2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

Russia's Public Stance on Cyberspace Issues

Keir Giles
Conflict Studies Research Centre
Oxford, UK
keir.giles@conflict-studies.org.uk

Abstract: Russian views on the nature, potential and use of cyberspace differ significantly from the Western consensus. In particular Russia has deep concerns on the principle of uncontrolled exchange of information in cyberspace, and over the presumption that national borders are of limited relevance there. Circulation of information which poses a perceived threat to society or the state, and sovereignty of the "national internet", are key security concerns in Russia.

This divergence undermines attempts to reach agreement on common principles or rules of behaviour for cyberspace with Russia, despite repeated Russian attempts to present norms of this kind to which other states are invited to subscribe.

This paper examines aspects of the two most recently released public statements of Russian policy on cyberspace: the "Draft Convention on International Information Security" (released 24 September 2011) and the Russian military cyber proto-doctrine "Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space" (released 22 December 2011) in order to describe the Russian public stance on cyberspace. Conclusions are drawn from the "Conceptual Views" on how the Russian Armed Forces see their role in cyberspace. The documents are referenced to the Information Security Doctrine of the Russian Federation (2000) as the underpinning policy document prescribing Russia's approach to information security overall, including its cyber elements.

The Russian authorities considered that protests over the State Duma election results in December 2011 arose at least in part because of a cyber/information warfare campaign against Russia. The informational and political response of the Russian authorities to this is taken as a case study to measure the practical impact of the Russian views outlined above. In addition, the dynamics of the London International Conference on Cyberspace are referenced in order to illustrate failure to achieve dialogue over the difference of these views from the Western consensus.

Keywords: *Russia, information security, social media, civil protest, policy, military*

1. INTRODUCTION

To external observers, dialogue between Russia and Western partners on cyberspace issues seems characterised by mutual incomprehension and apparent intransigence. Norms which are taken for granted on one side are seen as threatening by the other, and the lack of a common vocabulary or common concepts relating to cyberspace means that even when attempts are made to find common ground, these attempts soon founder.

According to Russia’s Communications Minister Igor Shchegolev, “for the time being, in the West not everybody always understands what rules we are following” [1]. This remains true despite the fact that Russia has for over a decade been attempting to gather international support for these rules in a variety of international fora including the United Nations [2] and others [3].

This paper reviews two of the most recent public statements of the Russian approach to information security, a concept which carries cyber security implicitly within it, in order to extract key principles of the Russian approach. It then measures these principles against official and unofficial Russian state action against protest movements following the parliamentary elections in December 2011.

2. THE DRAFT CONVENTION

In September 2011, a “Draft Convention on International Information Security” was released at an “international meeting of high-ranking officials responsible for security matters” in Yekaterinburg, Russia, narrowly post-dating the “International Code of Conduct for Information Security” presented by Russia and other states at the United Nations [4].

The key provisions of the document have been condensed into a list of 23 fundamental issues of concern to Russia in information space by the Institute of Information Security Issues (IISI) of Moscow State University, which is closely engaged in developing the draft Convention. These issues, each of which is reflected in one or more articles of the proposed document, include some provisions which should excite no controversy in any part of the world, such as avoidance of breaches of rights and freedoms, or “criminalisation of use of information resources for illegal purposes”. But at the same time, a number of the issues raised run counter to the views on use and governance of the internet that have emerged in the USA, UK and other like-minded states – a system of views which forms an unstated but nonetheless tangible concurrence - referred to further, for brevity and clarity, as “the Western consensus”. This consensus, while regularly voiced at international events like the London International Conference on Cyberspace on 1-2 November 2011, is also expressed in a number of published international documents, for example the Organisation for Economic Cooperation and Development (OECD) recommendations on principles for internet policy making released shortly afterwards [5].

A key divergence between Russian and Western approaches to cyber security is the Russian perception of content as threat [6]. In the Russian list of issues of concern, this is expressed as the “threat of the use of content for influence on the social-humanitarian sphere”. By contrast, the Western consensus recognises the threat from hostile code, but generally discounts the issue of hostile content. The OECD recommendations referred to above, for example, include

> free flow of information and knowledge, the freedom of expression, association and assembly, the protection of individual liberties, as critical components of a democratic society and cultural diversity [5]

It is regularly stated as a fundamental principle “that cyberspace remains open to innovation and the free flow of ideas, information and expression”, as stated by UK Foreign Secretary William Hague and others at the London Conference referred to above [7]. Yet at the same conference, Minister Shchegolev attached important caveats to the principle of free flow of information: this should be subject both to national legislation, and to counter-terrorism considerations - chiming with another principle on the list, “restrictions of rights and freedoms only in the interests of security” [8].

Thus while both sides publicly espouse the freedom of exchange of information, and thus occasionally give the illusion of consensus, the Russian reservations on how far this principle can safely be extended mean that in practical terms the two views are as far apart as ever.

Two further issues identified by IISI, “Refraining from using information and communications technology to interfere in the affairs of other states” and “Threat of use of a dominant position in cyberspace” lie behind the perception voiced by certain sections of the Russian leadership that protests following the parliamentary elections in December 2011 were inspired, facilitated and financed from abroad - to be discussed further below. In particular, the mention of a “dominant position in cyberspace” refers to the idea of “information space [being] a place of competition over information resources... The USA is currently the only country possessing information superiority and the ability significantly to manipulate this space [9].”

The principle of indivisibility of security is highlighted in the draft Convention. Here again, apparent consensus hides fundamental disagreement - simply because this common phrase has entirely different meanings in Russian and in English. Despite recognition and patient explanation that use of the identical phrase to refer to widely differing concepts leads to misunderstanding and frustration [10], the phrase continues to occur in both Western and Russian discourse leading to each side embarking on their own separate conversation [11].

“Internet sovereignty” is another key area of disagreement. Russia, along with a number of like-minded nations (for example members of the CIS, CSTO and SCO), strongly supports the idea of national control of all internet resources that lie within a state’s physical borders, and the associated concepts of application of local legislation - or as worded in the draft Convention itself, “each member state is entitled to set forth sovereign norms and manage its information space according to its national laws” (Article 5.5). This is in direct opposition to the approach of, for example, the USA, as expressed firmly by US Secretary of State Hillary Clinton in December 2011, saying that countries like Russia wished to

> empower each individual government to make their own rules for the internet that not only undermine human rights and the free flow of information but also the interoperability of the network. In effect, the governments pushing this agenda want to create national barriers in cyberspace. This approach would be disastrous for internet freedom [12].

The list of underlying principles provided by IISI includes “Taking essential measures to prevent destructive information activity from territory under the jurisdiction of a state”. This vaguely-worded but ominous-sounding provision refers to a section in the draft Convention which covers states ensuring that information infrastructure within their own jurisdiction is not used for hostile activity, and cooperating in order to identify the source of such activity. (Article 6.2). Consideration of the practical implications of a stipulation of this kind, and the obligations it entails, leads quickly to the realisation of an enormous legislative and administrative burden on states which might wish to subscribe to the draft Convention. Not only must they supervise the legality of content within their own jurisdiction, but also ensure that it is considered inoffensive and non-hostile in the jurisdictions of all other signatories – otherwise, they can immediately be accused of permitting hostile activity in breach of the Convention.

Another key stipulation which is gravid with misunderstanding is the provision for “taking measures of a legal or other nature which are essential for access with grounds and in a legal manner to specific parts of the information and communications infrastructure of a State Party”. In the current text of the draft Convention, this appears as “take necessary steps of legislative or other nature which will guarantee lawful access to specific parts of the information and communication infrastructure in the territory of the State Party which are legally implicated in being employed for the the perpetration of terrorist activities in information space” (Article 9.5).

Two important areas of conceptual divergence arise here: first, the mention of “terrorism”, and second, the issue of access to a foreign state’s information space.

Conceptual differences in the understanding of the nature of “terrorism” between Russian and other states provide an additional layer of complexity and indeterminacy to the already muddied picture of what constitutes “cyberterrorism”. As described by Anna-Maria Talihärm [13], Alex Michael [14] and others, “there is a great abundance of different definitions of the idea of ‘terrorism’... the addition of the prefix “cyber” has only extended the list of possible definitions and explanations”.

Thus without consensus with Russia on what precisely is covered by “perpetration of terrorist activities in information space”, this clause remains unusable. Such consensus is unlikely to be achieved given the fundamental and unresolved differences between the two sides on what constitutes both terrorism and counter-terrorist activity [15].

At the same time the call for authorised access to information infrastructure in another state’s jurisdiction is reminiscent of the text of Article 32 of the Council of Europe Convention on Cybercrime (the Budapest convention):

> A Party may, without the authorisation of another Party... access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system [16].

- yet this text constitutes Russia's main objection to ratification of the Budapest convention [17]. The key phrase which prompts Russian objections is "without the authorisation of another Party". In the Russian view, this is an intolerable infringement on the principle of sovereignty as described above. In addition, the range of options covered by "the person who has the lawful authority to disclose the data" is a source of concern, including as it may organisations other than the State. Russian concerns over practical application of the Budapest convention are illustrated by a report in the official government newspaper which highlighted the "dubious provision for foreign special services to invade our cyberspace and carry out their special operations without notifying our intelligence services" [18].

In sum, then, the articles of the draft Convention and its underlying principles serve well to illustrate the two emerging consensuses on governance of the Internet: the Western one, insisting on the free, unrestricted and ungoverned flow of information, and the consensus espoused by Russia and like-minded states, with important caveats on the flow of information and an insistence on national sovereignty in cyberspace.

3. "CONCEPTUAL VIEWS"

The most recent official Russian policy statement on cyber issues to be published at the time of writing is the "Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space". This document was presented at an information security conference in Berlin on 14 December 2011 [19], and released in text form on 22 December 2011 [20].

Despite a large volume of previous semi-official literature on information warfare, this is the first explicit public statement of the Russian military's role in cyberspace, and has been described as a Russian military cyber proto-doctrine. When compared to similar documents released in the USA, UK and elsewhere, it is as interesting both for what it includes and for what it omits.

This is a specifically Russian document, and does not resemble its foreign counterparts, for example the US Department of Defense Strategy for Operating in Cyberspace [21] - not only through references to supporting doctrinal documents (the Military Doctrine and Information Security Doctrine of the Russian Federation) but also in its underlying presumptions and definitions of information challenges.

In this way it reflects a long-standing recognition not only that potential operations in information space pose an entirely new set of challenges [22], but also that foreign concepts of information security, along with those of other areas of military endeavour, are not applicable to Russian circumstances - as expressed in 1995 by prominent Russian military commentator Vitaliy Tsymbal:

> It is false to presume that we can expediently interpret and accept for our own use foreign ideas about information warfare (IW) and their terminology in order to avoid confusion and misunderstanding at international discussions, during information exchanges, or during contact between specialists. Quite the opposite, it makes no sense to copy just any IW concept. Into the IW concept for the Ministry of Defence of the Russian Federation (RF) must be incorporated the constitutional requirements of the RF, its basic laws, specifics of the present economic situation of the RF, and the missions of our Armed Forces [23].

With the exception of references to the economic situation, this is precisely what the Views have done.

They echo the defensive theme of other Russian documents relating to cyberspace, including the draft Convention described above, and cite in their preamble a statement of the external threat to Russia's information security arising from other states developing information warfare concepts [6]. Further, they state that "a targeted system of activity has been established in the Armed Forces of the Russian Federation intended to provide for effective deterrence, prevention and resolution of military conflicts in information space".

The definition of the information war which the Armed Forces are called upon to deter and prevent is worth citing in full, as it illustrates the enduring holistic nature of the Russian perception of information warfare and cyber conflict as an integral part of it. Information war, according to the Views, is

> "conflict between two or more states in information space with the aim of causing damage to information systems, processes and resources, critically important and other structures, subverting the political, economic and social systems, **mass psychological work on the population to destabilise society and the state**, and coercing the government to take decisions in the interests of the opposing side." (Section 1, Fundamental Terms and Definitions - emphasis added.)

Legality (or, we should say, conforming with Russian law and international law as interpreted by Russia) is emphasised as the first principle governing military activity. Along with customary references to the primacy of international law, and the principle of non-interference in the internal affairs of other states, the Views note that use of the Armed Forces outside the Russian Federation is subject to a process of Federal Assembly approval, and states that "this provision should also be extended to the use of the Armed Forces of the Russian Federation in information space". (Section 2.1, Legality.) The Views also make provision for "deploying forces and resources to provide for information security on the territories of other states" (Section 3.2, Resolving Conflicts.) – which leads progressively-minded non-military Russian internet experts to speculate wryly on the picture of "commandos parachuting into server centres, iPads in hand".

The first priority for the Armed Forces is stated as "striving to collect current and reliable information on threats" and developing countermeasures - but this is explicitly for military purposes. The aim is primarily to protect military command and control systems and "support the necessary moral and psychological condition of personnel". This has become essential since "now hundreds of millions of people (whole countries and continents) are involved in the unified global information space formed by the internet, electronic media and mobile communications systems". What is absent is mention of a military role in assessing or countering threats to broader society or the Russian state. (Section 2.2., Priorities.)

Russian military activity in information space "includes measures by headquarters and actions by troops in intelligence collection, operational deception, radioelectronic warfare, communications, concealed and automated command and control, the information work of headquarters, and the defence of information systems from radioelectronic, computer and other influences". In common with other Russian public statements, and in contrast to similar statements from other nations [24] and overt preparations by those states [25], what is absent from the Views is any mention of offensive cyber activity. (Section 2.3, Complex Approach.)

Also in contrast to foreign doctrinal statements, the Views list "the establishment of an international legal regime" regulating military activity in information space as the main aim of international cooperation with "friendly states and international organisations". (Section 2.5, Cooperation.)

These friendly organisations are later defined: the priorities are the Collective Security Treaty Organisation (CSTO), the Commonwealth of Independent States (CIS) and the Shanghai Cooperation Organisation (SCO). But these are groups of states which have already made substantial progress in formalising their shared views on information security; views in line with those of Russia as described earlier in this paper. The CSTO has a "Program of joint actions to create a system of information security of the CSTO Member States" [26] while the SCO has concluded an "Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security" [27,6].

But in addition to this, the military are supposed to "work for the creation under the United Nations of a treaty on international information security extending the remit of commonly-accepted norms and principles of international law to information space". The Russian military is thus intended to have an explicit political role in promoting initiatives like the draft Convention on International Security referred to above, beyond simply having a voice in their drafting or having places on delegations; not a role which would sit naturally with most Western militaries.

This emphasis on international legal efforts echoes statements made by senior Russian military figures following the armed conflict with Georgia in August 2008. General Aleksandr Burutin, at the time Deputy Chief of the General Staff, said that the General Staff had recommended the development of an international mechanism to hold states to account for beginning information warfare, and furthermore that it was necessary "to move from the analysis of challenges and threats in information security to response and prevention" [28].

Both of these aspirations are reflected in the Views, and the intention to hold states to account for activity perceived as hostile which emanates from their territory is also reflected in the draft Convention as described above.

4. THE INFORMATION SECURITY DOCTRINE

Both of the documents described above make reference, either explicitly or implicitly, to the Information Security Doctrine of the Russian Federation (2000) [29].

This "doctrine", in the Russian sense of "national policy", is the fundamental document governing Russia's approach to information security, and as an integral subset of information security, cyber issues. It appears at first sight to contain the same liberal provisions for free exchange of information as called for by William Hague and Hillary Clinton as cited above. It is intended, inter alia, to "ensure the constitutional rights and freedoms of man and citizen to freely seek, receive, transmit, produce and disseminate information by any lawful means". (Article I, Part 1) It is only on closer inspection that the divergences with Western concepts and practices become clear.

A prime example lies in treatment of the media, whether state-owned or independent. The Doctrine stipulates "development of methods for increasing the efficiency of state involvement in the formation of public information policy of broadcasting organizations, other public media" (Article I, Part 4). The underlying concept, reflected in other doctrinal statements, is that media are a tool of the state for shaping public opinion in a manner favourable to the authorities. As tellingly explained by one leading Russian security specialist in the Ministry of Defence's "Red Star" newspaper:

> How can you successfully wage an information struggle if during [conflict in] Chechnya a significant part of the mass media is taking the side of the specialists? We need a law on information security [30].

- the implicit assumption being that information security must necessarily involve ensuring that the views transmitted by media, independent or not, are favourable to the government.

At the time of the release of the Information Security Doctrine, Col-Gen Vladislav Sherstyuk, then First Deputy Secretary of the Security Council of the Russian Federation responsible for information security and one of the key drafters of the document, explained that the doctrine would not be used to restrict independent media, but that nonetheless all media, government or private, must be under state supervision [31]. At the same time the visceral reaction of some sections of the Russian leadership to dissenting views voiced through independent media was evinced by the response of Prime Minister Putin to reporting on European missile defence plans by the Ekho Moskvy radio station: Putin described the experience of listening as "having diarrhoea poured over him day and night" [32]. How much more emphatic still must be the reaction of Putin, and those who think like him, to vitriolic online attacks on the current leadership via foreign-owned social media.

The Doctrine deals with issues such as these by stating that "the main activities in the field of information security of the Russian Federation in the sphere of domestic policy are … intensification of counter-propaganda activities aimed at preventing the negative effects of the spread of misinformation about the internal politics of Russia" (Article II, Part 6) as well as “development of specific legal and institutional mechanisms to prevent illegal information-psychological influences on the mass consciousness of society” (Article II Part 7). Capacity for “preventing negative effects” was tested by online organisation of mass protest rallies following the elections to the Russian parliament on 4 December 2011.

5. CASE STUDY: INFORMATION WARFARE AGAINST RUSSIA?

The official and unofficial Russian responses to protest and dissent following the parliamentary elections appeared confused and contradictory. Interference with information resources was evident, but stopped short of the complete information blockade expected by some commentators [33].

The examples given above of doctrinal concern over the circulation of information should illustrate that the permissibility or otherwise of expressing or organising dissent in cyberspace is not clear-cut. Civil protests over the election results perhaps fell in a grey area for some security practitioners in Russia between legitimate protest and dangerous subversion, leading to a mixed response including brief and sometimes ineffectual attempts to block opposition communications and internet resources.

Suspicion of foreign involvement triggered fear of subversion and “colour revolution”, linked to the pervasive Russian argument that political instability in North Africa and the Middle East resulted from the plotting of the West led by the USA [34]. In addition to the battery of colourful accusations on this topic from Russia’s more hawkish senior commentators, President Medvedev echoed the view that Russia was vulnerable to the same kind of interference. Speaking in February 2011, he said:

> Look at the situation that has unfolded in the Middle East and the Arab world. It is extremely bad. There are major difficulties ahead... We need to look the truth in the eyes. This is the kind of scenario that they were preparing for us, and now they will be trying even harder to bring it about [35].

And indeed the progress of the NATO campaign in Libya only deepened the sense of alarm felt in Russia [36] - not least because the Libya campaign precisely matched the pattern for “modern warfare” described by Chief of General Staff Nikolay Makarov in published articles including one the previous year: “use of political, economic and information pressure and subversive actions, followed by the unleashing of armed conflicts or local wars, actions that result in relatively little bloodshed” in order to achieve the aggressor’s intent [37].

Observing processes of this kind gives rise to two key concerns in Russia: first, the precedent set for interference in the internal affairs of a sovereign state with the intention of regime change; and second, the risk that intervention “could unpredictably lead to a large-scale war involving unforeseen adversaries” [37].

At the time of writing, both of these concerns are informing Russian objections to Western pressure on the Syrian government, most recently expressed in a Russian and Chinese veto of a UN Security Council resolution on 6 February 2012. But at least part of the threat perception appears to derive from mirror-imaging: projecting Russian views onto foreign partners, and assuming they proceed from motivations which appear logical and rational through a Russian prism.

As Tim Thomas points out in discussion of Russian information warfare techniques:

> Disinformation is a Russian technique that manipulates perceptions and information and misinforms people or groups of people. Some disinformation techniques are quite obvious, some are unconvincing, and others work through delayed perception, rumours, repetition or arguments. Specific persons or particular social groups can serve as disinformation targets... In Russia today, where an unstable public-political and socio-economic situation exists, the entire population could serve as the target of influence for an enemy disinformation campaign. This is a major Russian fear [38].

This fear gives rise to yet further incompatibilities between the Russian approach to internet freedom and that of other countries. At a U.N. disarmament conference in 2008 [39], a Russian Ministry of Defence representative suggested that any time a government promoted ideas on the internet with the intention of subverting another country's government, including in the name of democratic reform, this would be qualified as "aggression" and an interference in internal affairs [3]. This is immediately relevant to Russian suggestions that the USA was fostering and financing the post-election protests.

There appeared to be a coordinated campaign in response to the election protests, one neither avowed nor condemned by official Russian spokesmen. Distributed denial of service (DDoS) attacks were noted against election monitoring organisations and independent media, including against secondary targets that were reposting or hosting information from the primary list. With Twitter emerging as a key tool for organising rallies during December 2011 [40], Twitter activity by protesters was targeted for flooding by pre-positioned Twitter bots [41]. There was a formal request by the Federal Security Service (FSB) to the VKontakte social networking site to block specific pages organising protests, which was politely declined as illegal by VKontakte [42].

Yet this activity targeting opposition communications was brief in duration, and extended only a few days after the elections themselves; since when any repeat effort (at the time of writing, the most recent opposition protest of any significant size was on 4 February 2012) has been sporadic and on a much smaller scale.

One interpretation is that the Russian authorities wished to suppress communications but found the tools at their disposal to be limited. As described by analyst Kimberly Zenz, posting on LinkedIn in January 2012, "Targeting domestic sites didn't work, attempting to manipulate content on foreign sites didn't work, and domestic companies (LiveJournal and then VKontakte) did not prove to be reliable partners. Truly viable options for state management of online content appear to be lacking." This ties in with the commonly-held view that "the swift emergence of the protests caught the government by surprise and revealed its inability to understand both the degree of discontent among the Russian urban population and the growing power of social media [43].”

The sense that the online protests were permitted, although not officially in favour, left state media falling back on interviews and features describing the evils of social media, including privacy concerns over Facebook [44] and incidents of suicide following cyber bullying [45], not to mention running articles by leading information warfare theorist Igor Panarin describing the foreign-backed information campaign against Russia [46].

Meanwhile the aspiration for control of the media described above resulted, among other things, in the issuing of clear instructions to the independent media on the right way to cover pro-Putin demonstrations - the “right way” including emphasising that those present are participating spontaneously and voluntarily, and not showing officials or official buildings [47].

Other elements of “intensification of counter-propaganda activities” as per the Information Security Doctrine included a retreat to more old-fashioned methods of tackling the opposition. A succession of dirty tricks was carried out at varying levels of competence and effectiveness, from frankly poor attempts at photo editing to discredit opposition figurehead Aleksey Navalny [48], through the publication of hacked e-mails from the Golos election monitoring organisation demonstrating that it received foreign funding (which Golos had not previously concealed) [49], to the release of telephone intercepts of veteran opposition leader Boris Nemtsov obscenely excoriating fellow opposition figures [50] and the planting of fake interviews with opposition figures in US media [51]. In March 2012, a documentary by NTV, a broadcaster with a long history of turbulent and shifting relations with officialdom and the official line, attracted widespread scorn online for its hostile portrayal of the protests, their participants and organisers [52].

The mixed response to online protests appears to reflect mixed views among the Russian leadership regarding the desired extent of internet regulation. In an article entitled “USA Hides Behind Fairy Tales About Human Rights”, Secretary of the Security Council of the Russian Federation Nikolay Patrushev observed that some degree of internet regulation is essential. “Of course there should be reasonable regulation in Russia, just as it is done in the United States, China and many other countries,” Patrushev wrote [53]. This chimed with the recommendation from Maj-Gen Aleksey Moshkov of the Interior Ministry’s Bureau of Special Technical Measures (which includes Directorate K, responsible for dealing with cyber crime) that online anonymity should be restricted [54]. Meanwhile, among a range of other more ambiguous comments, Communications Minister Shchegolev stated uncompromisingly that “although cyber security and behaviour online are current problems in today’s world, blocking the internet or restricting access to social networks is unacceptable under any circumstances”. “There is an opinion that the Russian government is allegedly striving to achieve greater state control over the internet. But in Russia we are not even considering the possibility of blocking access to Twitter or Facebook, while in some European countries it has been openly stated that this will be done,” he continued [1].

6. CONCLUSION

While informed by a substantially different world view from what is commonly accepted in the West, the Russian response to online dissent following the December elections was neither as draconian as sometimes portrayed in Western commentary, nor as liberal as a superficial reading of Russian policy documents would suggest. Russia will continue to push for international agreements regulating cyberspace, along the lines of the consensus already achieved with like-minded states in the CSTO and SCO. The challenge for any Western interlocutor seeking to engage with Russia on these issues is to understand that in cyber, as in so much else, the fundamental assumptions governing the Russian approach are very different from our own – and in many cases, similar language with divergent meaning employed by the two sides serves only to mask these differences.

REFERENCES:

[1] Interfax, "Shchegolev: tsenzury Interneta v Rossii ne dopustyat," 20 January 2011. [Online]. Available: http://www.interfax.ru/print.asp?sec=1448&id=226823.

[2] T. Maurer, "Cyber Norm Emergence at the United Nations," September 2011. [Online]. Available: http://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf.

[3] T. Gjelten, "Seeing The Internet As An 'Information Weapon'," 23 September 2010. [Online]. Available: http://www.npr.org/templates/story/story.php?storyId=130052701.

[4] *International code of conduct for information security*, Annex to the letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359), 2011.

[5] OECD, "OECD Council Recommendation on Principles for Internet Policy Making," 13 December 2011. [Online]. Available: http://www.oecd.org/dataoecd/11/58/49258588.pdf.

[6] K. Giles, "Information Troops: A Russian Cyber Command?," in *Third International Conference on Cyber Conflict*, CCDCOE, 2011.

[7] W. Hague, "Chair's statement," 2 November 2011. [Online]. Available: http://www.fco.gov.uk/en/news/latest-news/?view=PressS&id=685663282.

[8] I. Shchegolev, in *London Conference on Cyberspace*, 2011.

[9] S. Modestov, "Prostranstvo budushchey voyny (The Space of Future War),," *Vestnik Akademii Voyennykh Nauk (Bulletin of the Academy of Military Science)*, No. 2, 2003.

[10] NDC, "The Indivisibility of Security: Russia and Euro-Atlantic Security," NATO Defense College, Rome, 2010.

[11] A. Monaghan, "NATO and Russia: resuscitating the partnership," May 2011. [Online]. Available: http://www.nato.int/docu/review/2011/NATO_Russia/EN/index.htm.

[12] H. Clinton, "Remarks by Hillary Rodham Clinton at Conference on Internet Freedom, The Hague, Netherlands," 8 December 2011. [Online]. Available: http://www.state.gov/secretary/rm/2011/12/178511.htm.

[13] A.-M. Talihärm, "Cyberterrorism: in Theory or in Practice?," *Defence Against Terrorism Review, Vol. 3, No. 2*, pp. 59-74, 2010.

[14] A. Michael, "Cyber Probing: The Politicisation of Virtual Attack," Defence Academy of the United Kingdom, Shrivenham, 2010.

[15] A. Monaghan, "The Moscow metro bombings and terrorism in Russia," June 2010. [Online]. Available: http://www.ndc.nato.int/research/series.php?icode=1.

[16] Council of Europe, "Convention on Cybercrime," 23 November 2001. [Online]. Available: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[17] V. P. Sherstyuk, *Presentation*, Brussels, 2011.

[18] T. Borisov, "Virtual'nyy mir zakryt," *Rossiyskaya Gazeta*, 12 11 2010.

[19] *Challenges in Cybersecurity - Risks, Strategies, and Confidence-Building*, Berlin, 2011.

[20] Russian Ministry of Defence, 22 December 2011. [Online]. Available: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

[21] US Department of Defense, " Strategy for Operating in Cyberspace," July 2011. [Online]. Available: http://www.defense.gov/news/d20110714cyber.pdf.

[22] V. M. Lisovoy, "O zakonakh razvitiya vooruzhennoy bor'by i nekotorykh tendentsiyakh v oblasti oborony," *Voyennaya Mysl'*, no. 5, 1993.

[23] V. Tsymbal, *Concept of Information Warfare*, Moscow, 1995.

[24] D. Miles, "Doctrine to Establish Rules of Engagement Against Cyber Attacks," 20 October 2011. [Online]. Available: /www.defense.gov/news/newsarticle.aspx?id=65739.

[25] T. Miles, "Army activates first-of-its-kind Cyber Brigade," 9 December 2011. [Online]. Available: http://www.army.mil/article/70611/Army_activates_first_of_its_kind_Cyber_Brigade/.

[26] Collective Security Treaty Organisation, "CSTO website," 2012. [Online]. Available: http://www.odkb.gov.ru/start/index_aengl.htm.

[27] Shanghai Cooperation Organisation, 2009. [Online]. Available: http://www.sectsco.org/EN/show.asp?id=182.

[28] ITAR-TASS, 29 January 2009.

[29] Security Council of the Russian Federation, "Information Security Doctrine of the Russian Federation (2000)," 2000. [Online]. Available: http://www.scrf.gov.ru/documents/6/5.html.

[30] G. Miranovich, "Voyennaya reforma: problemy i suzhdeniya (Military Reform: Issues and Judgements)," *Krasnaya Zvezda*, 31 July 1999.

[31] Interfax, 12 October 2000.

[32] G. Novostey, ""I don't get upset with you when you pour diarrhoea on me": Putin chats with media leaders," 19 January 2012. [Online]. Available: http://www.city-n.ru/view/296196.html.

[33] Deutsche Welle, "Russia holding back online shutdowns for now, expert says," 13 December 2011. [Online]. Available: http://www.dw.de/dw/article/0,,15599135,00.html.

[34] A. Monaghan, "Flattering to deceive? Change (and continuity) in post election Russia," March 2012. [Online]. Available: http://www.ndc.nato.int/research/series.php?icode=3.

[35] D. Medvedev, "Dmitriy Medvedev provel vo Vladikavkaze zasedaniye Natsionalnogo antiterroristicheskogo komiteta," 22 February 2011. [Online]. Available: http://www.kremlin.ru/transcripts/10408.

[36] K. Giles, The State of the NATO-Russia Reset, Oxford: Conflict Studies Research Centre, 2011.

[37] N. Makarov, "Kharakter vooruzhennoy borby budushchego (The Character of Future Armed Conflict)," *Vestnik Akademii Voyennykh Nauk (Bulletin of the Academy of Military Science)*, 2010.

[38] T. Thomas, Recasting the Red Star, Fort Leavenworth: Foreign Military Studies Office, 2011.

[39] UNIDIR, 2008. [Online]. Available: http://www.unidir.org/audio/2008/Information_Security/en.htm.

[40] R. Soloveitchik, "Twitter Becomes Key for Moscow Protests," 23 December 2011. [Online]. Available: http://www.themoscowtimes.com/arts_n_ideas/article/twitter-becomes-key-for-moscow-protest s/450350.html.

[41] B. Krebs, "Twitter Bots Drown Out Anti-Kremlin Tweets," 8 December 2011. [Online]. Available: http://krebsonsecurity.com/2011/12/twitter-bots-drown-out-anti-kremlin-tweets/.

[42] Forbes Russia, "Durov: FSB prosit "VKontakte" blokirovat oppozitsionnye gruppy," 8 December 2011. [Online]. Available: http://www.forbes.ru/news/77291-durov-fsb-prosit-vkontakte-blokirovat-oppozitsionnye-gruppy.

[43] FIIA, *Finnish Institute of International Affairs seminar, "Russian Society through the Prism of Current Political Protests"*, Helsinki, 2012.

[44] Russia Today, "Stallman: Facebook IS Mass Surveillance," 2 December 2011. [Online]. Available: http://rt.com/news/richard-stallman-free-software-875/.

[45] Russia Today, "Social networks – a threat for Russia?," 2 January 2012. [Online]. Available: http://rt.com/news/social-networks-bullying-russia-695/.

[46] I. Panarin, "December 2011: Information War against Russia," 30 December 2011. [Online]. Available: http://rt.com/politics/information-war-russia-panarin-009/.

[47] Gazeta.ru, "Ne pokazyvat i ne upominat (Don't Show and Don't Refer)," 30 December 2011. [Online]. Available: http://www.gazeta.ru/politics/elections2011/2012/01/30_a_3979953.shtml.

[48] A. Kramer, "Smear in Russia Backfires, and Online Tributes Roll In," 8 January 2012. [Online]. Available: http://www.nytimes.com/2012/01/09/world/europe/smear-attempt-against-protest-leader-backfires-in-russia.html?_r=1.

[49] Zeenews, "Russian website publishes vote monitor's e-mails," 9 December 2011. [Online]. Available: http://zeenews.india.com/news/world/russian-website-publishes-vote-monitor-s-e-mails_746183.html.

[50] G. Faulconbridge, "Phone hacking Russian style: Opposition under fire," 20 December 2011. [Online]. Available: http://in.reuters.com/article/2011/12/20/russia-phonehacking-idINDEE7BJ0AE20111220.

[51] T. Lipien, "VOA harms Putin opposition in Russia," 8 February 2012. [Online]. Available: http://www.washingtontimes.com/news/2012/feb/8/voa-harms-putin-opposition-in-russia/.

[52] *Anatomiya Protesta*. [Film]. NTV, 2012.

[53] Argumenty i Fakty, "Nikolay Patrushev: SShA prikryvayutsya skazkami o pravakh cheloveka," 14 December 2011. [Online].

[54] M. Falaleyev, "Politseyskoye upravleniye "K" predlozhilo zapretit anonimnyye vystupleniya v Internete," 8 December 2011. [Online]. Available: http://www.rg.ru/2011/12/08/moshkov.html.