Analysis
SE-164 90 Stockholm

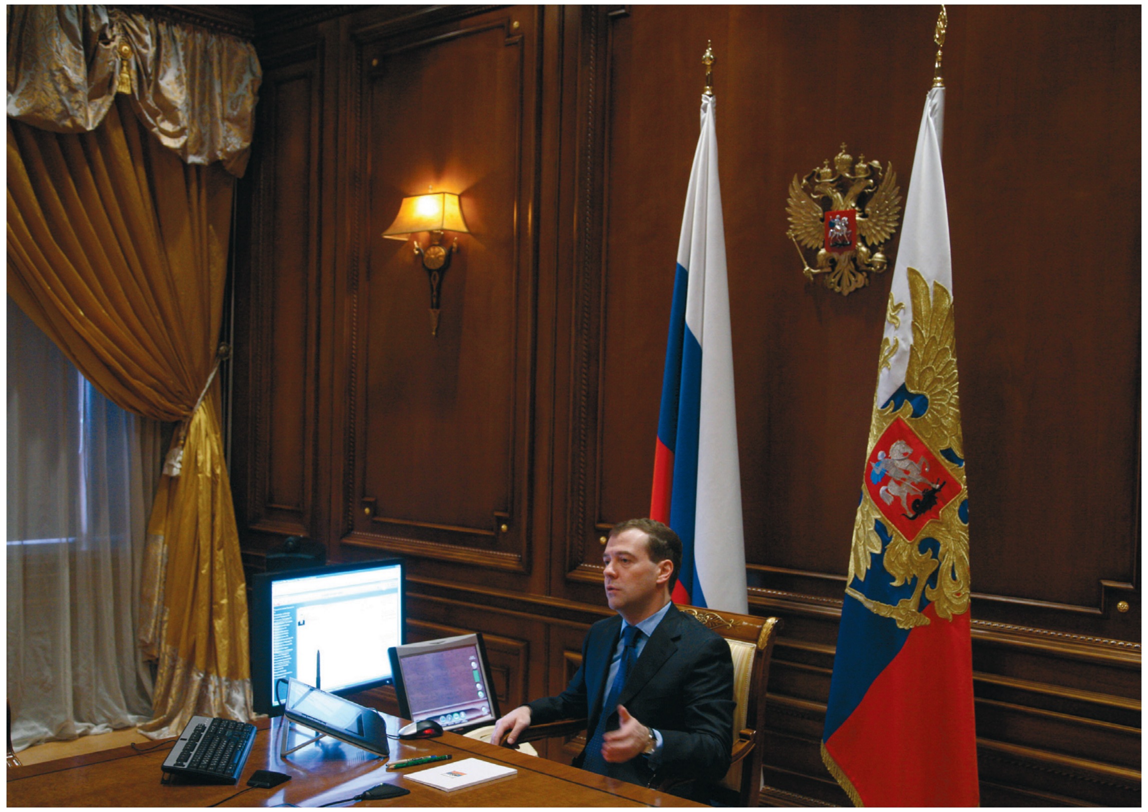
Phone: +46 8 555 030 00
Fax: +46 8 555 031 00

www.foi.se

FOI

Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations

ROLAND HEICKERÖ



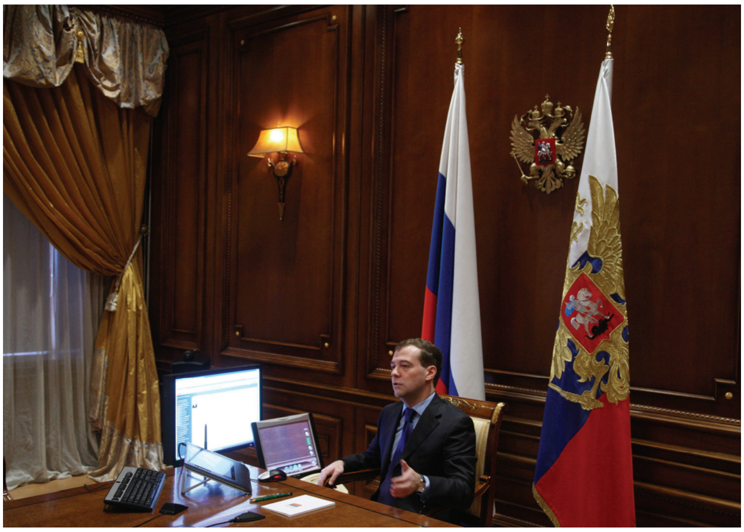
FOI-R--2970--SE
ISSN 1650-1942

User Report
March 2010

Defence Analysis

Roland Heickerö

Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations



Titel	Utveckling av cyberhot och den ryska synen på informationskrigföring och informationsoperationer
Title	Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations
Rapportnr/Report no	FOI-R--2970--SE
Rapporttyp Report Type	Användarrapport User Report
Månad/Month	March
Utgivningsår/Year	2010
Antal sidor/Pages	68 p
ISSN	ISSN 1650-1942
Kund/Customer	
Projektnr/Project no	A12001
Godkänd av/Approved by	

FOI, Totalförsvarets Forskningsinstitut	FOI, Swedish Defence Research Agency
Avdelningen för Försvarsanalys	Division of Defence Analysis
164 90 Stockholm	SE-164 90 Stockholm

Abstract

The objective of this report is to analyse Russian views on information warfare (IW) and information operations (IO). The goal is to get an overall picture of developments, and Russia's ambition and behaviour on the information arena. The report describes, analyses and discusses information operation doctrines and strategies. The organizations responsible for information warfare are examined. Examples are given of the driving forces behind and the resources required in developing IW capabilities. A short comparison is made between the Russian approach to information operations and the American and Chinese views in order to get a picture of the differences and similarities between the ways in which they interpret and use the IO concept. The text illustrates possible and likely malicious activities on the cyber arena that originate from Russia, such as cyber criminality and 'hacktivism'.

A short description is given of the Estonian cyber conflict in 2007, as well as the denial of service attacks and the website defacements directed against Georgia in 2008, in order to describe the development of a new modus operandi to conduct cyber operations on the Internet, used by different actors, and the potential implications of such a development. Other areas discussed in the report include the need for common criteria and agreements on how to behave in cyberspace in order to limit consequences of cyber attacks.

Key words: Russia, information warfare (IW), information operations (IO), cyber warfare, cyber attacks, hacktivism, cyber criminality, cyber regulations, Estonia cyber war, Georgia cyber attacks, SORM, Russian intelligence service, Russian secret service, Russian Business Network (RBN)

Summary

Cyberspace has become a decisive arena for modern warfare. It opens up new dimensions to conflicts with an inbuilt psychological impact. By using information warfare methods to attack an adversary's centres of gravity and critical vulnerabilities it is possible to win against an opponent, militarily as well as politically, at a low cost without necessarily occupying the territory of the enemy. Information warfare is viewed as a potent weapon for power projection to be used alone or in conjunction with military operations.

Like other major countries, Russia is developing capabilities for information warfare (IW) and information operations (IO). Within the Russian administration several organizations are responsible for handling information warfare capabilities including computer network operations, electronic warfare, psychological operations, deception campaigns (*maskirovka*) and mathematical programming impact. The latter could be interpreted as including the introduction of malware and malfunctions such as back-door functionalities and 'logic bombs'. The main organizations responsible for offensive and defensive cyber capabilities are most likely to be the FSO, the FSB and the GRU. The FSB is probably the authority responsible for information security for the Russian Federation.

The Russian approach to IW/IO differs to some extent from that of the Western countries as well as from the Chinese perspective. From the Russian point of view, information is per se a valuable asset, which it needs to protect in times of peace and war. In the information security doctrine of 2000, information protection has a strategic value and is seen as a key factor not only for the stability of the state but also for the regime and for influential and leading actors. In the Military Doctrine published in spring 2010, Russia notes the importance of information warfare during the initial phase of a conflict to weaken the command and control ability of the opponent and in the form of an information campaign during the actual battle to create a positive view within the international community.

Russia has been reported publicly several times over the years as not acting strongly enough against malicious activities in cyberspace originating from the country. The accusations involve a wide range of behaviours such as criminality on the Internet, cyber espionage and politically motivated hacking – so-called hacktivism. The critics

point out that the Russian law enforcement authorities have been reluctant to deal with the law-breakers. Two cases in particular have come up for discussion during recent years regarding cyber operations that might have emanated from Russia – the cyber assaults against Estonia in 2007 and on Georgia the year after. These incidents have been a wake-up call to highlight the risks, threats and vulnerabilities of information warfare. The operation directed against Estonia was one of the first official and publicly known cyber attacks against a country using large-scale botnets and distributed denial of service (DDoS) by nationalist-driven civilians. In the Georgian operation the methods were even refined further. There is no conclusive evidence of Russian government involvement in either case.

Both incidents show that a relatively small, skilled and dedicated group of individuals using social networks as tools for recruiting and for providing malware to the hackers can have a major impact. It set a standard for how future cyber conflicts could be conducted by proxy, including allowing actors deniability in combination with strategic benefits such as obtaining political goals.

The emerging cyber threats point to the need to improve both information security and international cooperation in order to hinder or reduce the negative effects of antagonistic cyber operations. Cyber aggression has jurisdictional and legal aspects. But there is a gap and a fundamental divergence between the Russian and the US views on the need to regulate hostile activities on the Internet. One conclusion is that the issue of cyber threats must be resolved on a worldwide scale, involving all major parties and the law enforcement agencies of all nations.

Acknowledgements

The RUFS (Russian Foreign, Defence and Security Policy) project at FOI focuses on Russia's military capability in a ten-year perspective viewed against a background of developments within several sectors of Russian society. These primarily include developments in Russian domestic, foreign and security policy, as well as democratic and economic developments, primarily focused on the defence economy. Another important area which the project is studying is the Russian view on information warfare and the development of capability for information operations.

For helpful comments and insights in Russian doctrines of information operations I would like to thank Mr Lars Nicander, director of CATS (the Center for Asymmetric Threat Studies) at the Swedish National Defence College. My gratitude is also due to Dr Carolina Vendil Pallin, project manager for RUFS, for accurate information and insightful comments, and Mr Fredrik Westerlund, as well as all the other participants in the Russian project.

Innehållsförteckning

1 Introduction

Russia has been reported publicly several times over the years as not acting strongly enough against malicious activities in cyberspace originating from the country. The accusations involve a wide range of behaviours such as criminality on the Internet, cyber espionage and politically motivated hacking – so-called hacktivism. Countries like Estonia and Georgia, among others, point out that organizations and groups related directly or indirectly to Russia are responsible for cyber attacks. Networks, servers and websites connected to critical infrastructures and information systems have been targeted by malicious software with viruses, worms and trojans. By using a large number of compromised computers and distributed denial of service (DDoS), the information flow has been hampered. In some cases networks and services have been forced to shut down for periods of time. The consequences for the parties attacked are severe.

The nature of the cyber arena makes it difficult to identify a specific aggressor. It is possible to hide digital traces as well as to put deceptive information on the Internet if you have the resources and knowledge. However, the *design* of trojans, worms or viruses might indicate that the malware originates from a specific environment and region.

Like other major countries, Russia is developing capabilities for information warfare (IW) and information operations (IO). IW/IO includes several types of capabilities such as computer network operations (CNO), electronic warfare (EW), psychological operations and deception activities. Different countries have their own interpretation of what should or should not be included in the term ‘IW/IO’. For instance, in some countries strategic communications, as well as controlling the mass media and the Internet, is seen as a part of defensive IO capabilities in order to protect the state. In other countries any attempts to censor or restrict public information flows would be regarded as very sensitive and be regulated by law. The official Russian view differs to some extent from that of the Western countries as well as from the Chinese perspective.

1.1 Objectives and goals

The objective of this report is to analyse Russian views on information warfare and information operations. The goal is to get an overall picture of developments and of Russia’s ambitions and behaviour on the information arena. The report describes, analyses and discusses information operation doctrines and strategies. The organizations responsible for information warfare are examined. Examples are given of the driving forces and the resources required in developing IW capabilities. A short comparison is made between the Russian approach to information operations and the US and Chinese views. The objective is to get a picture of the differences and similarities in the ways in which they interpret and use the IO concept. The text illustrates possible and likely malicious activities on the cyber arena that originate from Russia, such as cyber criminality and hacktivism.

A short description is given of the Estonian cyber conflict in 2007 as well as the denial of service attacks and the website defacements directed against Georgia in 2008. The purpose is to describe the development of a new modus operandi to conduct cyber operations on the Internet, used by different actors, and the potential implications of such a development. Other areas discussed in this report include the need for common criteria and agreements on how to behave in cyberspace in order to limit the consequences of cyber attacks.

1.2 Limitations

The implications of the development of IW capability are mainly examined here on a security policy level and not on a technical level. Regarding information operations, the study's main focus is on *computer network operations* what is usually called cyber war. Other capabilities, for instance electronic warfare and psychological operations, are not examined.

The Russian state's ambition to control the mass media is only briefly mentioned in the study. Information security as such, such as network, computer and information protection, has not been a subject for analysis.

1.3 Methodology

The method is based on information retrieval of open-source reports and documents as well as on Internet searches on mainly English-language websites. When Russian-language sources have been used, translations have been made using translation software. The number of open and relevant reports that explore Russian doctrines on information warfare and the development of IW capabilities are limited, at least in terms of non-Russian-language sources. In some cases the available information is based on secondary interpretations by Western scholars, thus involving the risk that the information may be biased. The material referred to may itself be part of an information operation aimed at influencing a specific audience.

Primary sources have been used as far as possible, including the Russian Military Doctrine from 2000 translated into English. One primary source is *Military Thought*, a journal covering Russian military policy, which is regarded as an official channel where high-ranking officers and military analysts present ideas and thoughts for a wider domestic and international audience. Other primary sources include conference papers authored by Russian state officials.

In some cases it has been difficult to verify the correctness of the open sources. The assessments of the reliability of the information used and the origin of the sources have been based on previous knowledge and experience from research into cyber warfare issues. Discussions have also been conducted with persons with good knowledge of Russian IW. Some of the reports referred to in the study were published in the mid-1990s and early 2000s, but they are considered to provide insights relevant for today's situation.

1.4 Outline

The Russian views on and definitions of information warfare and information operations are discussed in chapter 2. The chapter highlights issues such as information warfare in peacetime and wartime, how IW relates to deception (*maskirovka*), and differences between and similarities in the Russian, US and Chinese approaches to information operations. In chapter 3 the military and civilian organizations responsible for IW capabilities are examined.

The fourth chapter describes emerging cyber threats and the driving forces behind malicious activities such as cyber criminality and hacktivism. Chapter 5 discusses the evolution towards a new modus operandi for malicious activities by presenting two cases, the cyber attacks against Estonia and Georgia. The purpose of chapter 6 is to point out the need for cooperation on an international level to reduce tensions and the effects of cyber attacks. Finally, in chapter 7, some conclusions are drawn.

2 The Russian view on information warfare and information operations

The development of doctrines and strategies in a country must be understood in and related to a wider context. It is based on a whole range of factors and assumptions such as historical experiences, geographical tensions, varied military threats, the economic situation, ideological background, and technological standards, as well as the country's constitutional foundations – for instance, the type of leading actors and institutions. Russia is by no means an exception. With the end of the Cold War and the transition through the years of instability to a society based on a strong leadership, the 'strong state' of President Vladimir Putin has influenced mindsets.[1] For obvious reasons the modern Russian experience differs from the West's. This affects its military thinking in general and more specifically the views of information warfare.

Regarding doctrines and policy documents, there is as of today no open and official Russian doctrine specifically describing information operations and information warfare[2] that would correspond to the US Joint Pub 3-13,[3] the Joint Vision 2010 (JV-2010) and Joint Vision 2020 (JV-2020). In current US doctrine the purpose of IO is to influence, disrupt, corrupt or usurp an adversary's human and automated decision making while protecting its own. Information operations could be used offensively and defensively.

The Russian view regarding threats to its national sovereignty is described in doctrines and strategic documents such as the Military Doctrine[4] and the

[1] Hanson, S. (2001) 'Putin and the Dilemmas of Russia. Anti-Revolutionary Revolution', *Current History 333*

[2] The term 'information warfare' was first used by the USA and NATO within its C2W framework, on 2 December 1992, by the US Department of Defense. In *Information Operations*, Joint Publication 3-13, 13 February 2006, IW was removed as a term from the joint IO doctrine

[3] *Information Operations*, 13 February 2006 (updated version). IO is described as the integrated employment of electronic warfare (EW), computer network operations (CNO), military deceptions (MILDEC) and operation security (OPSEC) in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting a country's own. IO could be used offensively (IO-O) and defensively (IO-D). The doctrine is under review and a new doctrine will probably be defined during 2010

[4] *Voyennaia Doktrina Rossiiskoy Federatsii. Utverzhdena Ukazom Prezidenta RF ot 21 aprelya 2000 g. No. 706*, on the Internet: http://www.scrf.gov.ru/Documents/Decree/2000/706-1.html. It is referred to in Sokov, N. (2004) 'Russia's 2000 Military Doctrine'. Revised July 2004, on the Internet: http://nti.org/dbnisprofs/over/doctrine.htm (retrieved 11 December 2009)

Doctrine of Information Security of the Russian Federation,[5] both from 2000 and approved by the Security Council. Three types of military conflicts are identified as threats to Russia.[6] The first threat is the risk of a conflict escalating in the areas immediately surrounding the Russian borders. The second threat is the possibility of a direct confrontation with the USA and its Western alliances. The third threat is a possible conflict with an expansive China. The risk of the two latter occurring is considered as low.

In the Information Security Doctrine the security policy discourse extends into the domain of information. The document discusses information-related threats to Russia and how the state should act in order to guarantee the protection of strategically important information.[7] The doctrine could be viewed as a policy instrument primarily focused on Russian society but also intended to influence an international audience. In spring 2010, a new Russian Military Doctrine was published. In the doctrine Russia notes the importance of information warfare during the initial phase of a conflict to weaken the command and control ability of the opponent and then, in the form of an information campaign during the actual battle, to create a positive view within the international community.[8]

Although there is no defined and officially sanctioned doctrine on information warfare, there are of course a good many theories and much concept building done by leading scientists, analysts and military specialists. The Russians' views have been discussed publicly in scientific papers and conference presentations since the mid-1990s. They are considered as having some bearing on today's situation.

2.1 Views and definitions

The American analyst Colonel Timothy Thomas points out that there are several unique elements in Russia's approach to information warfare.[9] [10] [11]

[5] *Doktrina Informatsionnoi Bezopasnosti Rossiiskoi Federatsii.* on the Internet: http://www.scrf.gov.ro/Documents/Decree/2000/09-09. html (retrieved 6 December 2009). The document is translated and discussed for instance in Carman, D. (2002) 'Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass media and the politics of identity'. *Pacific Rim Law & Policy Journal Association*

[6] Leijonhielm, J., Hedenskog, J., Knoph, T., Larsson, R., Oldberg, I., Roffey, R., Tisell, M., Westerlund, F. (2008) 'Rysk militär förmåga i ett tioårsperspektiv – ambitioner och utmaningar' 2008. Användarrapport FOI-R-2707--SE (Stockholm, FOI)

[7] Carman (2002) Ibid,

[8] Vendil Pallin, C., Westerlund, F. (2010) 'Russia's Military Doctrine – Expected News'. *RUFS Briefing* no. 3, February. Swedish Defence Research Agency (Stockholm, FOI,)

[9] Thomas. T. (1996) 'Deterring Information Warfare: A new strategic challenge'. IWS - the Information Warfare Site. Reviewed 7 November 1996, on the Internet:

Due to lack of resources and budget constraints during the 1990s, in the aftermath of the Cold War, Russian scientists spent more time on IO theory than the West, with the latter focusing on practice over theory. But over time this could be advantageous. There is nothing as practical as good theories in the long term. There is also the possibility to learn from mistakes made by forerunners.

The Russian view on IW has been influenced by the debate on the Revolution in Military Affairs (RMA) during the 1980s and 1990s, as well as the concept building of network-centric warfare (NCW). The elements of the RMA could be summarized as precision strikes, concepts of information-led warfare (command and control warfare), and information dominance over the battlefield.[12]

The NCW concept involves a number of factors such as network-enabled capability by using networks, sensors and information more efficiently in order to coordinate and allocate resources, units and tasks.[13] Other parts are self-synchronization and improved situational awareness. One goal is to influence the opponents' decision process and thereby to control his actions. System thinking is a key factor in the NCW concept in the sense that an opponent could be viewed as a system with centres of gravity (CoGs) and critical vulnerabilities (CVs). By attacking the enemy's key critical systems such as its telecommunications, banking and financial systems, power grids and so on, using different means – both traditional weapons and IW – a system breakdown, and thus victory, could be achieved in a very short period of time.

http://www.iwar.org.uk/iwar/resources/parameters/iw-deterrence.htm (retrieved 16 November 2009)

[10] Thomas, T. (1998a) 'Dialectical versus Empirical Thinking: Ten key elements of Russian understanding of information operations'. *FMSO Special Study Center For Army Lesson Learned. Fort Leavenworth, KS 66027-1327*

[11] Thomas, T. (1998b) 'Russia's Information Warfare Structure: Understanding the roles of the Security Council, FAPSI, the State Technical Commission and the military', *European Security*, vol. 7, no. 1 (Spring), pp. 156–72

[12] Mowthorpe, M. (2005) 'The Revolution in Military Affairs (RMA): The United States, Russian and Chinese Views'. *University of Hull,* vol. 5, no. 2 (Summer)

[13] Alberts, D., Gartska, J., Stein, F. (1999) 'Network Centric Warfare: Developing and leveraging information superiority'. *CCRP. Publication services*. Revised August 1999 (2nd edition), on the Internet: http://www.dodccrp.org/files/Alberts_NCW.pdf (retrieved 15 November 2009)

One of the first persons to draw attention to the change to digitalized warfare was Marshal Nikolai Orgakov, chief of the Soviet General Staff in the 1980s. He used the term Military Technical Revolution (MTR) to describe the fundamental change from mass armies into technology-driven operations. The term 'MTR' was supplanted by the use of RMA by Pentagon officials.[14]

In line with Marshal Orgakov's vision, some Russian military analysts recognized that information technologies could be used as formidable weapons of the 21st century comparable to weapons of mass destruction.[15] [16] In coming conflicts there will be no clearly drawn battle lines and the fighting will take place in several dimensions and arenas. Warfare has shifted from being a duel of strike systems to being a duel of information systems. The arms race is moving into the sphere of software.[17] The analysts also viewed outer space as a potential theatre of military action. They declared the Gulf War of 1990–91 as the first technical operation. By using command and control warfare the Coalition forces succeeded in totally destroying the Iraqi communications and information infrastructure. To a great extent the Iraqi military equipment was Soviet-made. It was the wake-up call to Russia to change doctrines based on the old Cold War ideas.

The Afghanistan war of 1979–89 as well as the Chechnya war 1994–96 and the war started in 1999 have also influenced the Russian mindset and brought practical knowledge and insights to the Russian approach to IW. In particular the need to gain control over the information flow in and from a battlefield and its psychological impacts on the society has been identified as of supreme importance.[18] From a psychological warfare point of view Russia suffered severe problems in Afghanistan and failed to influence its adversaries.[19]

Both wars in Chechnya showed that in some areas even a small and relatively impoverished adversary could achieve information dominance over a stronger opponent by using the mass media component efficient. The Chechens

[14] Mowthorpe (2005) 'The Revolution in Military Affairs'

[15] Fitzgerald, M. (1994) 'Russian Views on Electronic Warfare. The growing role of information technology is rapidly lowering the barrier between war and peace'. Powerpoint pictures, on the Internet: http://www.nationalstrategies.com (retrieved 8 December 2009)

[16] Korotchenko, Y. and Plotnikov, N. (1994) 'Information is Also a Weapon: About what should not be forgotten when working with personnel', *Krasnaya Zvezda*, 17 February

[17] Fitzgerald, M. (1996) 'Russian Views on Information Warfare'. December 1996. *Hudson Institute.* Washington D.C, USA

[18] Thomas, T. (2003) 'Manipulating the Mass Consciousness: Russian & Chechen information war. Tactics in the second Chechen–Russian conflict'. 14 April, on the Internet: http://call.army.mil/fmso/fmsopubs/issues/chechiw.htm (retrieved 15 November 2009)

[19] Serookiy, Yu. (2004) 'Psychological-Information Warfare: Lessons of Afghanistan', *Military Thought*, vol. 13 no 1

were much more flexible than the Russian side in using the Internet and other tools to broadcast their view and to gain influence over public opinion. This was evident to the Russian military after the first war in Chechnya.

> The high effectiveness of 'information warfare' systems in combination with highly accurate weapons and 'non-military means of influence' makes it possible to disorganise the system of state administration, hit strategically important installations and groupings of forces, and affect the mentality and moral spirit of the population. In other words, the effect of using these means is comparable with the damage resulting from the effect of weapons of mass destruction.[20]

The US Congress Report of 2001 on cyber warfare[21] refers to V. I. Tsymbal[22] and points out that some Russian analysts rank the effects of cyber warfare (interpreted as computer and network operations) as second only to that of nuclear war. Several senior Russian military officers have supported the notion that

> …from a military point, the view of Information Warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict whether it will be causalities or not… considering the possible catastrophic use of information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces… Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself.[23]

[20] In a speech made by General Viktor Samsonov, chief of the Russian General Staff, 23 December 1996

[21] CRS Report for Congress. *Cyberwarfare.* Updated 19 June 2001, on the Internet: http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL30735_06192001.pdf (retrieved 20 November 2009)

[22] Tsymbal, V.I. (1995) 'Kontseptsiya Informatsionnoi Voiny' (Concepts of Information Warfare). Speech given at the Russian–U.S. conference on Evolving Post Cold War National Security Issues, Moscow, 12–14 September, p. 7. Cited in Thomas, Timothy (Col) (1996) 'Russian Views on Information-Based Warfare'. Paper published in a special issue of *Airpower Journal*, July

[23] Grau. L-W., Thomas, T. (1996) 'A Russian View of Future War: Theory and direction', *Journal of Slavic Military Studies*, issue 9.3 (September), pp. 501–18

The Congress report states that Russian cyber warfare activities have a military role in the sense that gaining and holding information advantage over an opponent are substantial goals. They could be accomplished by using specific information capabilities to affect an adversary's information systems, decision-making process, command and control system, and even populace.[24] Viruses and other information-related weapons could be used as force multipliers.

One proposed definition for information warfare offered by military theorists attached to the General Staff of the Armed Forces is the following:

> (The) main objectives will be to disorganize (disrupt) the functioning of the key enemy military, industrial and administrative facilities and systems, as well as to bring information-psychological pressure to bear on the adversary's military-political leadership, troops and population, something to be achieved primarily through the use of state-of-the-art information technologies and assets.[25]

2.3 Information control, a stability factor for the state

In contrast to the Western approach, Russian analysts put strong emphasis on information-psychological processes in terms of protecting one's own society from the influence of information put out by an adversary. [26] Striving for control covers not only the concern for state security but also the stability of the regime, as well as the personal interests and ambitions of leading actors. Different interests among different actors come together into a common view on the need for state security.

By controlling the information-psychological aspects such as the mass media – for instance TV, radio and newspapers – as well as the information flow, stability can be achieved. The Russian view should be understood in the per-

[24] Ibid.

[25] Dylevsky, I.N., Komov, S.A., Korotkov, S.V., Rodionov, S.N., Fedorov, A.V. (2007) 'Russian Federation Military Policy in the Area of International Information Security: Regional aspect', *Moscow Military Thought*, 31 March, referred to by Carr, J., 27 July 2009, on the Internet: http://intelfusion.net/wordpress/?tag=russia (retrieved 26 December 2009)

[26] Thomas (1998a)

spective of the disintegration of the Soviet Union as well as experiences from the Chechnya wars and the successful use of media opinion by the opponents. Several analysts argue that one of the major reasons for the breaking up of the Soviet Union was enemy psychological operations.[27] [28] The feeling of vulnerability towards foreign campaigns for influence and the impact of those operations on society was intensely debated during the aftermath of the Cold War.

One of the main components in the Information Security Doctrine adopted by the Security Council in 2000 is to guarantee the protection of what is called 'strategically important' information from foreign activities directed against the interests of the Russian Federation in the information sector. The doctrine is a synthesis of the official position of state policy for maintaining information security. It has been interpreted as the ultimate authority of a nation state to regulate its information and media networks, for instance, by nationalizing free media.[29] The doctrine discusses a wide variety of issues – not only the need for protection of networks and information but also how to strengthen national identity and preserve the cultural heritage in order to ensure that the younger generations develops constructive moral values, patriotism, and civic responsibility for the fate of the country.

The Information Security Doctrine has been a valuable tool for the Kremlin to get a grip on the information flow of Russia. By nationalizing media such as NTV and other free channels, the state has created an instrument for monopolizing the truth.[30]

2.4 IW in peacetime and wartime

Russia's approach to IW and its view on what should be included in the concept is not the same as the West's. Information warfare, in the Russian view, is conducted in *peacetime*, in the *prelude to war* and in *wartime* on three levels – *strategic* (the state level involving different ministries and agencies, as well as operations on two or more fronts), *operational* (the scale of the operations of a front, an army, a corps) and *tactical* (the scale of operations of a combined unit, a subunit).[31]

[27] Thomas (1998b)

[28] Hoffman, D. (2008) 'KGB Comes in from the Cold', *Washington Post*, 8 December, cited in Carman (2002) Translation and Analysis

[29] Carman (2002) Translation and Analysis

[30] Ibid.

[31] Limno, A.N., Krysanov, M.F. (2003) 'Information Warfare and Camouflage, Concealment and Deception', *Military Thought*, vol. 12, no. 2

In the Russian Armed Forces, IW consists of *electronic warfare*, *psychological operations*, *reconnaissance* (intelligence)*, deception* and *mathematical programming impact*.[32] It should be stressed that the current definition does not explicitly mention computer network operations (CNO) but the term 'mathematical programming impact' probably does involve offensive and defensive capabilities for computer and network exploitation, attack and defence.

Regarding the information weapon, one definition is the following:

> Information weapon can be any technical, biological or social means or system that is used for purposeful production, processing, transmitting, presenting or blocking of data or processes that work with the data.[33]

Alexandr Burutin, deputy chief of the General Staff, has made the following statement:

> Information weapons ... do not require specialized manufacturing facilities and a complex infrastructure. A small group or even one expert can develop and carry out an act of destruction while not having to physically cross borders and expose human lives to risk.[34]

The statement could be interpreted as meaning that even a small number of skilled and dedicated hackers could inflict great harm on an adversary's critical systems.

In peacetime IW is related to the information security of society and government, including a wide range of aspects that have to do with protecting the state.[35] Information warfare is conducted secretly by means of intelligence, politics and psychological actions. On the interstate level it involves

[32] Ibid.

[33] Rastorguyev, S.G. (1998) 'Informatsionnoi Voiny' (Information warfare). Radio i Svjaz, referred to in Thomas, T. (2004) 'Russian and Chinese Information Warfare: Theory and Practise'. *Foreign Military Studies Office, Fort Leavenworth*. PowerPoint. June

[34] Speech in Info-Forum, 10 February 2008, referred to by Carr in AppSec Asia Conference, 17 November 2009

[35] Pirumov, V. (1996) 'Nekotorye aspekty informatsionnoi voiny' (Certain aspects of information warfare). Conference speech in Brussels in May 1996, referred to in Thomas (1998a)

diplomatic and economic measures and methods of impact. On the state level the objective of special information operations (SIO) is to shape public opinion (at home and on the international arena) as well as thwarting a possible coalition of allies of a possible adversary.[36]

Maskirovka (methods for deception) is a constituent element in peacetime IW. It is an element of stratagems which 'control' the enemy by creating a false impression of the actual situation and the status of forces opposing the enemy and about the concept, time and nature of their operations, forcing him to act in a predictable manner that will be unfavourable to himself.[37]

Regarding network and computer operations in peacetime IW, viruses and other malware are important in order to compromise the information assets of the engineering systems of the enemy. Other aspects of IW are accumulating (stealing) information on the enemy, by intelligence gathering, while developing and testing one's own IW weapons.

In wartime IW refers to the achievement of information superiority (information dominance) over the enemy, to gain and maintain information advantage but also to protect a country's own information and information systems.[38] IW operations in wartime are more overt than in peacetime and could support traditional forms and methods of warfare, including information and intelligence activities. They involve the physical destruction of military information systems, electronic countermeasures, specially programmed hardware and software (interpreted as malware such as viruses, worms and trojans as well as back-door functionalities and logic bombs), and the distortion, deception and manipulation of information, including psychological operations.

The main components of IW in wartime according to Pirumov are:

- Special operations to disrupt enemy command and control
- Electronic warfare attacks (to blind and disrupt enemy equipment and activity)
- Information blockade (interpreted as using electronic saturation techniques, DDoS, and spamming)
- The systematic actions of forces and assets utilized by IW functions.[39]

[36] Donskov, Y., Nikitin, O.G. (2005) 'Special Information Operations in Armed Conflicts', *Military Thought*, vol, 14, no. 3

[37] Fitzgerald (1996) 'Russian Views on Information Warfare'

[38] Pirumov, Ibid

[39] Ibid.

The Russian IW toolbox also includes means such as radio frequency weapons to disturb the human brain and nervous systems, and electromagnetic energy weapons to knock out electronics and components.

Other areas of a specifically Russian character are microorganism-damaging electronic components and 'psychotropic' or 'psychical' weapons. The purpose of the latter is to affect the human physiology and the brain by using neurolinguistic influences and audiovisual effects through computer programming.[40] The area is ringed around with strong security and there is very little open information on this type of mind-control weapon. If they exist, they could to some extent be compared to the development of non-lethal weapons to reduce human physical and psychological abilities by using electromagnetic pulse waves for crowd control and thermal and voice energy.

2.5 Maskirovka as a sub-function of IW

Russia has a long tradition of conducting deception campaigns. In the light of the rapid penetration of information technology to all aspects of society and human activities, including military activities, there is an increased focus on creating effective means and methods of information warfare. From a Russian viewpoint, *maskirovka* – camouflage, concealment and deception (CC&D) – is a crucial component of information warfare.[41]

The Russian definition of CC&D is the following: *maskirovka* is a variety of activities in support of combat operations and everyday activities of troops (forces) – a set of interconnected organizational, operational-tactical, and engineer-technical measures carried out with to conceal from the adversary the troops as well as the command's plans.[42]

Maskirovka is carried out on strategic, operational and tactical levels, in both peacetime and wartime. It is used as an independent set of measures and actions in order to deceive the adversary. In the Russian view, CC&D is aimed at deceiving foreign (enemy) intelligence services. It involves for instance deception activities against enemy reconnaissance systems (interpreted as sensors and technical systems such as radar stations, air traffic control etc.) and against command and control centres with the purpose of inducing (influencing) an adversary to make decisions benefiting the Russian

[40] Thomas, (2004) 'Russian and Chinese Information Warfare'

[41] Limno and Krysanov (2003) 'Information Warfare'

[42] 'Voyennaya entsiklopedia', Vol, 5, *Voenizdat Publishers*, Moscow, 2001. Referred to in Limno and Krysanov, ibid.

forces. The opinion is that this type of activities should be flexible and predominantly *selective*.

CC&D includes subsystems such as *psychological operations*, *mathematical programming impact* and *counteraction to technical reconnaissance* (directed against the Russian Armed Forces), including protection of data transmission and processing equipment that may be adapted to both defensive and offensive use.[43]

Offensive components of CC&D could for instance include the introduction of malware and malfunctions on all levels in order to corrupt or compromise an adversary's computer and network system (not necessarily military command and control systems but also civilian ones). Through interference and sending misleading information from sensors to radar stations, the decision process of an adversary could be influenced directly or indirectly. By inducing malfunctions it is possible to manipulate control functions, for instance, in precision-guided weapons.

Regarding the defensive and protecting parts of CC&D, Kukashkin and Yefimov have addressed concerns about hostile actions in the form of 'algorithm bombs' and 'software bombs'.[44] This type of malware can distort a section of an algorithm and limit the functionality, thus causing unreliable behaviours. Another type of concern is distance virus weapons, for instance, viruses introduced through radio channels and laser lines of communication directly onto computers and user terminals.[45]

The logic bombs could be *syntactical*, intended to destroy the logic of information system by delaying information and/or by developing unpredictable behaviours through the introduction of malware such as viruses and trojans. Alternatively it could also be *semantic*, that is, it manipulates processes to destroy trust in the system by changing information and inserting deceptive information that may be harmful for the decision-making process.[46]

To summarize, *maskirovka* involves a number of methods, including both psychological and technical aspects, on all levels of conflict. It is an everyday activity directed (primarily) against enemy intelligence services and systems but also towards civilian command and control systems. The objective is to achieve both syntactical and semantic effects by manipulating information

[43] Limno and Krysanov, Ibid.

[44] Kukashkin, A.N., Yefimov, A.I. (1995) 'The Security of the Infosphere of Strategic Defence Systems', *Military Thought*, no. 5

[45] Fitzgerald (1996) 'Russian Views on Information Warfare'

[46] Nunes, V. (1999) 'The Impact of New Technologies in the Military Arena: Information Warfare'. Conference Paper: International Congress of Military Press, Lisbon, 13–16 September

and information systems. It also includes a subsystem of counteraction to adversarial technical reconnaissance.

2.6 Differences and similarities between Russian, US and Chinese views on IW

In order to understand the Russian view in a wider context, a comparison has been made with Russia's most important competitors – the USA and China – and their approach to information operations. The objective is to get a picture of the differences and similarities and of how they interpret and use the IW/IO concept.

One distinction is that Russia and China lack doctrines on IW/IO, at least official doctrines that are open and known to a wider audience outside their countries (in contrast to the US Joint Pub 3-13 and the Joint Vision documents). It should be noted that the term 'IW' has been removed from the latest version of the Joint Pub 3-13, although both Russia and China use it. Moreover, the US doctrine on IO is under consideration and a new doctrine will probably be drafted during 2010. In general the Americans are moving away from the 'five core competencies' (CNO, EW, Psyops, Deception and Opsec). A proposed new definition of IO is the following: the planned and integrated employment of capabilities in the information environment across the spectrum of military operations.[47]

All three countries agree on the important role information has in today's conflicts. Over time its importance will grow. The USA has influenced the mindsets of the others, especially regarding ideas about information superiority and information dominance, as well as command and control warfare. Information adds a new dimension to warfare and IW weapons could be used offensively and defensively to protect a country's own information resources and systems.

Russia and China take a broader view of the essence of information warfare than the USA in the sense that in their approach it covers both peacetime and wartime situations, while the US definition is more narrow and related to times of crisis or conflict.[48]

[47] Kuehl, D., National Defence University, Washington D.C. Presentation on 19 November 2009 at the Swedish Defence College

[48] Thomas (1998a)

The Chinese view[49] [50] [51] is based on four parameters: *pre-emptive strike capability, asymmetric warfare* (inferior versus superior), *high-tech local war*[52] and *people's war.*[53] In some documents the term '*unlimited warfare*' has been mentioned as being a core part of a Chinese view of IW, but the term is disputed by several analysts.

The Chinese concept originates from Sun Tzu's 36 stratagems, described in his *Art of War* from 500 BC. One of the most important key factors in the Chinese concept is deception. The IW perspective covers a long period of time and is not limited to a specific moment, period or conflict. Chinese experts criticize the US doctrine for being much too technology-driven and for not considering the strategic dimension sufficiently. Moreover it is too focused on the information and information system of the opponent and does not consider the softer, psychological factors. In the Chinese conceptual framework, cognitive elements are added, such as the opponent's *will and capability* to fight. It has a clear political dimension. According to Sun Tzu; 'To win the war without the fight is the greatest victory'.

In the Chinese approach IO is a component of IW, contrary to the US view.[54] For American experts *IO is a way to fight* while the Chinese think that *IW is the fight itself* and is ongoing on many different levels and dimensions over the years.

The Russian view is more closely related to the Chinese where the information-psychological impact of IW is concerned, as well as in the idea that IW is conducted in both peacetime, in the prelude to a conflict, and in wartime and more or less constantly; and on the strategic level as well as the operational and tactical.

Regarding deception, all three parties consider the term as being a vital part of IW/IO. The USA uses the term *military deception* (MILDEC) as a core capability of IO in order to mislead an adversary's decision makers (in a conflict situation). Compared to the US view, the Russian Armed Forces treat

[49] Weigung Shen (1996) 'A New Form of People's War'. 26 June, on the Internet: http://www.fas.org/irp/world/china/docs/iw_wei.htm (retrieved 16 June 2008)

[50] Li Yinnan (1996) 'New Subjects of Study Brought about Information Warfare'. *Jiefangjun Bao*

[51] Zhenxing, Pu Feng (1995) 'The Challenge of Information Warfare'. April, on the Internet: http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm (retrieved 16 June 2008)

[52] Niu, Li., Jiangzhou, Li., Dehui, Xu (2000) 'Planning and Application of Strategies of Information Operation in High Tech Local War', *Zhongguo Junshi Kexue* (China Military Science), no. 4, 20 August

[53] Weiguang, Ibid

[54] Barret, B.M. (2008) 'Information Warfare: China's response to U.S. technological advantages', *International Journal of Intelligence*, vol. 18, no. 4

maskirovka as an independent type of operational (combat) support to influence an adversary. It is conducted on a daily basis and on all levels.

The time perspective is probably longer for the Chinese, covering several decades or more compared to the Russian view. In the US view the time perspective is shorter than it is in both the Russian and the Chinese approaches and is related to specific conditions and conflict situations. On the other hand the Americans occasionally use the term *strategic communication* in order to exert influence on the strategic and political levels over a longer period of time. It is not necessarily limited to a specific conflict. Strategic communication is not an integrated component of information operations. Moreover, it is also important to note that MILDEC and strategic communication are not necessarily parts of each other.

The US joint doctrines[55] describe information superiority or information dominance as a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control. By gaining information superiority one party gets an advantage over another party. Russian analysts point out that information superiority will be the main condition of victory in 21st-century wars.[56] Bogdanov states that '…it will be impossible to attain strategic and operational objectives in future wars without achieving superiority over the adversary in the information sphere'[57]. The Russian and Chinese views are similar to the US approach in that aspect. Another similarity, according to Thomas, is the concept of protecting one's own information while affecting the information of an adversary.[58]

Information control, as defined in the Doctrine of Information Security of the Russian Federation, has an inbuilt psychological dimension related to the stability of the state. It is directed toward the country's own population as well as against what is seen as foreign campaigns to exert influence. The Russian and Chinese views show some similarities, although their practices when it comes to how to gain control over the mass media, the Internet and other communication channels (for instance) often differ. In Western democracies the ability to restrict or control the mass media component and the information flow is regulated by laws.

In the Russian and Chinese concepts of IW, cyber operations are directly connected to psychological activities. They are integrated factors. On the US

[55] CRS Report for Congress (2001) 'Cyberwarfare'

[56] Limno and Krysanov (2003) 'Information Warfare'

[57] Bogdanov, S.A. (2004) 'Warfare of the Future', *Military Thought*, vol. 13, no.1

[58] Thomas (1998a)

side, the line between these does not seems to be as important as it is for China and Russia. The reasons could be both historical and organizational.

One major difference between the USA and Russia, and probably China, is their ideas on how to react to adversarial cyber attacks (e.g. computer network operations) and the risk of conflict escalating. Some Russian analysts put IW on a par with weapons of mass destruction. This is somewhat controversial and is probably not the official view. In their view, if Russia's critical information and communication systems are attacked by information warfare means, they reserve the right to use nuclear weapons against eventual attackers. The Russian statement could be understood as a strategy for deterrence. At least this is the message they would like to create.

This is not a coincidence but an accepted form and common procedure. Russia's main form and method for deterrence – designed to show a potential aggressor the costs of launching an attack – are based on following: (a) *demonstration* of the deployment of Russian defensive forces in the sector (direction) of threat, (b) an *ultimatum-like statement* that the Russian will immediately use nuclear weapons in the event of threats to its sovereignty and territorial integrity, and also make unlimited use of precision-guided weapons to destroy critical functions, and (c) *preparation and implementation of special operations in the information sphere* to mislead the adversary about Russia's readiness to repulse an act of aggression.[59] The latter could be interpreted as *maskirovka*.

[59] Bogdanov (2004) 'Warfare of the Future'

3. Russian military and civilian organizations responsible for IW capability

Since the early 1990s significant efforts have been made to strengthen the security of the Russian state against both international and domestic threats. IW is seen as an important capability to develop for both offensive and defensive purposes. Within the Russian administration several federal authorities are responsible for handling information warfare capabilities, including all forms of networked and digital activities not limited to the Internet and cyberspace but also covering electromagnetic warfare and influencing campaigns. The military system for collective security is divided according to the regional principle. Every military district has its own capacity for IW.

There are four major agencies dealing with IW in a broader sense – the *Federal Protection Service* (FSO), the *Federal Security Service* (FSB), the *Foreign Intelligence Service* (SVR) and *Military Intelligence* (GRU). With the exception of the GRU, all these organizations are the results of the breaking up of the KGB. The FSO, the FSB and the SVR are subordinated to the president. The GRU is a part of the Defence Ministry as the central organ of military intelligence for the General Staff.

Within the Russian Armed Forces there are also special units such as the signals troops and radio-electronic combat units dealing with electronic warfare capabilities on the operational and tactical levels. Sources of signals intelligence (SIGINT) and electronic intelligence (ELINT) are captured by aerial and sea assets as well as by the Strategic Rocket Forces. Another organization connected to the Russian Federation is the RU-CERT (Computer Emergency Response Team) which is responsible for reporting cyber incidents.[60]

3.1 Strategic Signals Intelligence

FAPSI

From 1991 to 2003, the Federal Agency of Government Communication and Information, FAPSI, was responsible for special communications, cryptographic security, technical intelligence, counterintelligence, code cracking

[60] On the Internet: http://www.cert.ru/en/about.shtml

and telecommunications and information protection, in the same way as the US National Security Agency.[61] It provided special information to higher bodies of authority for the benefit of the Russian Federation.[62] Other responsibilities were to monitor information security in the credit, financial and banking sector. The agency also fought domestic criminality, foreign special services and different forms of IW-related activities. The main tasks were to intercept and decipher other countries' communications.[63] The task probably involved some CERT functionality to analyse and manage cyber incidents.

In April 2003 the 54 000 -strong organization was dismantled and FAPSI's resources were divided between the FSB, the SVR, the FSO and the Defence Ministry, e.g to the GRU. One reason for the breaking up of FAPSI was accusations of corruption.

FSO

The Federal Protection Service[64] has taken over many of FAPSI's former duties. It employs about 20 000 people and is one of successors of the KGB and its headquarters are in block 14 in the Kremlin. The organization supervises top-level communications. It provides the Kremlin with strategic signals intelligence from surveillance facilities, and is also responsible for the 'black box' handling the nuclear missile system. The FSO has inherited responsibility for ensuring the exploitation of special information systems for state agencies; this is carried out by the FSO Special Communication and Information Service.[65] Its main tasks are the monitoring of telegraph and wired telephone lines as well as surveillance of the Internet, satellites and wireless communications.

[61] Staar, R., Tacosa, C. (2004) 'Russia's Security Services', *Mediterranean Quarterly,* vol. 15, issue 1

[62] Thomas (1998) 'Russia's Information Warfare Structure'

[63] Bennet, G. (2000) 'FAPSI - The Federal Agency of Governmental Communication & Information', on the Internet: http://kgb-militaryschool.com/view/Fapsi (retrieved 15 December 2009)

[64] Pike, J. (1997) 'Federal Protection Service (FSO)', 26 November, on the Internet: http://fas.org/irp/world/russia/fso/index.htm (retrieved 12 December 2009). Also in *Directory of Defence Related Agencies and Personnel* from the CIA's website the Foreign Broadcast Service (FBIS), on the Internet: http://ftp.fas.org/irp/world/russia/fbis/MAININDEXPAGE.html (retrieved 12 December 2009)

[65] Chuen, C. (2006) 'Russia: Government and Selective Ministries'. Updated 23 January2006, on the Internet: http://www.nti.org/db/nisprofs/russia/govt/ministry.htm. *NTI, Centre for Non-proliferation Studies at Monterey Institute of International Studies* (retrieved 12 December 2009)

3.2 The Federal Security Service

FSB

The Federal Security Service, the former KGB, is divided into chief directorates, directorates, services and departments. Its main tasks are law enforcement functions, security and counter-intelligence. The number of employees in 2003 was approximately 270 000. The practice of the FSB involves a wide variety of tasks, for instance, deploying agents under cover of other agencies, collecting intelligence, and the fight against terrorism, political crimes and foreign agencies, all in order to protect state secrets. The focus is on state security.

According to the Interdepartmental Commission of the Russian Security Council, which is directed by a deputy director of the FSB, the secret service is probably the authority responsible for information security on the federal level.[66] Organizationally, within the FSB a specific service is appointed for that mission. The FSO is also represented on the Commission by a deputy director responsible for a security service within the FSO organization.

Regarding IW capabilities, the *Law on Operative Search and Seizures* from 1995 permits the FSB to use wiretapping of telephone lines, open mails and monitor other forms of communication channels such as Internet surveillance. The law also enables the FSB to conduct intelligence activities in Russia as well as abroad in cooperation with the SVR.[67] In the interests of Russian security, the law permits agents to enter private residences without a court order.[68]

The FSB probably has overall responsibility for operative signals intelligence through the SORM II system.[69] SORM is used for monitoring Internet traffic. On request by the FSB, all Internet service providers (ISPs) have to invest in

[66] Security Council of the Russian Federation (2006) 'Dostav Mezhvedomstvennoi kommissii Soveta Bezopanosti Rossiiskoi Federatsii po informatsionnoi bezopasnosti po dolzhostiam', *Presidential Decree* No. 601, 12 June 2006, on the Internet: http://www.scrf.gov.ru/documents/46.html (retrieved 5 February 2010)

[67] 'On Organs of the Federal Security Service in the Russian Federation'. *Russian Federation Law* No, 40-ZFZ. Adopted by the State Duma 22 February 1995. Signed by Russian Federation President B. Yeltsin and dated 3 April 1995, on the Internet: http://fas.org/irp/world/russia/docs/law_950403.htm (retrieved 12 December 2009)

[68] Staar and Tacosa (2004) 'Russia's Security Services'

[69] SORM is a Russian acronym for System for Operational-Investigative Activities. It could be compared to the FBI's Carnivore and the British Government Technical Assistance Centre (GTAC); see Leijonhielm, J., Hedenskog, J., Knoph, J., Oldberg, I., Unge, W., Vendil, C. (2000) 'Rysk military förmåga i ett tioårsperpektiv. En förnyad bedömning 2000'. Användarrapport FOA-R-01758-17--SE (Stockholm, FOA)

this type of surveillance system. One source mentions that more or less all communications that are transmitted through operators such as Rostelekom, Transtelekom and Elektrotelekom are forwarded to the FSB.[70]

With the breaking up of FAPSI, the FSB inherited a Special-purpose Information and Telecommunication System (ITKS). The ITKS consists of a series of situation centres[71] from federal level to regional level for ensuring information security, cryptology and code breaking. The FSB issues certificates and licences for information and communication systems used by federal agencies.

The FSB probably has capability for conducting computer network operations[72] including exploitation, attack and defence. The Chief Directorate 'Service A', for instance, is responsible for deception campaigns, *maskirovka*, to coordinate the dissemination of false and provocative information under the name *'active measures'*. The term 'active measure' was a form of political warfare conducted by the Soviet security services to influence opponents. It ranged from media manipulation to special actions involving various degree of violence.

3.3 Foreign Intelligence

SVR

The Foreign Intelligence Service also comes under the president and is responsible for providing intelligence information, operations and analysis to the Russian president, Federal Assembly and government. Together with the GRU, its main function is to provide the state leadership with foreign intelligence. The objective is to contribute to the decision-making process in the areas of politics, economics, defence, science, technology and ecology. Identifying scientific advances that might threaten or benefit Russian security is a specialized task. In 2003 the organization was estimated to have 11 800 persons on its payroll.

The SVR conducts human intelligence activities against adversaries, but it also has capacity for strategic signals intelligence and managing military and commercial satellite systems and fixed and wireless communications. Up to

[70] InfoSecurity (2009) 'Grey Goose 2 Ties Kremlin More Closely to Georgia Cyber-attacks', 20 March. On the Internet: http://www.infosecurity-magazine.com/view/762/grey-gosse-2-ties-kremlin-more-closely-to-georgia-cyber.htm (retrieved 27 December 2009)

[71] Thomas (1998b)

[72] Computer network operations (CNO) is divided into: (i) CNE – computer network exploitation, (ii) CNA – computer network attack, and (iii) CND – computer network defence

autumn 2001 the agency manned the radio-electronic centres in Lourdes in Cuba and Rahm Bay in Vietnam together with FAPSI and the GRU. Due to budget cuts the centres have since been withdrawn.[73] [74] Information indicates that the SVR and/or the GRU facilitate intelligence centres at the People's Democratic Republic of Yemen's Ras Karma Military Airbase, near QaDub on Socotra Island in the Indian Ocean.[75] The surveillance facility lies opposite the coast of Somalia in the Gulf of Aden.

GRU

Military Intelligence was established in 1918. Over the years it has changed designation several times. It comprises the foreign intelligence organization of the Defence Ministry and the central organ of military intelligence for the General Staff. The GRU gathers information on military, military-political, military-economic and ecological issues. Military attachés and foreign agents are important means of information gathering. The GRU is an intelligence system that makes comprehensive use of practically all forces and means of intelligence.[76] It maintains units for signals intelligence, imagery reconnaissance (IMIT) and satellite imagery capabilities (SATINT). It also conducts open source intelligence (OSINT).

The GRU has over 26 000 staff, divided into 24 individual brigades numbering 1500 men each. Under the GRU's command, there are special operation units, the Spetznaz (special purpose troops), responsible for surveillance of communications and electronic intelligence.

[73] Bennet (200) 'FAPSI – thefederal Agency of Governmental Communication & Information'. http://kgb-militaryschool.com/view/Fapsi (retrieved 15 December 2009)

[74] Shcherbakov, A. 'Major Loss of Intelligence Gathering Capacity', on the Internet: http://www.fas.org/irp/world/russia/fapsi/shcherbakov.htm (retrieved 20 December 2009)

[75] Ibid.

[76] Babaeva, S. (2003) 'VALENTIN KORABELNIKOV: SMART AND WELL-TRAINED PEOPLE WORK WITH US. An interview with the chief of Russian military intelligence', *CDI Russia Weekly*, 17 July, on the Internet: http://www.cdi.org/russia/265-17.cfm (retrieved 26 December 2009). Also described in Project Grey Goose Phase II Report, 'The Evolving State of Cyber Warfare', 20 March 2009, on the Internet: http://intellibriefs.blogspot.com/2009/03/cyber-warfare-project-grey-goose-phase.html (retrieved 27 December 2009)

3.4 Some driving forces behind the development of IW capability

A crucial factor and a basic foundation for the development of IW capabilities are well-deployed information and communication infrastructures. Russia in general, like many other countries, puts a great deal of emphasis on modernizing its landline telecommunication systems. It is investing in fixed and wireless broadband technologies accessible to the Internet as well as in satellite communication systems. In remote areas, for instance, the Internet may be accessed through satellites.

According to the International Telecommunications Union (ITU), the number of Internet users in Russia in 2009 exceeded 45 million, which is approximately 32% of the population.[77] Mobile phone penetration is estimated to be more than 130% in 2009, in total 191 million subscribers.[78] [79] Densely populated areas such as the Moscow and Leningrad regions have the best coverage and the highest penetration rates. Over time the coverage will extend to other parts of the country.

From a military point of view the Russian Armed Forces have invested in general-purpose communication systems and command and control systems. But, judging from the Five-Day War in Georgia, the investment has not been sufficient. There is a need for continuous upgrading and improvement.[80] The Russian command and control capability was hampered by communication equipment that was inferior to Georgia's. Russia lacked equipment in combination with compatibility problems between systems. In some cases Russian commanders had to rely on private mobile phones. The ground unit, for instance, could not communicate with attack helicopters and aircraft crews due to incompatibility.[81] The forces are developing and launching satellite communication systems and navigation systems such as GLONASS. It is an

[77] Internet World Statistic (2009) 'Russia Internet Usage and Marketing Report'. On the Internet: http://www.internetworldstats.com/euro/ru.htm (retrieved 21 December 2009)

[78] Regarding mobile penetration, users could have several subscriptions. Machine-to-machine communications also require subscriptions. According to the International Telecommunications Union (ITU), mobile penetration in Russia in 2007 was almost 120%. On the Internet: http://www.itu.int/ITU-D/connect/cis/figures.html (retrieved 21 December 2009)

[79] 'Russia Reports Mobile Penetration of 131.4 %'. *Wireless Federation*. 21 April 2009, on the Internet: http://wirelessfederation.com/news/15415-russia-reports-mobile-penetration-of-131.4/ (retrieved 21 December 2009)

[80] Vendil Pallin, C., Westerlund, F. (Swedish Institute of International Affairs and Swedish Defence Research Agency) (2009) 'Russia's War in Georgia: Lessons and consequences', *Small Wars & Insurgencies*, vol. 20, no. 2 (June), pp. 400–24. On the Internet: http://dx.doi.org/10.1080/09592310902975539 (retrieved 15 January 2010)

[81] Ibid.

alternative and complementary system to the United State's Global Positioning System (GPS). Due to financial problems and a subcritical number of satellites in orbit, GLONASS is still not 100% operative in 2010. This has implications for war fighting. In Georgia the Russian units lacked an autonomous targeting system and this affected their ability to conduct joint operations.[82]

Regarding IT, the Russian software industry is one of the most productive sectors in the country with a competitive edge on the international market.[83] The hardware industry on the other hand is lagging behind Western and Chinese companies. Electronic components are viewed as vital parts of the Russian defence industry. In 2007 the government adjusted a federal programme for the period 2008–15 to develop the foundations for components and radio-electronics.[84]

From the Soviet era, Russia inherited a tradition of preferring independence – developing and producing its own computer systems, both hardware and software. Formerly this approach was to a great extent based on necessity due to the country's isolation and the economic constraints of the Cold War, but the approach is more or less the same today. By developing and producing its own technology and products, a country can gain better control of critical systems and thereby improve overall information security. One specific area of research, for instance, is neuro-computers and neural networks known as artificial organic brain computers.[85] The nanotechnology sector is another area of interest.

Information security is a prominent focus area. Due to the very high educational standards in mathematics and physics in the country, the Russians are seen as very competent software programmers. Compared to American IT specialists, highly educated labour is cheap. Russian computer companies such as the well-known Kaspersky Laboratory are working with information security – cryptology, ciphering and algorithms, the integration of complex security systems and the development of secure networks, computers and wireless terminals.

[82] Tsyganok, A. 'Uroki piatidnevnoi voiny v Zakavkaze' in Vendil Pallin and Westerlund (ibid. 2009) (retrieved 21 December 2009)

[83] 'IT & Software Opportunities in Moscow'. *Moscow Investment Gateway.* On the Internet: http://74.125.77.132/search?q=cache:ktOSEdAuIOcJ:moscow.e-regulations.org/Media/Editor_Repo/undp_it%2520%26%2520software.ppt+unemployment+rate+ict+sector+russia&cd=2&hl=sv&ct=clnk&gl=se (retrieved 15 January 2010)

[84] Leijonhielm et al. (2008) 'Rysk militär förmåga i ett tioårsperspektiv'

[85] Galushkin, A., Koroba, S., Kazantsev, P. (2003) 'Neuromathematics: Development tendencies', *Applied Computer. Math.* 2, no. 1. On the Internet: http://www.elm.az/acm/pp.57-64.pdf (retrieved 20 December 2009)

3.5 Development of IW units

There is very little open information describing the development of specific IW units for computer network operations where capability, organization and structure are concerned. A qualified assumption is that all four intelligence and security agencies have their own resources for conducting offensive and defensive networked and digital activities due to their specific tasks and areas of responsibility.

As a consequence of the poor performance in the Georgia conflict, a process has started under the command of the General Staff to build up Russia's electronic warfare capability by creating independent EW troops with modern EW systems and contract soldiers.[86]

On a strategic level the FSO has overall responsibility for conducting signals intelligence, the FSB for internal security, and the GRU and SVR for international threats. Due to the logic[87] of cyber warfare, cooperation and coordination are required between intelligence and security officers, the so-called *siloviki.*[88] However, as in other countries, perfect coordination is hard to achieve and there is a considerable degree of competition between the services.

[86] Tikhonov, A, 'Protivoborstvo v diapazonakh chastot' in Vendil Pallin and Westerlund, 'Russia's War in Georgia' (2009)

[87] Cyber warfare is by logic asymmetrical. It is possible to act anonymously on the Internet and activities lack geographical boundaries

[88] Bremmer, I., Charap, S. (2006/07) 'The Siloviki's in Putin's Russia: Who they are and what they want', *Washington Quarterly*, Winter. Centre for Strategic and International Studies and Massachusetts Institute of Technology. On the Internet: http://www.twq.com/07winter/docs/07winter_bremmer.pdf (retrieved 14 January 2010). See also *Siloviki.* Global Security.Org, On the Internet: http://www.globalsecurity.org/military/world/russia/siloviki.htm (retrieved 14 January 2010)

4. Russia and emerging cyber threats

It has been notified that a lot of malicious activities in cyberspace are originating from Russia. The accusations involve a wide range of activities, from spreading malware and spamming, cyber criminality and cyber espionage to hacktivism directed against adversaries. Here Russia is seen, together with China, as an unregulated area and a safe haven for the development and spreading of malicious codes worldwide.

The so-called black economy of hackers, data burglars and code thieves is a multibillion-dollar European business, with the majority of players producing code in Eastern Europe, Russia and Asia.[89] Cyber espionage is a growing sector worldwide. In 2008 more than 1 trillion USD-worth of data was lost to cyber espionage, including industrial espionage and intellectual property theft as well as theft of trade secrets.[90] The Americans have pointed out Russia and China in particular as acting aggressively in this regard.

This chapter discusses briefly the potential cyber threats – from criminals and nationalist-driven hacker groups – that are said to emanate from Russia.

4.1 Driving forces for malicious activities

Thanks to its high educational standards in the natural sciences, mathematics and physics, there is a great number of skilled and IT-trained people in the country. For instance, about 250 000 people are employed in the information and communications technology (ICT) sector in the Moscow area alone.[91] For younger people it is quite hard to get employment. Many well-educated younger people are applying for jobs abroad. It is estimated that more than 70 000 Russians are working in the American IT industry. The software industry in Russia is growing, especially firms within the information security sector. Russian programmers are seen as among the best in the world and are often used by Western companies such as Microsoft, IBM and Google and others. In Russia there are several universities that maintain high international

[89] Keggler, J. (2008) 'Taking the Fight to the Net'. *Armada International*, vol. 32, issue 2 (April/May),

[90] Ackerman, R. (2009) 'Threats Imperil the Entire U.S. Infrastructure. From the military to the economy, the country is open to vast damage', SIGNAL. *AFCEA International Journal*, July

[91] *IT & Software opportinities in Moscow.* Moscow Investment Gateway. Source: Moscow Government; Goskomstat; Statistics on Russian Education; Watson Wyatt, on the Internet: http://74.125.77.132/search?q=cache:ktOSEdAuIOcJ:moscow.e-regulations.org/Media/Editor_Repo/undp_it%2520%26%2520software.ppt+unemployment+rate+ict+sector+russia&cd=2&hl=sv&ct=clnk&gl=se (retrieved 21 December 2009)

standards and have a good reputation teaching computer sciences and network security.

There are several elements behind the forces driving the development of malicious cyber activities. Unemployment among the younger generations is a problem. The total unemployment rate in 2009 was approximately 8–9% and the social security system is inadequate.[92] Corruption in Russia is on a huge scale and covers all levels of society. There is a huge and growing difference in living standards between people in the big cities and in the rural parts of the country which creates social pressures. The laws for protecting property, not least intellectual property, are also weak, as is the court system.

Many citizens do not see cyber criminality, such as phishing, identity and card theft, Internet fraud, hacking into banking accounts, as well as website defacements in order to blackmail companies and organizations, as major threats to the society compared to other types of crime. There are several reasons for this.

First and foremost, most activities are directed against foreign commercial websites run by banks and financial institutions, not Russian ones. If cyber crime is not aimed against Russia and Russian interests and does not affect local targets, the law enforcement agencies in general do not know much about it and do not have much will to investigate and take legal proceedings. If foreign companies fail to protect their own systems, it is a problem for themselves to solve and it is not necessarily a task for the Russian authorities to deal with. Another reason is that, because it is possible to act anonymously on the Internet and to hide digital traces, it is hard for the law enforcement agencies to discover, detect and catch potential criminal cyber activists. It takes a great deal of resources that could be better used on more urgent matters against other types of crimes.

An increasing problem is Russia spammers stealing personal information and money from accounts. On the Internet there are special websites run by criminal groups, where it is possible to buy lists of stolen card numbers to be used for fraud. Information is available on Internet forums on how to hack into commercial systems. One well-known hacker website is the Khaker's (hackers) website xakep.ru. Khaker also provides a news magazine which is easily accessible with the same title. There are also 'hacker schools' that teach basic skills on how to crack computers and network systems. In one well-known hacker school around 10 000 people have applied for admission

[92] 'Russia Employment Rate. Trading economics'. *Global Economics Research*. On the Internet: http://www.tradingeconomics.com/Economics/Unemployment-rate.aspx?symbol=RUB (retrieved 21 December 2009)

since it was founded in 1996.[93] The courses are advertised in the public media.

There is evidence that Russian organized crime syndicates are also involved in cyber crimes. The modus operandi regarding coordination, sophistication and the choice of specific target objects indicates that cyber attacks are committed by a well-financed, organized and experienced group (or groups) of criminals.[94]

4.2 The Russian Business Network

One infamous group of cyber criminals is the Russian Business Network (RBN). The group has acted as an ISP and rented servers that could be used for cyber crimes until 2007.[95] By then its IP addresses and domains were blocked and blacklisted by the information security community and forced to move its domain servers to China and Taiwan. It is uncertain whether the group is still active and operative.[96] Some information on blogs says that the network was involved in the Georgian cyber conflict in 2008. Others point out that it no longer exists.[97] The RBN has been involved in various aspects of cyber criminality such as phishing, malware distribution, malicious code, botnets, DDoS attacks and even child pornography.[98] Between early 2006 and November 2007, when the RBN served as an ISP, it was linked to 60% of all cyber crime.[99] [100] Its history can be traced back to early 1996. In 2002, the group became more organised and structured and its activities increased. For instance, the RBN has been accused of attacking the US Department of

[93] Osipovich, A. (2007) 'Inside a Hacker School', *Foreign Policy*, issue 163 (November/December)

[94] Flook, K. (2009) 'Russia and the Cyber Threat'. 13 May, on the Internet: http://www.criticalthreats.org/russia/russia-and-cyber-threat (retrieved 12 December 2009)

[95] 'Russian Business Network (RBN)'. October, 2007. On the Internet: http://rbnexploit.blogspot.com/2007_09_01_archive.html (retrieved 12 December 2009)

[96] Shactman, N. (2008) 'U.S. Embassy in Russian Hackers' Crosshairs?', 12 August, on the Internet: http://www.wired.com/dangerroom/2008/08/investigators-a/ (retrieved 12 December 2009)

[97] MacQuaid, J. (2008) 'The RBN Operatives Who Attacked Georgia Secure Home Network', 18 August, on the Internet: http://securehomenetwork.blogspot.com/2008/08/rbn-operatives-who-attacked-georgia.html (retrieved 12 December 2009)

[98] Flook (2009) 'Russia and the Cyber Threat'

[99] Verisign (2008) 'The Russian Business Network: Rise and fall of criminal ISP'. *IDefence Security Report,* 8 March

[100] Richard, J. (2008) 'Number of Computer Viruses Tops One Million'. *Times online,* 10 April, on the Internet: http://technology.timesonline.co.uk/tol/news/tech_and_web/article3721556.ece (retrieved 13 December 2009)

Defense and the Russian Department of the Treasury in 2003, but this has not been proved officially.[101]

4.3 Hacktivism

There is a suspicion that nationalistically oriented groups of computer-skilled individuals originating from Russia are conducting malicious cyber activities themselves or by proxy. One group alleged to be involved in incidents on the Internet is the *Nashi Youth Group* (Democratic Anti-Fascist Movement 'Ours').

The 120 000-member strong organization was officially announced by Vasilii Yakemenko[102] on 1 March 2005. The group was ostensibly formed to stamp out Nazi sentiment. There is reason to assume that it receives direct subsidies from the Kremlin[103] and was supported by the first deputy chief of the Kremlin's presidential staff, Vladislav Surkov, who has met the movement several times, giving speeches and holding private talks. Pro-business owners looking to ingratiate themselves with the regime are said to be funding the youth movement.

The organization has been accused of acting aggressively against opponents with harassment, spying and physical violence. It acts both in the physical sphere and in cyberspace. In April and May 2007, Nashi members protested daily in front of the Estonian embassy in Moscow against the moving of the memorial statue of a Soviet soldier of Tallinn to a military cemetery. In an interview with the *Financial Times*, Nashi activist Konstantin Goloskolov confirmed that the group was behind the cyber attack against Estonia of spring 2007.[104] Whether this is true or not is open to debate.

[101] Verisign (2008) 'The Russian Business Network'

[102] Wapedia. http://wapedia.mobi/nashi_(youth_movement) (retrieved 14 December 2009)

[103] Young, C. (2007) 'Putin's Young "Brown Shirts"', *Boston Globe*, 10 August

[104] Shactman, N. (2009) 'Kremlin Kids: We Launched the Estonian Cyber War'. *Wired,* 11 March, on the Internet: http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/ (retrieved 14 December 2009)

5. Towards a new modus operandi? – The Estonian and Georgian cyber war experiences

Two cases especially have been subject for discussion during recent years regarding cyber operations that might emanate from Russia – the cyber assault against Estonia in 2007 and that against Georgia the year after. These attacks have been attributed to the Russian state by Estonia and Georgia, and a number of attacks originated from servers and were clearly encouraged by Russian websites. Both cases could be seen as examples of how cyber operations might be conducted in future conflicts.

5.1 The Estonian case

The Estonian cyber conflict in the spring of 2007 has attracted a great deal of interest. Some describe the case as the first official and publicly described cyber war against a country. Others point out that it was not a war but a cyber riot.[105] Nevertheless it was the wake-up call showing the potential risks of hacktivism. The incident was provoked by the removal of a Soviet military statue from the centre of Tallinn to a nearby military graveyard. Many Estonians see the war monument as a symbol of the Soviet occupying force and the annexation of the Baltic states. Its removal caused much anger among native Russians in the country and riots started in the streets of the capital. In conjunction with that, feverish activity began on the Internet. An operation was initiated with the objective of attacking Estonian computer systems and various national websites.

[105] Brenner, B. (2007) 'Black Hat 2007: Estonian attacks were a cyber riot, not warfare', *Information Security Magazine*, 3 August. On the Internet: http://searchsecurity.techtarget.com/news/article/0,289142, sid 14_gci1266728,00.html (retrieved 26 January 2010)

The first phase of attack:

According to Lauri Allman,[106] Estonia's permanent undersecretary of defence, there were two phases of attacks. The first[107] was carried out at 1 am, 28 April. Relatively primitive and simple attack tools were used. On several web pages and Internet forums hacktivists were encourage to contribute. On mostly Russian websites ordinary people could download attack tools and instructions on how to attack Estonian websites. The target objects were the Estonian Government Briefing Room, the Estonian Ministry of Defence and leading political parties in the country. The attack peaked around 3 May and slowly subsided after a period of general fatigue. The effect was not sufficient enough due to a lack of a critical mass of people engaging in the operation.

The second wave:

The second phase of the attacks peaked around 8 and 9 May 8, two of the most celebrated dates in Russian calendar when the country marks Victory Day over Nazi Germany. The attack tools this time were more sophisticated, using mainly large botnets of compromised computers conducting DDoS attacks to overwhelm information flow. The websites of the Estonian Parliament, two of the country's largest banks, almost all of the country's government ministries and three of six biggest news organizations were targeted.[108] Within a few days' servers and networks were overloaded with information which led to reduced functionality. Websites were forced to shut down. Some defacement attacks were also made during the operation. Especially mission-critical computers, for example the telephone exchanges, were targeted. This indicates that the originator of the attackers probably had inside information regarding specific and important systems to approach. The cyber attack ceased as fast as it started. The attackers stopped of their own volition rather than be shut down.[109]

[106] Kash, W. (2008) 'Lessons from the Cyberattacks on Estonia. Interview with Lauri Allman, Estonia's permanent undersecretary of defence', *Government Computer News*, 13 June. On the Internet: http://www.gnc.com/articles/2008/06/13/Lauri-Almann-Lesson-from-the cyberattacks-on Estonia.aspx (retrieved 26 January 2010)

[107] The first indication of the attack came during 27 April 2007

[108] Traynor, I. (2007) 'Russia Accused of Unleashing Cyberwar to Disable Estonia'. *Guardian.co.uk*, 17 May, on the Internet: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (retrieved 26 January 2010)

[109] McAfee Virtual Criminology Report. 'Cybercrime: The next wave, 2007'

Estonian counteractions:

After the first indications that they were under attack, a team of people were engaged very fast to start working on how to protect the country's Internet sovereignty. The Estonian CERT and private entities cooperated intensively to solve the problem. There was informal agreement to share information openly between the protectors and not to compete on security. Coordination of resources was easier in a country like Estonia because it is a small state with only about 1.4 million citizens and the CERT knows pretty well everybody working within the information security community.[110]

A first response by the Estonians was to increase the Internet throughput capacity in cooperation with other countries. This was done incrementally. They also tried to block external servers. During the operation the Estonians identified several ping messages being sent in order to measure the country's throughput capacity. Intelligence shows that the result of the measures changed the behaviour of the attackers, who adjusted their actions in response.[111] It was a struggle between actions and counteractions. The attackers kept getting new information on how to attack and respond to defences.

Analysis:

A rough estimate is that the attacks emanated from 75 or more jurisdictions using 1 million or more computers.[112] At the height of the attacks more than 20 000 networks of compromised computers were linked.[113] Analysis of the IP addresses of the attacking computers shows a long list of states from all around the world – up to 178 different countries.[114] It should be noted that it is possible to fake IP addresses. The opinion of analysts is that the attacks were carried out by a well-organized group of people with features of command and control. It required both financial and intellectual resources. The attacks came in waves. In peak time the attack measured about 100 MB per second of traffic, which is considered to be quite moderate. In com-

[110] Brenner (2007) 'Black Hat 2007'

[111] Kash (2008) 'Lessons from the Cyberattacks'

[112] Ibid.

[113] McAfee (2007) 'Cybercrime: The next wave'

[114] A comment made by Katrin Pargmae, as spokeswoman for the Estonian Informatics Centre in Homeland Security News Wire (HSNW) (2009) '2007 Cyber Attack on Estonia Launched by Kremlin-backed Youth Group', published 13 March 2009, on the Internet: http://homelanssecuritynewswire.com/2007-cyber-attack-estonia-launched-kremlin-backed-youth-group (retrieved 26 January 2010)

parison, the largest DDoS attacks have measured up to 40 GB per second.[115] Several Internet security experts, such as the Russian Internet pioneer Anton Nossik, say that 'compared to the scale of the problem in general, Estonia is small' .[116] Mike Witt, deputy director at the US CERT, also believes that, while the 'size of the cyber attacks was certainly significant to the Estonian Government, from a technical standpoint is not something we would consider significant in scale'.[117]

In general, for moderately computer-skilled persons it is not too difficult to lease botnets with a large number of compromised computers for conducting malicious activities such as DDoS attacks. The rental cost for botnets is somewhere between 1000 and 5000 USD.[118] One interpretation as to why the DDoS attacks stopped was that the rental time of the leased botnets was over. By that time the originators of the attacks had achieved their goal. The message sent to the opponent was clear.

Effects and consequences:

It has not yet been fully established who or what groups and organizations lay behind the operation. Some of the IP addresses indicating servers are probably faked. There is no indication of Russian government involvement. Persons connected to Nashi Youth have said that they were behind the operation, but the statement is disputed. State Duma Deputy Sergey Markov claimed that one of his assistants was responsible for instigating the cyber attack in Estonia.[119] This should be interpreted as a provocative message and is not necessarily true.

Estonia is one of the world's most connected countries and is therefore more vulnerable to cyber attacks than less modern societies. For instance, more than 97% of all banking transactions are made online. The cyber attacks show built-in vulnerabilities and the need for investment in cyber security. One

[115] A comment made by Jose Nazario from the information security company Arbor Networks referred to in Homeland Security News Wire (HSNV), Ibid.

[116] BBC News, 'The Cyber Raiders Hitting Estonia', 17 May 2007, on the Internet: http://news.bbc.co.uk/2/hi/europe/6665195.stm (retrieved 26 January 2010)

[117] United Press International (2007) 'Analysis: Who Cyber Smacked Estonia?' On the Internet: http://www.upi.com/security/security_terrorism/Analysis/2007/06/analysis_who_cybersmacket_estonia/2683/print_view/ (retrieved 26 January 2010)

[118] Francis, B. (2005) 'Hacker Sells Their Information Anonymously through Secretive Websites. Know thy hacker'. *Infoworld*, 28 January, on the Internet: http://www.inoworld.com/article/05/28/05OPPsecadvice_11.html (retrieved 27 August 2009)

[119] 'Transmission. Behind The Estonia Cyberattacks'. 8 March 2009. On the Internet: http://www.rferl.org/Content/Behind_The_Estonia_cyberattacks/1505613.html (retrieved 26 January 2010)

effect of the attacks is that Estonia has strengthened its cyber emergency response team. In cooperation with NATO, a cyber security centre with the official name Cooperative Cyber Defence Centre of Excellence (CCD COE) was set up in August 2008, usually referred to by the code name K5. In total a group of 30 experts are permanently stationed in the Tallinn area.[120] Estonia is working on a national cyber defence strategy. It involves factors such as making the backbone Internet infrastructure more robust and expanding the Internet throughput capacity.[121] Other areas are investment in capabilities to detect cyber attacks. A method for central online operating and controlling government databases used for e-services has been implemented, called X-Road.

5.2 The cyber operation against Georgia

The cyber attack against Georgia in summer 2008 has, together with the Estonian attack, been a wake-up call highlighting the risks, threats and vulnerabilities of information warfare. New insights have been gained regarding the means and methods by which an aggressor could act on the Internet to conduct computer network operations in conjunction with psychological and military activities against an adversary. Basically this is the first time an online operation has been combined with a military offensive.[122]

The cyber conflict shows some interesting features in the way in which it was prepared and conducted as well as the consequences. A new modus operandi can be discerned, setting the standard for future malicious activities in cyberspace. Some remarks about or characteristics of the operation are as follows.

Prelude to the conflict:

Almost two months before the actual start of the five-day military conflict between Russia and Georgia, the first distributed DDoS occurred on a small scale in June 2008.[123] The attacks were carried out by botnets using zombie

[120] Johnson, B. (2009) 'No One Is Ready for This'. *Guardian.co.uk*, 16 April 2009. On the Internet: http://www.guardian.co.uk/technology/2009/apr/16/internet-hacking-cyber-war-nato (retrieved 26 January 2010)

[121] Kash (2008) 'Lessons from the Cyberattacks'

[122] *WMD Insights*. 'Recent Events Suggest Cyber Warfare Can Become New Threat'. December 2008/January 2009 issue, on the Internet: http://wmdinsights.com/129/129_G3_recentEvents.htm (retrieved 18 December 2009)

[123] Hart, K. (2008) 'Longtime Battle Lines Are Recast in Russia and Georgia's Cyberwar', *Washington Post*, 14 August, on the Internet: http://www.encyclopedia.com/doc/1P2-17018128.html (retrieved 18 December 2009)

computers infected with malware, specifically constructed to attack designated targets.

On 20 July, multiple DDoS attacks were registered by the Shadowserver Foundation, which is an Internet watchdog group of volunteers specializing in malicious online activities. The attack was aimed at the official website of the Georgian president, which was forced to shut down for 24 hours. Analysis showed that the attack was directed by a command and control server based in the USA. The server was set up just weeks before the actual conflict started.[124]

Cyber attack coordinated with military offensive:

On 8 August, the same day as the military offensive started, with Russian forces moving across the borders of Georgia, the websites of the president of Georgia, the Georgian Parliament, the ministries of defence and foreign affairs, the National Bank of Georgia and the online news agencies were attacked by hacktivists. The websites were forced to shut down. Shadowserver detected that the first coordinated online assault was run by several different botnets. The number of cyber attacks escalated as the military conflict became more intense.[125]

Website defacements were also conducted as part of psychological pressure aimed at discrediting Georgian President Mikheil Saakashvili. Images of the president on his personal website were digitally manipulated and juxtaposed against photographs of Nazi leader Adolph Hitler.[126]

The Georgian response:

The Georgian government tried to counter the aggression in different ways. Installing attack filters to block Russian IP addresses was one method used to reduce the effects of the DDoS. Another was to move the websites of the Ministry of Foreign Affairs and civil.ge to a blogspot domain that was better protected. As the cyber conflict escalated, contacts were made with Estonia and other countries and organizations to help reduce the effects. Estonia

[124] Markoff, J. (2008) 'Before the Gunfire, Cyberattacks', *International Herald Tribune*, 13 August. On the Internet: http://www.nytimes.com/2008/08/13/technology/13iht-13cyber.15227999.html (retrieved 18 December 2009)

[125] Waterman, S. (2008) 'Analysis: Russia-Georgia Cyberwar Doubted'. *United Press International*, 14 August

[126] Porthillo-Shrimpton, T. (2008) 'Battle for South Ossetia Fought in Cyberspace', *The Independent*, 17 August

dispatched information security specialists from the national CERT to help Georgia to defend its own cyber sovereignty. Poland also helped the Georgian government by providing Polish websites to be used by the Georgian authorities to dispatch information on their view of the hostile activities.

Means and methods:

Project Grey Goose 2, an open source intelligence (OSINT) initiative led by the cyber analyst Jeffrey Carr, has tried to answer the question whether the Russian government or groups loosely connected to it was involved in the cyber operation or if it was the work of a grass-roots hacker movement alone.[127] The method the project used to unwind possible connections is based on semantic analysis of hacker blogs discussing the Georgian issue. By searching on Internet forums and blogs, the Grey Goose team member could collect information on the 'kill chain' – how novice hackers were recruited to participate, the development of target lists, the selection of malware to be used and finally the decision on how to launch the attack.[128]

Other organizations such as the US Cyber Consequence Unit (US-CCU) have also studied the issue. The result of their investigation is confidential.[129]

The Grey Goose project identified two Russian hacker forums as originators where the attacks were organized during the operation – *stopgeorgia.ru* and *Xakep.ru*. For instance, stopgeorgia.ru was set up within hours of the Russian Armed Forces invading South Ossetia. Information was constantly updated in the forum in order to instruct potential hackers on how to attack Georgian sites. Lists of target websites were featured and visitors were encouraged to download a free software program, which allowed them to participate instantly in massive DDoS attacks.

The stopgeorgia.ru website used an IP address connected to a hosting firm called Steadyhost (www.steadyhost.ru). Although the Steadyhost operator is registered in New York, it operates from St Petersburg. The interesting thing about it is that Steadyhost is believed to have its offices in the same building

[127] Project Grey Goose Phase II Report. 'The evolving state of cyber warfare'. 19 March 2009. On the Internet: http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report (retrieved 26 December 2009)

[128] Matthews, W. (2008) 'New Ways of War: Cyber attacks likely in any military conflict'. Reports. 26 October. On the Internet: http://www.defensenew,com/story.php?i=3788684 (retrieved 26 December 2009)

[129] US-CCU (2009), 'Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008'. Special report, August

as a Ministry of Defence institute, the Russian Centre for Research of Military Strength of Foreign Countries. The GRU's headquarters is also situated on the same street.[130]

As an attack method to complement DDoS, SQL injections (junk code that confuses a website's back-end database) were used to exploit application vulnerabilities within MySQL software. Millions of junk queries were sent, overwhelming the target databases with the consequence that the corresponding server became inoperable.

Compared to DDoS, SQL injection is difficult to detect and it requires fever computers to achieve the same objective as DDoS attacks. The Grey Goose report points out that the SQL injection attack 'shows moderate technical sophistications, but more importantly, it shows, planning, organization, target reconnaissance, and evolution of attacks'.

5.3 Key findings and conclusions:

The operation against Estonia was one of the first official and publicly known cyber attacks against a country using large-scale botnets and DDoS by nationalist-driven civilians. In the Georgian operation the methods were even more refined.

Both cyber operations were well coordinated in time and space and the attacker seemed to know what type of website to strike and how to take them down. This implies that computer network exploitation was prepared and other reconnaissance methods were used in advance. In the Georgian case the actual cyber operation was initiated and conducted in conjunction with the military offensive.

The Georgian operation was carried out by civilians – nationalistically oriented individuals and groups of people possibly with the support of cyber criminals. Social networks were the main tool for recruiting potential hacktivists and for providing malware to the hackers. Basically three methods were used by the attackers – distributed denial of services, SQL injections and website defacements. These were relatively unsophisticated types of attacks but carried out in an innovative way.

The targets were government and news media websites as well as Georgian financial and educational institutions. The cyber attacks reduced the ability of

[130] http://intellibriefs.blogspot.com/2009/03/cyber-warfare-project-grey-goose-phase.html (retrieved 26 December 2009)

the Georgian government to counter the Russian invasion. The defenders' resources had to be split between different activities and areas. Besides that, the operation had psychological impacts in the sense that it interfered with the government's ability to communicate with the public. The coordination between the cyber campaign and the military offensive is probably not a coincident. Any connection to the Russian authorities in both cases is very hard to prove. The Russian government rejects any accusation of intervention, and there is no evidence that it initiated or conducted the campaigns.

The events could be seen as a new modus operandi that could set the standard for future cyber conflicts. In theory, it would be possible for an actor to use nationalist hackers, thus gaining deniability together with the ability to enjoy the strategic benefits of their actions, but not sharing the risks. Moreover the cyber weapon could be used in order to put psychological pressure on opponents to act in a favourable way.

The impact of the cyber operation against the Georgian communication and information infrastructure was limited due to the low Internet penetration in the country. But it demonstrates the possible effect that could be achieved. The consequences of a well-coordinated cyber operation against critical systems and networks in more advanced countries that are dependent on modern information infrastructure would be far more serious, as the Estonia case shows. The implication of the new modus operandi points up the need for improved information security on all levels of society as well as the need to cooperate on international levels to reduce the tensions and effects of cyber attacks.

6. The need for a treaty on cyberspace

The proposal to equate cyber weapons with weapons of mass destruction, which some Russian analysts have put forward, is somewhat drastic. If a country that believed itself to be threatened by cyber attack were to resort to a deterrence strategy, this could lead to a dangerous escalation of a situation, especially bearing in mind that it is very easy to hide digital traces and to mislead adversaries in cyberspace. Such a development could in a short period of time lead in a nasty direction that would be hard to control or manage. There could be escalation more or less unintentionally. Following the cyber attacks against Estonia in 2007 and Georgia a year later, there is a growing concern that activists of different kinds could and will carry out large and coordinated cyber operations against critical objects.

Such operations could have security policy consequences and spread to other areas. A snowball effect could occur, with national security implications, and diffuse rapidly over national borders. At the same time it would be very difficult to identify the originator of a cyber attack, as well as his purpose and motives. There is an obvious risk of the wrong perpetrator being identified and of the responses to an attack being disproportionate.

Regarding the consequences, some questions arise; is the response to a potential cyber operation a task for the law enforcement authorities or a matter for the military or some other organization to deal with?[131] [132] Should it be carried out and resolved on a national level or internationally? How should phenomena such as cyber terrorism, cyber crime and cyber espionage be handled? One tricky issue is how to deal with non-state hackers engaging in every aspect of cyber aggression while providing plausible deniability to the host governments. For instance, the activities of ‘black hat’ hackers are not limited to any one specific area; they cover a wide range over the whole scale of malicious behaviours, from cyber crime to cyber warfare.

This points to the need for common criteria and agreements between all major nations on how to behave in cyberspace and the level of response if an attack occurs. There is a need for regulations and operating procedures providing guidance on how to act in order to limit consequences. The problem is

[131] The Russian opinion is that the USA sees international information security as crime control in the information sphere, ignoring the existence of information warfare weapons: see Komov, S.A., Korotkov, S.V., Rodionov, S.N. (2003) ‘International Information Security: Military aspects’, *Military Thought*, vol. 12, no. 4

[132] Ibid,

what should be regulated, how it should be regulated and in what form this should be done.

6.1 The divergence between the US and Russian views

Cyber aggression has jurisdictional and legal aspects. There is a gap and a fundamental divergence between the Russian and US views on the need to regulate hostile activities on the Internet. The US standpoint is that a treaty is unnecessary. Instead the USA advocates improved cooperation among international law enforcement groups. By cooperating to make cyberspace more secure against criminal intrusion, their work will also lead to improved security for military campaigns.[133] The USA is also resistant to any agreement that would allow governments to censor the Internet in favour of totalitarian regimes.

The Russian view is the opposite. From a Russian perspective, the absence of a treaty is permitting a kind of arms race that could have unpredicted consequences. From a Russian perspective the IW weapon' should be taken into account in disarmament negotiations in a way similar to the generalized potentials of groupings of troops (forces, weapons, combat equipment etc.). Russia has proposed a disarmament treaty that would ban a country from secretly embedding malicious codes or circuitry that could later be activated remotely in the event of war.[134] Other Russian proposals include the application of humanitarian laws banning attacks on non-combatants and a ban on deception in operations in cyberspace. The latter is an attempt to manage anonymous attacks.

Russia has been active in this area for several years. In 1998 UN General Assembly Resolution No. 53/70 was drafted from an initiative by the Russians.[135] In 2009 a Group of Governmental Experts (GGE) was set up by UNIDIR[136] to look into the impact of information communication technology on international security.[137] The reasons for the Russians' engagement in the work of UNIDIR and other forums are complex.

[133] Markoff, J., Kramer, A. (2009) 'U.S. and Russia Differ on Treaty for Cyberspace', *New York Times*, 27 June, on the Internet: http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=2&partner=rss&emc=rss (retrieved 7 December 2009)

[134] Markoff and Kramer (2009) 'U.S. and Russia Differ'

[135] Komov et al. (2003) 'International Information Security'

[136] The United Nations Institute for Disarmament Research

[137] 'ICT and International Security' (2007) *Disarmament Forum*, 3, on the Internet: http://www.unidir.org

One reason could be that they are greatly concerned about the effects of massive cyber attacks on critical information infrastructure. An operation could disrupt the system of state administration; demoralize the population; and destroy or disable key elements of the important military–industrial complex. The psychological consequences as well as the economic and military implications could be severe. Dangerous situations would arise in a very short time, spreading to other areas, and would cause pressures on the security policy level.

A second interpretation of the Russian engagement is that both the USA and China, Russia's most daring competitors, are investing heavily in information warfare capabilities, for instance, the development of an American Cyber Command under the Strategic Command, as well as the building up of the Chinese IO Corps and information militias. Bearing in mind that both the USA and China are major suppliers of hardware and software worldwide there is a fear on the Russian side of implanted back-door functionalities and logic bombs hidden inside computers and networks. Russia, on the other hand, does have very good skilled programmers and competitive software companies within the information security area.

The Russians might have the feeling that they are lagging behind their opponents, and in their experience regulation could be one way to gain control over the progress the opponent is making. Bogdanov for instance points out that during recent decades Russia's military-economic capacity has seriously weakened and the Ground Forces 'have not more than 20 percent of modern weapons and military equipment'.[138] Moreover, 'The Russian military will have to fight with weapons that are qualitatively inferior to those of possible adversaries on a number of parameters, especially regarding communication and intelligence systems as well as EW and precisions guided weapons'. The statement could of course be a part of a *maskirovka* in the sense that the Russians are presenting themselves publicly as weaker than they actually are in order to win time to build up their resources. Information from the Georgian five-day war shows that Russia to some extent lacks sufficient EW equipment.

A third reason could be that the Russians want to act proactively in order to tone down the ongoing discussions in various forums indicating that activists from Russia were behind the cyber attacks against Estonia in 2007 and Georgia in 2008 – suggestions which Russia strongly denies. There is no evidence that Russian authorities or groups connected to them have been involved in the cyber conflicts, although non-confirmed information on the

[138] Bogdanov (2004) 'Warfare of the Future'

Internet points out that persons connected to the Russian authorities might have encouraged patriotic hackers to act in the early phases of the Estonian and Georgian conflicts. By engaging with regulatory bodies for cyber protection, Russian could win political points. Major-General Alexander Burutin, acting deputy chief of the General Staff, has mentioned the need to establish an 'Agency for positive image of Russia' to counteract negative attitudes towards the country.[139]

This said, however, there are some areas where Russia is not keen on regulation. For instance, a proposal to regulate cyber criminality under a UN directive is still under consideration by the relevant Russian authority. One reason for the delay could be that many of the criminal activities conducted on a large scale worldwide originate from Russia or are connected directly or indirectly to the country. The infamous Russian Business Network, RBN, is said to be the mother of all cyber crimes.[140] There is a suspicion that there are some connections between persons related to the Russian authorities and groups dealing with cyber criminality.[141]

Whatever the possible explanations or reasons for engaging or not engaging in organizations such as UNIDIR for cyber arms control, as well as cyber crimes, cyber terrorism and cyber espionage, it is of great importance to pursue international cooperation to hinder or reduce the negative effects of antagonistic cyber operations. This issue must be solved on a broad scale involving all major parties, nations and law enforcement agencies. Conventions have to be rewritten due to the fact that cyber war confounds traditional principles such as proportionality, neutrality and distinction. Cyber rules of engagements need to be discussed.

There are many areas to be addressed and resolved. An agreement on cyberspace will have to deal with issues such as censorship of the Internet, sovereignty, and how to handle rogue actors who might not be subject to a treaty. It must also include all forms of networked and digital activities not limited to the Internet and the cyberspace but also covering the overall field of electromagnetic pulse weapons and other related areas.

[139] IntelliBriefs (2008) 'Project Grey Goose: Some lessons learned, and more to come', 22 October, on the Internet: http://intellibriefs.blogspot.com/2008/10/project-grey-goose-some-lessons-learned (retrieved 27 December 2009)

[140] O'Connell, K. (2007) 'INTERNET LAW: Russian company outed as mother of all cybercrime'. 24 October, on the Internet: http://www.ibls.com/internet_law_news_portal_view.aspx?id=1887&s=latestnews (retrieved 14 December 2009)

[141] Flook (2009) 'Russia and the Cyber Threat'

7. Conclusions

The objective of this study was to analyse Russian views on information warfare and information operations in order to get a picture of developments, ambitions and behaviour on the information arena.

From the Russian point of view information is a valuable asset per se, which it needs to protect in times of peace and war. This asset creates new dimensions to conflicts and constitutes an arena for conflicts in cyberspace with an inbuilt psychological impact. Cyberspace has emerged as a dimension in which to attack enemy centres of gravity and critical vulnerabilities and break the enemy's resistance. By using information warfare it is possible to win against an opponent, militarily as well as politically, at low cost and without necessarily occupying the territory of the enemy. It is a shift towards what some military analysts describe as 6th-generation warfare. Information warfare has become a potent weapon for power projection.

A key objective for Russia is to gain control over the Russian nation's own information and information systems in order to protect it against the influence of adversaries of various kinds as well as to have the capability to influence the opponent's important systems, such as command and control. In the Russian Military Doctrine, information protection has a strategic value and is seen as a key factor not only for the stability of the state but also for the regime and for influential and leading actors. The different interests of different actors come together into a common view on the need for security of the Russian Federation.

Russian information warfare tools are used both offensively and defensively on strategic, operational and tactical levels. Important parts of the IW toolbox are computer network operations, electronic warfare, psychological operations and mathematical programming impact, and deception activities (*maskirovka*). The mathematical programming tool is interpreted to include the introduction of malware and malfunctions such as back-door functionalities and logic bombs. Overt and covert techniques could be used to influence events and behaviour, and the actions of targeted foreign countries as well as other targets such as specific organizations and individuals.

IW could also be used as a strategy for deterrence. Some Russian officials have pointed out the risks and dangers of information warfare and spoken of the possibility of using weapons of mass destruction in order to protect the country's sovereignty and territorial integrity from large-scale cyber attacks. In the new Military Doctrine from 2010 this is not mentioned specifically.

The Russian approach has been influenced by US doctrinal thinking, although their opinions of IW and IO differ. From the Russian point of view, the USA and its modern warfare capabilities are dimensioning factors. Over a period of time, the US Army will be the superior player in many areas. But within the information warfare arena the difference in knowledge and the resource gap between the opponents are not necessarily as big as they are in other spheres. Due to the asymmetrical logic of IW, the capability could be an equalizer between the opponents and cyberspace could be the battlefield of the 21st century. It could be used in the prelude to a conflict but also as a force multiplier combined with other military capabilities. The result of IW could be to disrupt the functioning of elements of enemy infrastructure as well as a psychological impact directed to reducing the opponent's capabilities and will to fight.

Within the Russian administration several organizations are responsible for handling information warfare capabilities including all forms of networked and digital activities, not limited to the Internet and cyberspace, but also covering electromagnetic warfare and influencing campaigns. The main organizations responsible for offensive and defensive cyber capabilities are most likely to be the FSO, the FSB and the GRU. The FSB is probably the authority responsible for information security for the Russia Federation.

In 1995, the Law on Operative Search and Seizures permitted the FSB to use the practices of tapping telephone lines, opening mail and monitoring other communication channels such as the Internet. The FSB uses a system called SORM II for monitoring Internet traffic. At the FSB's request, all ISPs in Russia have to invest in the SORM system for legal intercept. The Russian Federation's right to protect what is seen as strategically important information transmitted through the ether and on the Internet is described in the Information Security Doctrine from 2000. The doctrine as it is defined implies a psychological dimension related to the stability of the state. It is directed at the country's own population as well as against what are seen as foreign influencing campaigns.

One growing concern is malicious activities emanating from Russia, such as cyber criminality and cyber espionage. In some cases, the country is seen as a safe haven for cyber criminality directed against foreign interests and to some extent domestic cyber criminality. The black economy of hackers, data burglars and code thieves is a multibillion-dollar business. Spreading malware and spamming worldwide causes a great deal of distraction from the real work of governments and businesses. The critics point out that the law enforcement agencies have not acted resolutely enough to deal with the lawbreakers. One of the largest criminal networks on the Internet, the RBN, originates from Russia. The group is seen as a premier cyber criminal organization. The well-coordinated and sophisticated identification of target objects to attack indicates a connection to 'traditional' criminals and mafias. But it is uncertain if the network still exists.

Nationalist-driven hacktivism is another problem. The cyber attacks on Estonia and Georgia show that a relatively small, skilled and dedicated group of individuals using social networks as tools for recruiting and for providing malware to the hackers can have a major impact. The attacks against Georgia were relatively unsophisticated, using distributed denial of services, SQL injections and Web defacements, but were carried out in an innovative way. The 'physical' effects were small due to a low Internet penetration and a low level of dependence on advanced communication infrastructure in the country. But the psychological impact was high in the sense that it interfered with the government's ability to communicate with the public. Moreover, the government's resources had to be split between different activities and areas.

For a more advanced country that is dependent on modern information and communication technologies – as showed by the Estonian case – the consequences of coordinated cyber attacks for the society could be severe.

Both incidents set a standard for how future cyber conflicts could be conducted. It is more or less impossible to pinpoint the originator or to tie an actor to a specific operation. The new modus operandi gives deniability for actors in combination with strategic benefits such as obtaining political goals. The possibility to deny any involvement could be a tempting driver for an aggressor. The implication is that the IW weapon will be used more in future conflicts both as a stand-alone method and in conjunction with military operations. Moreover the development of a new modus operandi gives a psychological impact that could be used for deterrence and to put pressure on adversaries.

But there are risks involved in using independent groups of antagonists such as hacktivists. An originator could not be certain either of the antagonists' real motives and will to be involved in an operation or of the effects achieved. A highly connected citizen could, for example, act patriotically on the Internet but in the same time be critical of government repression. It is a dualistic problem. Moreover, there is always a risk of undesired consequences connected to hacktivism. There is a possibility that hacker groups from an opposed side will engage in the cyber struggle and the contracting parties will gradually raise the stakes and thereby also the level of risk. Such a development could quickly lead in a dangerous direction that would be hard to control or manage. There could be escalation, more or less unintentionally. Such operations could have security policy consequences and therefore spread to other areas as well. A snowball effect could occur with national security implications and also diffuse rapidly over national borders. At the same time it would be very difficult to know who or what groups initiated the attack and for what purpose. There is an obvious risk of the wrong perpetrator being pinpointed and of the responses to an attack being disproportionate.

The emerging cyber threats show the need to improve both information security and international cooperation in order to hinder or reduce the negative effects of antagonistic cyber operations. The issue of cyber threats must be resolved on a worldwide scale, involving all major parties and the law enforcement agencies of all nations. Conventions have to be rewritten because cyber warfare confounds principles such as proportionality, neutrality and distinction. Cyber rules of engagement need to be discussed further.

Abbreviations

Bot – a computer infected by a virus, worm, or other malware that reprograms the computer to respond, on command, to an outside server

Botnet – a network of compromised computers

Carding – the process of verifying stolen credit card data before using it for large-scale fraud

CC&D – camouflage, concealment and deception

CERT – Computer Emergency Response Team, responsible for cyber incident reporting

Command and control (C&C) server – the server that controls bots in a denial of service attack

Cyberspace – a global interconnected communication and information system often referred to as the virtual community space, facilitated mainly by the medium of the Internet and involving all forms of networked and digital activities

Cyber attack – an attack that involves the cyber domain

Cybercrime – any criminal activity that takes place in, through, or directly with cyberspace

Cyber security – the field of maintaining the integrity and confidentiality of systems, networks, equipment, and communications that use cyberspace

Cyberterrorism – the premeditated threat or use of disruptive activities against computers and networks, with the goal of causing harm or intimidation or to further a political, social, religious, or other agenda

Cyberwarfare – a wide range of activities in cyberspace directed against adversaries with the cause to widespread harm. Cyber attacks could take place alongside actual military operations

DoS attack –a denial of service attack is a cyber attack with the intent of making a computer resource unavailable; the most typical method involves overloading a machine, website or server with external communication requests, slowing it down and preventing it from receiving or responding to legitimate requests

DDoS attack – a distributed denial of service attack originates from multiple compromised computers; the individual computers become part of the bot network controlled by the C&C server

ELINT – Electronic Intelligence

FAPSI – the Federal Agency of Government Communication and Information

FSB – the Federal Security Service

FSO – the Federative Protection Service

GUSP – the Main Directorate of Special Programs of Russia Federation

GRU –Military Intelligence

Hacktivist – a hacker who has a political, religious and or nationalistic purpose

IMINT – imagery intelligence

IO – information operations

ITKS – Information and Telecommunication System

IW – information warfare

Malware – malicious software designed to infiltrate or damage a computer or server

Maskirovka – deception

MILDEC – military deception

MTR – Military Technical Revolution

NCW – network-centric warfare

OSINT – open source intelligence

Phishing – a form of fraud involving trying to obtain sensitive information by masquerading as a legitimate or trustworthy entity

RBN – the Russia Business Network

RMA – Revolution in Military Affairs

SIGINT – Signals intelligence

UNIDIR – United Nation Institute for Disarmament Research

SATINT – Satellite intelligence

Script kiddie – an amateur malicious hacker (usually someone who uses programs developed by others)

SIO – Special Information Operation

SORM – a Russian acronym for System for Operational-Investigative Activities

Spamming – abusing e-mail to indiscriminately send bulk messages

STRATCOM – Strategic Command

SVR – the Foreign Intelligence Service

SQL injection – inducement of junk code to confuse website's back-end databases

Trojan – a type of malware that masquerades as something useful or something that performs a desired function

Virus – a malicious computer program that can copy itself and infect a computer without the permission or knowledge of the computer's user

Worm – a self-replicating program that uses the network to send copies of itself to other computers; unlike viruses, which usually damage the infected computer, worms usually damage the network

Bibliography

Alberts, D., Gartska, J., Stein, F. (1999) ‘Network Centric Warfare: Developing and Leveraging Information Superiority CCRP’. *Publication services.* Revised August 1999 (2nd edition), on the Internet: http://www.dodccrp.org/files/Alberts_NCW.pdf (retrieved 15 November 2009)

Ackerman, R. (2009) ‘Threats Imperil the Entire U.S. Infrastructure. From the military to the economy, the country is open to vast damage’, *SIGNAL.* AFCEA International Journal, July

Babaeva, S. (2003) ‘VALENTIN KORABELNIKOV: *SMART AND WELL-TRAINED PEOPLE WORK WITH US.* An interview with the chief of Russian military intelligence’, *CDI Russia Weekly,* 17 July, on the Internet: http://www.cdi.org/russia/265-17.cfm (retrieved 26 January 2010)

Barret, B.M. (2008) ‘Information Warfare: China’s response to U.S. technological advantages’, *International Journal of Intelligence,* vol. 18, no. 4

Bennet, G. (2000) ‘FAPSI - The Federal Agency of Governmental Communication & Information’. On the Internet: http://kgb-militaryschool.com/view/Fapsi (retrieved 15 December 2009)

Bogdanov, S.A. (2004) *‘*Warfare of the Future’, *Military Thought*, vol. 13, no. 1

Bremmer, I., Charap, S. (2006/07*)* ‘The Siloviki’s in Putin’s Russia. Who they are and what they want’*, Washington Quarterly*, Winter. Centre for Strategic and International Studies and Massachusetts Institute of Technology, on the Internet: http://www.twq.com/07winter/docs/07winter_bremmer.pdf. (retrieved 14 January 2010)

Carman, D. (2002) ‘Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass media and the politics of identity’. *Pacific Rim Law & Policy Journal Association*

Chuen, C. (2006) ‘Russia: Government and Selective Ministries’. Updated 23 January 2006. *NTI, Centre for Non-proliferation Studies at Monterey Institute of International Studies*, on the Internet:

http://www.nti.org/db/nisprofs/russia/govt/ministry.htm (retrieved 12 December 2009)

CRS Report for Congress. Cyber warfare. Updated 19 June 2001, on the Internet: http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL30735_06192001.pdf (retrieved 20 November 2009)

'Doktrina Informatsionnoi Bezopasnosti Rossiiskoi Federatsii', on the Internet: http://www.scrf.gov.ro/Documents/Decree/2000/09-09. html. The document is translated and discussed for instance in Carman, D. (2002). 'Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass media and the politics of identity'. *Pacific Rim Law & Policy Journal Association*

Donskov, Y., Nikitin, O.G. (2005) 'Special Information Operations in Armed Conflicts', *Military Thought,* vol. 14, no. 3

Dylevsky, I.N., Komov, S.A., Korotkov, S.V., Rodionov, S.N., Fedorov, A.V. (2007) 'Russian Federation Military Policy in the Area of International Information Security: Regional aspect', *Moscow Military Thought*, 31 March, referred to by Carr, J., 27 July 2009 at http://intelfusion.net/wordpress/?tag=russia
(retrieved 26 December 2009)

Fitzgerald, M. (1994) 'Russian Views on Electronic Warfare. The growing role of information-technology is rapidly lowering the barrier between war and peace'. Power point pictures. www.nationalstrategies.com

Fitzgerald, M. (1996) 'Russian Views on Information Warfare'.
Hudson Institute, Washington D.C., USA. December

Flook, K. (2009) 'Russia and the Cyber Threat', 13 May, on the Internet: http://www.criticalthreats.org/russia/russia-and-cyber-threat (retrieved 12 December 2009)

Galushkin, A., Koroba, S., Kazantsev, P. (2003) 'Neuromathematics: development tendencies', *Applied Computer.* Math. 2 , no. 1, on the Internet: http://www.elm.az/acm/pp.57-64.pdf (retrieved 20 December 2009)

Grau, L-W., Thomas, T. (1996) 'A Russian View of Future War: Theory and direction'*, Journal of Slavic Military Studies*, issue 9.3 (September), pp. 501–18

Hanson, S. (2001) 'Putin and the Dilemmas of Russia. Anti-Revolutionary Revolution', *Current History*, 333

Hart, K. (2008) 'Longtime Battle Lines are Recast in Russia and Georgia's Cyberwar'*, Washington Post,* 14 August, on the Internet: http://www.encyclopedia.com/doc/1P2-17018128.html (retrieved 18 December 2009)

Hoffman, D. (2000) 'KGB Comes in from the Cold', *Washington Post*, 8 December

InfoSecurity (2009) 'Grey Goose 2 Ties Kremlin More Closely to Georgia Cyber-attacks', 20 March, on the Internet: http://www.infosecurity-magazine.com/view/762/grey-gosse-2-ties-kremlin-more-closely-to-georgia-cyber.htm (retrieved 27 December 2009)

Keggler, J. (2008) 'Taking the Fight to the Net', *Armada International,* April/May, vol. 32, issue 2

Komov, S.A., Korotkov, S.V., Rodionov, S.N. (2003) 'International Information Security: Military aspects'*, Military Thought*, vol. 12, no. 4

Kuehl, D., National Defence University, Washington D.C. Presentation 19 November 2009 at the Swedish Defence College

Kukashkin, A.N., Yefimov, A.I. (1995) 'The Security of the Infosphere of Strategic Defence Systems', *Military Thought,* no. 5

Leijonhielm, J., Hedenskog, J., Knoph, J., Larsson, R., Oldberg, I., Roffey, R., Tisell, M., Westerlund, F. (2009) 'Rysk militär förmåga i ett tioårsperspektiv – ambitioner och utmaningar 2008'. Användarrapport FOI-R-2707-SE (Stockholm, FOI)

Leijonhielm, J., Westerlund, F. (eds) (2007) 'Russian Power Structures – Present and Future Roles in Russian Politics'. Base Data Report. Swedish Defence Research Agency. FOI-R-2437-SE (Stockholm, FOI)

Leijonhielm, J., Hedenskog, J., Knoph, J., Oldberg, I., Unge, W., Vendil, C. (2000) 'Rysk military förmåga i ett tioårsperpektiv. En förnyad bedömning 2000'. Användarrapport FOA-R-01758-170-SE (Stockholm, FOA)

Leijonhielm, J., Clevström, J., Nilsson, P.-O., Unge W. (2002) 'Den ryska militära resursbasen. Rysk forskning, kritiska teknologier och vapensystem'. Användarraport FOI-0618--SE Stockholm

Li Yinnan (1996) 'New Subjects of Study Brought About Information Warfare', *Jiefangjun Bao*

Limno, A.N., Krysanov, M.F. (2003) 'Information Warfare and Camouflage, Concealment and Deception', *Military Thought,* vol. 12, no. 2

MacQuaid, J. (2008) 'The RBN Operatives Who Attacked Georgia Secure Home Network'*,* 18 August, on the Internet: http://securehomenetwork.blogspot.com/2008/08/rbn-operatives-who-attacked-georgia.html (retrieved 12 December 2009)

Markoff, J. (2008) 'Before the Gunfire, Cyberattacks', *International Herald Tribune,* 13 August, on the Internet: http://www.nytimes.com/2008/08/13/technology/13iht-13cyber.15227999.html (retrieved 18 December 2009)

Markoff, J., Kramer, A. (2009) 'U.S. and Russia Differ on Treaty for Cyberspace', *New York Times,* 27 June 27, on the Internet: http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=2&partner=rss&emc=rss (retrieved 7 December 2009)

Matthews, W. (2008) 'New Ways of War. Cyber Attacks Likely in Any Military Conflict' *Reports.* 26 October, on the Internet: http://www.defensenew,com/story.php?i=3788684 (retrieved 26 December 2009)

Mowthorpe, M. (2005) 'The Revolution in Military Affairs (RMA): The United States, Russian and Chinese Views'. *University of Hull,* vol. 5, no. 2 (Summer 2005)

Niu, Li., Jiangzhou, Li., Dehui, Xu (2000) 'Planning and Application of Strategies of Information Operation in High Tech Local War', *Zhongguo Junshi Kexue* (China Military Science), no. 4, 20 August

Nunes, V. (1999) ‘The Impact of New Technologies in Military Arena: Information Warfare’. Conference paper: International Congress of Military Press, Lisbon, 13–16 September

O’Connell, K. (2007) ‘INTERNET LAW - Russian company outed as mother of all cybercrime’, 24 October 2007, on the Internet: http://www.ibls.com/internet_law_news_portal_view.aspx?id=1887&s=latestnews (retrieved 14 December 2009)

Osipovich, A. (2007) ‘Inside a Hacker School’, *Foreign Policy*, issue 163 (November/December)

Pike, J. (1997) ‘Federal Protection Service (FSO)’, 26 November, on the Internet: http://fas.org/irp/world/russia/fso/index.htm (retrieved 12 December 2009). Also described in Directory of Defense Related Agencies and Personnel’s from the CIA’s website the Foreign Broadcast Service (FBIS) at http://ftp.fas.org/irp/world/russia/fbis/MAININDEXPAGE.html

Pirumov, V. (1996) ‘Nekotorye aspekty informatsionnoi voiny’ (Certain aspects of information warfare). Conference speech in Brussels May 1996, referred to in Thomas (1998a)

Porthillo-Shrimpton, T. (2008) ‘Battle for South Ossetia Fought in Cyberspace’, *The Independent*, 17 August 2008

Rastorguyev, S.G. (1998) ‘Informatsionnoi Voiny’ (Information warfare). Radio i Svjaz, Referred to in Thomas 2004

Richard, J. (2008) ‘Number of Computer Viruses Tops One Million.’ *Times online,* 10 April, on the Internet: http://technology.timesonline.co.uk/tol/news/tech_and_web/article3721556.ece (retrieved 13 December 2009)

Serookiy, Yu. (2004) ‘Psychological-Information Warfare: Lessons of Afghanistan’, *Military Thought,* vol. 13, no. 1

Sokov, N. (2004) ‘Russia’s 2000 Military Doctrine’. Revised July 2004, on the Internet: http://nti.org/dbnisprofs/over/doctrine.htm (retrieved 11 December 2009)

Shactman, N. (2008) ‘U.S. Embassy in Russian Hackers’ Crosshairs?’, 12 August, on the Internet: http://www.wired.com/dangerroom/2008/08/investigators-a/ (retrieved 12 December 2009)

Shactman, N. (2009) 'Kremlin Kids: We Launched the Estonian Cyber War'. *Wired.* 11 March, on the Internet: http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/ (retrieved 14 December 2009)

Shcherbakov, A.' Major Loss of Intelligence Gathering Capacity', on the Internet: http://www.fas.org/irp/world/russia/fapsi/shcherbakov.htm (retrieved 20 December 2009)

Staar, R., Tacosa, C. (2004) 'Russia's Security Services', *Mediterranean Quarterly*, vol. 15, issue 1

Thomas, T. (2004) 'Russian and Chinese Information Warfare: Theory and Practise'. *Foreign Military Studies Office,* Fort Leavenworth. PowerPoint. June.

Thomas, T. (2003) 'Manipulating the Mass Consciousness: Russian & Chechen information war. Tactics in the second Chechen–Russian conflict'. 14 April, on the Internet: http://call.army.mil/fmso/fmsopubs/issues/chechiw.htm (retrieved 15 November 2009)

Thomas, T. (1998a) 'Dialectical versus Empirical Thinking: Ten Key Elements of Russian Understanding of Information Operations' *FMSO Special Study Center For Army Lesson Learned*. Fort Leavenworth, KS 66027-1327

Thomas, T. (1998b) 'Russia's Information Warfare Structure: Understanding the roles of the Security Council, FAPSI, the State Technical Commission and the military', *European Security,* vol. 7, no. 1 (Spring), pp. 156–72

Thomas. T.(1996) 'Deterring Information Warfare: A New Strategic Challenge'. IWS - the Information Warfare Site. Reviewed 7 November 1996, on the Internet: http://www.iwar.org.uk/iwar/resources/parameters/iw-deterrence.htm (retrieved 16 November 2009)

Tsymbal. V.I. (1995) 'Kontseptsiya Informatsionnoi Voiny' (Concepts of Information Warfare). Speech given at the Russian-U.S. conference on Evolving post Cold War National Security Issues, Moscow, 12–14 September 1995, p. 7. Cited in Timothy Thomas, 'Russian Views on Information-Based Warfare'. Paper published in a special issue of *Airpower Journal*, July 1996

Ulfving, Lars (2000) 'Den stora maskeraden', Försvarshögskolan, Stockholm

US-CCU (2009) 'Overview by the US-UCC of the Cyber Campaign against Georgia in August of 2008'. Special report. August

Vendil Pallin, C., Westerlund, F. (2010) 'Russia's Military Doctrine – Expected News'. *RUFS Briefing* no. 3, February. Swedish Defence Research Agency (Stockholm, FOI)

Vendil Pallin, C., Westerlund, F. (2009) 'Russia's War in Georgia: Lessons and Consequences', *Small Wars & Insurgencies,* vol. 20, no. 2, pp. 400–24. Swedish Institute of International Affairs, Swedish Defence Research Agency (Stockholm). On the Internet: http://dx.doi.org/10.1080/09592310902975539 (retrieved 20 January 2010)

Vendil Pallin, C. (2006) 'De ryska kraftministerierna: Maktverktyg och maktförsäkring' [The Russian Power Ministries: Tools and the Ensuring of Powers]. Base Data Report FOI-R-2004 --SE (Stockholm, FOI)

Verisign (2008) 'The Russian Business Network. Rise and fall of criminal ISP'. *IDefence Security Report*, 8 March

'Voyennaia entsiklopedia', Vol. 5 (2001). *Voyennizdat Publishers,* Moscow

'Voyennaia Doktrina Rossiiskoy Federatsii'. Utverzhdena Ukazom Prezidenta RF ot *21 aprelya 2000 g. No. 706*, on the Internet: http://www.scrf.gov.ru/Documents/Decree/2000/706-1.html, referred to in Sokov, N 'Russia's 2000 Military Doctrine'. Revised July, 2004, on the Internet: http://nti.org/dbnisprofs/over/doctrine.htm (retrieved 11 December 2009)

Waterman, S. (2008) 'Analysis: Russia-Georgia Cyberwar Doubted.' *United Press International*, 14 August

Weigung Shen (1996) 'A New Form of People's War'. 26 June, on the Internet:http://www.fas.org/irp/world/china/docs/iw_wei.htm (retrieved 16 June 2008)

Korotchenko, Yevgenii and Plotnikov, Nikolai (1994) 'Information Is Also a Weapon: About what should not be Forgotten When Working with Personnel', *Krasnaia Zvezda*, 17 February

Young, C. (2007) 'Putin's Young "Brown Shirts"', *Boston Globe*, 10 August

Zhenxing, Pu Feng (1995) 'The Challenge of Information Warfare'. April, on the Internet: http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm, (retrieved 16 June 2008) '

Other references on the Internet

'ICT and International Security', *Disarmament Forum*, no. 3, 2007, on the Internet: http://www.unidir.org

Internet World Statistic. 'Russia Internet Usage and Marketing Report'. On the Internet: http://www.internetworldstats.com/euro/ru.htm (retrieved 21 December 2009)

IntelliBriefs. 'Project Grey Goose: Some lessons Learned, and more to come'. 22 October 2008, on the Internet: http://intellibriefs.blogspot.com/2008/10/project-grey-goose-some-lessons-learned (retrieved 27 December 2009)

http://intellibriefs.blogspot.com/2009/03/cyber-warfare-project-grey-goose-phase.html (retrieved 26 December 2009)

IT & Software Opportunities in Moscow. Moscow Investment Gateway, on the Internet: http://74.125.77.132/search?q=cache:ktOSEdAuIOcJ:moscow.e-regulations.org/Media/Editor_Repo/undp_it%2520%26%2520software.ppt+unemployment+rate+ict+sector+russia&cd=2&hl=sv&ct=clnk&gl=se (retrieved 21 December 2009)

'Project Grey Goose Phase II Report: The evolving state of cyber warfare'. 19 March 2009, on the Internet: http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report (retrieved 26 December 2009)

‘Russian Business Network (RBN)’. October 2007, on the Internet: http://rbnexploit.blogspot.com/2007_09_01_archive.html (retrieved 12 December 2009)

RU-CERT; Computer Security Incident Response Team for Russian Federation, on the Internet: http://www.cert.ru/en/about.shtml

‘Russia Reports Mobile Penetration of 131.4 %’. *Wireless Federation*. 21 April 2009, on the Internet: http://wirelessfederation.com/news/15415-russia-reports-mobile-penetration-of-131.4/ (retrieved 21 December 2009)

‘Russia Employment Rate. Trading economics.’ *Global Economics Research*, on the Internet: http://www.tradingeconomics.com/Economics/Unemployment-rate.aspx?symbol=RUB (retrieved 21 December 2009)

Security Council of the Russian Federation (2006)
’Dostav Mezhvedomstvennoi kommissii Soveta Bezopanosti Rossiiskoi Federatsii po informatsionnoi bezopasnosti po dolzhostiam,’ *Presidential Decree* No. 601, 12 June on the Internet: http://www.scrf.gov.ru/documents/46.html
(retrieved 5 February 2010)

‘Siloviki’. Global Security.Org, on the Internet: http://www.globalsecurity.org/military/world/russia/siloviki.htm

Speech in Info-Forum February 10, 2008 Referred to by Carr in AppSec Asia Conference, 17 November 2009

Wapedia, on the Internet: http://wapedia.mobi/nashi_(youth_movement) (retrieved 14 December 2009)

WMD Insights. ‘Recent Events Suggest Cyber Warfare Can Become New Threat’. December 2008/January 2009 Issue, on the Internet: http://wmdinsights.com/129/129_G3_recentEvents.htm (retrieved 18 December 2009)