Russia and Cyber Security

Keir Giles

Keir Giles is a director of Conflict Studies Research Centre (CSRC), a UK think tank specialising in Eurasian security affairs. After a firstdegree in Russian, Keir worked in aviation in the former Soviet Union before joining the BBC Monitoring Service to report on Russian economic and military affairs. A secondment to the UK Defence Academy led to work with CSRC, which Keir took into the private sector in 2010.

Resumo
A Rússia e a Cibersegurança

O artigo examina os conceitos russos de "guerra da informação" e a forma como afetam a política da Rússia face ao ciberespaço, através da análise de documentos oficiais recentemente tornados públicos, a saber: uma proposta de uma convenção internacional, e uma proto-doutrina militar de cibersegurança. Procura-se demonstrar que existe um fosso conceptual face ao Ocidente, o qual mina as possibilidades de um acordo mútuo baseado em princípios e regras comuns de utilização do ciberespaço, apesar das repetidas tentativas russas em sujeitar estas normas a aprovação por parte de outros Estados. Assim, serão necessários mais esforços no sentido de um maior e melhor entendimento conjunto se se pretender estabelecer e fortalecer uma confiança e segurança mútuas.

Abstract

This paper examines Russian "information warfare" concepts, and how they affect the Russian approach to cyberspace, through the analysis of recently released public statements of Russian policy on cyberspace: one proposed international security convention, and one military cyber proto-doctrine. It will show how the conceptual gap with the West undermines attempts to reach agreement on common principles or rules of behavior for cyberspace with Russia, despite repeated Russian attempts to present norms of this kind to which other states are invited to subscribe. Further efforts to achieve mutual understanding are essential if meaningful confidence and security building measures are to be realized.

Introduction

Russia and a range of Western nations have expressed the desire to cooperate more closely in cyber security, in particular in order to build confidence and security in cyberspace (Gorman, 2010; Blitz, 2012). But there are significant differences between the Russian and Western (for example US, UK, NATO) approaches to cyber warfare, and even between definitions of basic cyber terminology, and this severely hampers mutual understanding and cooperation in this area (Giles, 2011a). According to Russia's Communications Minister Igor Shchegolev, "for the time being, in the West not everybody always understands what rules we are following" (Interfax, 2011). 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 (Maurer, 2011) and others (Gjelten, 2010).

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", is a key security concern in Russia, but not recognized as such in the West. Russia is not alone in this, and similar concerns inform the Chinese approach to information security, which makes the achievement of mutual understanding with China on cyber security issues similarly challenging (Hagestad, 2012).

This paper examines Russian "information warfare" concepts, and how they affect the Russian approach to cyberspace, by means of studying recently released public statements of Russian policy on cyberspace: one proposed international security convention, and one military cyber proto-doctrine. It will show how the conceptual gap with the West undermines attempts to reach agreement on common principles or rules of behavior for cyberspace with Russia, regardless of the repeated Russian attempts to present norms of this kind to which other states are invited to subscribe.

Definitions and Concepts

When attempting to have a conversation about cyber issues across the language gap between English and Russian, literal translations of common terms used in discussing cyber are almost always unhelpful and misleading. In the most fundamental example, Western states talk about cyber security as a stand-alone issue, while Russia considers it more sensible to discuss information security as an

overall holistic concept, implicitly including cyber security as a subset of concerns. The lack not only of a common vocabulary but even of common concepts relating to cyberspace means that even when attempts are made to find common ground, these attempts soon founder.

In at least one instance, intensive and sincere efforts to bridge the divide have only succeeded in sowing further confusion. The "Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations" published by the EastWest Institute in April 2011 appeared at first sight to be a major step forward in achieving a common basis of understanding for the 20 key terms it selected for definition in both Russian and English; it only became clear on closer inspection that neither was this a "Russia-US bilateral" document, nor did the definitions in Russian and English actually match up with each other[1] – so in fact, the document represents a step backward by giving the impression of agreement where in fact none exists (East-West Institute, 2011b). Perhaps fortunately, an attempt in October 2011 to expand the list of definitions to a further 20 terms does not as yet appear to have borne fruit (EastWest Institute, 2011a).

The failure to achieve a common understanding of even the most fundamental concepts in cyberspace between the US, Russia and China to name but three is recognised, and is the subject of ongoing work at a number of levels. One of the topics chosen for the flagship annual conference of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn in 2013 is "Defining cyber conflict, cyber war, cyber attack, cyber weapon, etc.; (non-)essentiality and (non-)feasibility of a common terminology" (CCDCOE, 2012).

The Problem of Content

Dialogue between Russia and Western partners on cyberspace issues is hampered not only by a difference in understanding of specific concepts, but also in fundamental assumptions and in norms which are taken for granted by one side but seen as threatening by the other. One such assumption regards the free circulation of information on the internet.

1 To take one example, the definition of "Cyber Warfare" in English reads "cyber attacks that are authorized by state actors against cyber infrastructure in conjunction with a government campaign". The Russian text, however defines cyber warfare as "cyber attacks carried out by states or groups of states or organised political groups against cyber infrastructure and which are part of a military campaign" (кибератаки, проводимые государствами (группами государств, организованными политическими группами), против киберинфраструктур, и являющиеся частью военной кампании).).

The consensus among Western states is voiced at international events like the London International Conference on Cyberspace on 1-2 November 2011, and 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. (OECD, 2011). It is regularly stated as a fundamental principle in the West "that cyberspace remains open to innovation and the free flow of ideas, information and expression", as put by UK Foreign Secretary William Hague (2011) and others at the London Conference. The Western consensus recognises the threat from hostile code, but generally discounts the issue of hostile content. The OECD (2011) recommendations, 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".

Yet at the same conference, Russian Communications Minister Igor Shchegolev (2011) attached important caveats to the principle of free flow of information. This illustrates a key divergence between Russian and Western approaches to cyber security, namely the Russian perception of content as threat (Giles, 2011a). In Russian documentation, this is expressed as the "threat of the use of content for influence on the social-humanitarian sphere."

In part this results from Russian concerns that the internet can be used as a tool against Russia. The notion of content as threat is reinforced by projection onto foreign partners of Russia's own preconceptions of how international relations work, and by the presumption that a primary aim of Western powers is to disrupt and undermine Russia. As renowned expert on Russian information warfare theory Timothy Thomas (2011) points out:

> "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".

This extends to the promotion of democratic ideas: at a U.N. disarmament conference in 2008 (UNIDIR, 2008), 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 (Gjelten, 2010).

Behind and beyond direct Russian concern about targeted information attack lies a deeper and more nebulous unease about the vulnerability of Russia's national culture to outside influences – perhaps understandable in a nation which, as Timothy Thomas (2010) puts it, is "armed mentally with the experience of losing an ideology at the end of the Cold War (described by some as 'World War III')". This is another facet of the holistic approach to information security in Russia which is largely unrecognized in the West, but is expressed in Russia's Information Security Doctrine, the underpinning document defining Russia's approach to cyber issues, which includes as threats:

> "the devaluation of spiritual values, the propaganda of examples of mass culture which are based on the cult of violence, and on spiritual and moral values which run counter to the values accepted in Russian society" (Security Council of the Russian Federation, 2000; Sheynis, 2010).

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 poles apart.

Internet as Threat

This is symptomatic of a still deeper dissonance between attitudes to the internet in Russia and the West. Put simply, while the Western view of the internet is almost universally that of an opportunity and an enabler, significant sections of the Russian authorities see it instead as a threat.

In 1996, Russia faced a strategic choice of whether to embrace or reject the internet. At parliamentary hearings entitled "Russia and the Internet: The Choice of a Future," the internet as a whole was characterized as a threat to Russian national security by Vladimir Markomenko, First Deputy Director General of FAPSI, the Russian security body which at the time was responsible for cyber affairs (State Duma, 1996). This attitude can still be detected today. Speaking in April 2011, the head of the Federal Security Service (FSB) Information Protection and Special Communications Centre, Aleksandr Andreyechkin, said that:

> "Recently the problem of usage on public communications networks of encryption mechanisms, primarily of foreign manufacture, has been causing the FSB increasing concern... in particular services like Gmail, Hotmail and Skype… The uncontrolled use of these services could lead to a large-scale threat to the security of Russia".

While the real extent of this concern has been called into doubt, with some suggesting that the comments were a canard intended to lull transgressors who were using foreign internet services to exchange dubious content into a false sense of online security, the public statement does point to a continuity of views among the security structures, which continues to inform Russian attitudes to online activity and to cooperation with foreign partners.

Information Warfare and Information Weapons

Debates in the West over the nature of cyber conflict are followed with interest in Russia (Shavayev and Lekarev, 2003; Sharikov, 2009) but are not mirrored in the Russian public narrative. For example, considerations of whether cyberspace is the "fifth domain" for warfare, or simply is a common factor to the other four, did not feature in discussion visible in open sources, except in citations of Western thinking – in fact the word "cyber" is strikingly absent from home-grown Russian analysis, which until recently portrayed "cyber warfare as a purely American phenomenon, with the Chinese People's Liberation Army in a supporting role" (Sidorov, 2008; Shcherbakov, 2010).

Instead, the Russian view of "information war" (*informatsionnoye protivoborstvo, informatsionnaya bor'ba*, or increasingly commonly, *informatsionnaya voyna*) is a more holistic concept than its literal translation suggests, carrying cyber operations implicitly within it alongside disciplines such as electronic warfare (EW), psychological operations (PsyOps), strategic communications and Influence. At a time when the term has been written out of US information operations doctrine (Joint Chiefs of Staff, 2006), "information war" is still alive and thriving in Russian security considerations (Thomas, 2000; 2002; 2010).

This principle in Russian writing extends to the notion of "information weapons" – signifying a much broader tool than what we might call a cyber weapon. One characteristic study issued in 2001 noted that "propaganda carried out using the mass media is the most traditional and most powerful general-purpose information weapon," but furthermore that "information weapons are being actively developed at the present time based on programming code" – a definition which we would more readily associate with our own view of cyber weapons. As a further illustration that the Russian concept is broader and more holistic than in the West, the study went on to note that "information weapons also include means that implement technologies of zombification and psycholinguistic programming"(Fedorov and Tsigichko, 2001).

Treaty Initiatives

These Russian concerns and specific Russian views of cyberspace inform the long-standing Russian attempts to introduce international treaties or agreements to restrain the activities of states in cyberspace. As put by Professor Igor Panarin (2004) of the Russian Ministry of Foreign Affairs (MFA) Diplomatic Academy, the author of one of the standard works on Russian theory of information war, Russia needs to use "the mechanisms of the UN and the mechanisms of Russian-American consultations to create new rules of the game, rules of information balance and rules for protecting our sovereign national information space" (Panarin, 2009).

At roughly the same time as the Western consensus was being expressed by events such as the London International Conference on Cyberspace and the OECD recommendations for internet policy referred to above, a "Draft Convention on International Information Security" was released at an "international meeting of high-ranking officials responsible for security matters" in Yekaterinburg, Russia. The draft neatly illustrates many divergences between Western and Russian preconceptions about the nature of the internet and the basic assumptions on how it should be governed.

- The principle of indivisibility of security is highlighted in the draft Convention. This is a principle also espoused by Russia's foreign partners, including the US – but 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 (NDC, 2010), the phrase continues to occur in both Western and Russian discourse leading to each side embarking on their own separate conversation (Monaghan, 2011).
- The draft's 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" (Modestov, 2003). This is a concern largely unrecognised in the West.
- "Internet sovereignty" is another key area of disagreement. Russia, along with a number of like-minded nations, 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). These like-minded nations are to be found primarily among the Collective Security Treaty Organisation (CSTO), the

Commonwealth of Independent States (CIS) and the Shanghai Cooperation Organisation (SCO) – groups of states which have already made progress in formulating a common approach to cyber security. The CSTO has a "Program of joint actions to create a system of information security of the CSTO Member States" (Collective Security Treaty Organisation, 2012) 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" (Shanghai Cooperation Organisation, 2009; Giles, 2011b). Yet this sovereignty approach is in direct opposition to the approach of, for example, the USA, as expressed firmly by US Secretary of State Hillary Clinton (2011) 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".

- A section in the draft Convention covers states ensuring that information infrastructure within their own jurisdiction is not used for offensive 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 "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 perpetration of terrorist activities in information space" (Article 9.5). Two important areas of conceptual divergence arise here: first, the word "terrorist", 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 (2010), Alex Michael (2010) 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 (Monaghan, 2010).

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" (Council of Europe, 2001).

Yet this text constitutes Russia's main objection to ratification of the Budapest convention (Sherstyuk, 2011). 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" (Borisov, 2010).

It should come as little surprise, therefore, that while the provisions of the draft Convention appear perfectly sensible to Russia and other states holding similar views on the nature of the internet, they are largely incomprehensible to the Euro-Atlantic community and are therefore receiving a less than sympathetic hearing there.

The Russian Military and Cyberspace

Another recently-released document illustrating key differences between the Western and Russian approaches to cyber issues is the "Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space", released in December 2011 (Russian Ministry of Defence, 2011). This, the first official doctrinal statement on the role of the Russian military in cyberspace, describes cyber

force tasks which bear little resemblance to those of equivalent commands in the West. The differences from published doctrine in the US or UK are substantial. In particular, the "Views" contain no mention of the possibility of offensive cyber activity. The document is entirely defensive in tone, and focuses on force protection and prevention of information war, including allowing for a military role in negotiating international treaties governing information security.

At first sight, this would seem a continuation of the pattern whereby offensive cyber activity is not seen as the domain of the military. Following mixed performance in the information aspects of the armed conflict with Georgia in 2008, there was intense discussion of the possible creation of "Information Troops", whose role would include cyber capability; but this initiative was publicly scotched by the Federal Security Service (Giles, 2011a).

Indeed the vast majority of Russian public writing on cyber conflict is defensive in tone, and focused on information security and information assurance. This is at least in part a response to official discussion of cyber issues in the US in particular, where reference to defense against hostile cyber operations is balanced with references to carrying out offensive cyber operations in return. It remains the case that the stated aim of US information operations is "to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own" (Joint Chiefs of Staff, 2006) – and despite careful avoidance by the USA of casting the Russian state in the role of an adversary in cyberspace, this language is mirrored in Russia's Information Security Doctrine, which emphasizes:

> "the development by certain states of 'information warfare' concepts that entail the creation of ways of exerting a dangerous effect on other countries' information systems, of disrupting information and telecommunications systems and data storage systems, and of gaining unauthorized access to them" (Security Council of the Russian Federation, 2000).

The "Conceptual Views" is a specifically Russian document, and does not resemble its foreign counterparts, for example the US Department of Defense Strategy for Operating in Cyberspace (US Department of Defense, 2011) – 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. It reflects a long-standing Russian presumption not only that potential operations in information space pose an entirely new set of challenges (Lisovoy, 1993), 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 (1995):

> "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".

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 (Giles, 2011a). 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 once again 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 to 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". Yet once again, in common with other Russian public statements, and in contrast to similar statements from other nations (Miles, 2011a) and overt preparations by those states (Miles, 2011b), 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 CSTO, CIS and SCO, which as noted above have already made substantial progress in formalising their shared views on information security; views which are in line with those of Russia. 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.

In fact, although it was announced in March 2012 that Russia intended to create a "Cyber Security Command" (billed as a response to the creation of similar entities abroad, with particular reference to the US), references to tasks for the potential new command which tally with those foreign counterparts have to be sought elsewhere than in the published proto-doctrine. The defensive tone of the "Views" was belied by comment by Russian Chief of General Staff Nikolay Makarov (*et al.*, 2012) at a briefing which gave a very different picture of the new command's three main tasks:

- "Disrupting adversary information systems, including by introducing harmful software;
- Defending our own communications and command systems;
- Working on domestic and foreign public opinion using the media, Internet and more".

The reference to "introducing harmful software" appears to be the first official avowal of an offensive cyber role for a Russian government body, and is more in keeping with overseas concepts of the purpose of cyber commands. At the same time the third task, influencing public opinion, is a further reminder that as noted in the discussion of information weapons above, unlike some other nations with advanced cyber capabilities, Russia deals in cyber warfare only as an integral component of information warfare overall.

Russia's Information Security Doctrine

Both of the public documents discussed above build on principles established in the Information Security Doctrine of the Russian Federation, the fundamental document governing Russia's approach to information security, and as an integral subset of information security, cyber issues (Security Council of the Russian Federation, 2000).

Once again, when compared to foreign counterparts, this document 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 terrorists? We need a law on information security" (Miranovich, 1999).

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.

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).

This doctrinal concern over the circulation of information gives rise to doubt over the precise boundaries of freedom of expression in cyberspace. A highly topical issue at the time of writing which illustrates precisely this point is the passing in the Russian State Duma of a so-called "internet blacklist" bill. This widely misrepresented law is portrayed by opponents as a tool for censorship of public opinion in Russia, and in particular of dissent, whereas in fact the bill was substantially modified to address precisely these concerns (Giles, 2012). At the same time, state media reporting continues to betray unease over the uncontrolled use of social media in particular, and statements by officials convey mixed views over the basic issue of whether the internet should be viewed by Russia as an opportunity or a threat (Russia Today, 2011; 2012; Panarin, 2011).

Conclusion

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. Until now, the basic premises of these agreements have been largely rejected, or indeed ignored, by the Euro-Atlantic community (Conflict Studies Research Centre, 2012). But as Russia continues to gain support for its view of the internet among those states that discern similar threats to their security emanating from more advanced cyber powers, this competing consensus will become ever harder to disregard.

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, once again as in other areas of relations with Russia, similar language with divergent meaning employed by the two sides serves only to mask these differences. Further efforts to achieve mutual understanding are essential

if meaningful confidence and security building measures are to be realized in accordance with the newly-emerging Euro-Atlantic ambition (Blitz, 2012).

These mixed views are reflected in the manner in which the Russian authorities already possess extremely strong legislative tools for controlling content, and have at their disposal all the necessary methods for a clampdown on freedom of expression should they choose to use them, but contrary to reputation, ordinarily apply these with a very light touch. The protests over election results in Russia at the end of 2011, in large part organized using social media, provoked an example of this apparent mixed response from the authorities (Deutsche Welle, 2011; FIIA, 2012). Pressure on websites, including allegedly government-sponsored online attacks, was occasional and unsustained (Krebs, 2011) and in at least one case, subject to successful legal challenge: the Russian Facebook equivalent VKontakte (now renamed VK) refused to supply subscriber information to the Federal Security Service on the grounds that the request was illegal (Forbes Russia, 2011). Meanwhile sections of the Russian authorities defaulted to more old-fashioned, offline methods of smearing and discrediting opposition leaders (Kramer, 2012; Zeenews, 2011; Faulconbridge, 2011). This provides an indication that far from being rigid, the overall Russian attitude to online dissent is still to crystallize – a factor as applicable to domestic politics as to international initiatives. As put by Prime Minister Dmitriy Medvedev, the internet "should be regulated by a set of rules, which mankind has yet to work out. It's a very difficult process."

References

Anatomiya Protesta (2012) [Film] s.l.: NTV.

Anon. (2011a). *Challenges in Cybersecurity - Risks, Strategies, and Confidence-Building*. Berlin: s.n.

Anon. (2011b). *International Code of Conduct for Information Security*. s.l.:Annex to the letter dated September 12, 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).

Argumenty i Fakty (2011). *Nikolay Patrushev: SShA prikryvayutsya skazkami o pravakh cheloveka*. [Online].

Blitz, J. (2012). "UK Seeks Deal to Counter Cyber Attacks". *Financial Times*, 2 October.

Borisov, T. (2010). "Virtual'nyy mir zakryt". *Rossiyskaya Gazeta*, 12 November.

CCDCOE (2012). *Call for Papers Announced for CyCon 2013.* [Online] Available at http://ccdcoe.org/cycon/400.html [Accessed 1 October 2012].

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

Collective Security Treaty Organisation (2012). *CSTO Website.* [Online] Available at http://www.odkb.gov.ru/start/index_aengl.htm.

Conflict Studies Research Centre (2012). *Russia's "Draft Convention on International Information Security" – A Commentary.* Oxford: Conflict Studies Research Centre.

Council of Europe (2001). *Convention on Cybercrime.* [Online] Available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

Deutsche Welle (2011). *Russia Holding Back Online Shutdowns for Now, Expert Says.* [Online] Available at http://www.dw.de/dw/article/0,15599135,00.html.

EastWest Institute (2011a). *EWI's Eighth Annual Worldwide Security Conference.* [Online] Available at http://www.ewi.info/wsc8 [Accessed 1 October 2012].

EastWest Institute (2011b). *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations.* New York: EastWest Institute.

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

Faulconbridge, G. (2011). *Phone Hacking Russian Style: Opposition Under Fire.* [Online] Available at http://in.reuters.com/article/2011/12/20/russia-phone-hacking-idINDEE7BJ0AE20111220

Fedorov, A. V. and Tsigichko, V. N. eds. (2001). *Information Challenges to National and International Security.* Moscow: PIR Center.

FIIA-Finnish Institute of International Affairs (2012). *Russian Society Through the Prism of Current Political Protests.* Seminar, Helsinki: s.n.

Forbes Russia (2011). *Durov: FSB prosit "VKontakte" blokirovat oppozitsionnye gruppy*. [Online] Available at http://www.forbes.ru/news/77291-durov-fsb-prosit-vkontakte-blokirovat-oppozitsionnye-gruppy.

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

Giles, K. (2012). "Still writing the online rulebook". *The World Today*, October-November, p. 21.

Giles, K. (2011a). "Information Troops: A Russian Cyber Command?", in *Third International Conference on Cyber Conflict*. s.l.:CCDCOE.

Giles, K. (2011b). *The State of the NATO-Russia Reset.* Oxford: Conflict Studies Research Centre.

Gjelten, T. (2010). *Seeing The Internet As An "Information Weapon"*. [Online] Available at http://www.npr.org/templates/story/story.php?storyId=130052701

Gorman, S. (2010). "U.S. Backs Talks on Cyber Warfare". *Wall Street Journal*, 4 June.

Hagestad, W. (2012). *Information Security in the People's Republic of China,* s.l.: Forthcoming publication.

Hague, W. (2011). *Chair's Statement.* [Online] Available at http://www.fco.gov.uk/en/news/latest-news/?view=PressS&id=685663282.

Interfax (2011). *Shchegolev: tsenzury Interneta v Rossii ne dopustyat.* [Online] Available at http://www.interfax.ru/print.asp?sec=1448&id=226823.

Interfax (2000). October12.

ITAR-TASS (2009). 29 January.

Joint Chiefs of Staff (2006). *Joint Publication 3-13: Information Operations.* [Online] Available at http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf [Accessed 2012].

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

Krebs, B. (2011). *Twitter Bots Drown Out Anti-Kremlin Tweets*. [Online] Available at http://krebsonsecurity.com/2011/12/twitter-bots-drown-out-anti-kremlin-tweets/.

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

Lisovoy, V. M. (1993). "O zakonakh razvitiya vooruzhennoy bor'by i nekotorykh tendentsiyakh v oblasti oborony". *Voyennaya Mysl',* Issue 5.

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

Makarov, N., Ostapenko, O., Rogozin, D. and Falichev, O. (2012). "We Await Help from Military Science and Defence Industrialists; Without This, Creation of Modern Armed Forces Will Not Be Successful". *Voyenno-promyshlennyy kuryer*, 8 February, Issue 5 (422).

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

Medvedev, D. (2011). *Dmitriy Medvedev provel vo Vladikavkaze zasedaniye Natsional-nogo antiterroristicheskogo komiteta.* [Online] Available at http://www.kremlin.ru/transcripts/10408.

Michael, A. (2010). *Cyber Probing: the Politicisation of Virtual Attack.* Shrivenham: Defence Academy of the United Kingdom.

Miles, D. (2011a). *Doctrine to Establish Rules of Engagement Against Cyber Attacks.* [Online] Available at http://www.defense.gov/news/newsarticle.aspx?id=65739.

Miles, T. (2011b). *Army Activates First-of-Its-Kind Cyber Brigade.* [Online] Available at http://www.army.mil/article/70611/Army_activates_first_of_its_kind_Cyber_Brigade/.

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

Modestov, S. (2003). "Prostranstvo budushchey voyny" (The Space of Future War). *Vestnik Akademii Voyennykh Nauk* (Bulletin of the Academy of Military Science) n.º 2.

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

Monaghan, A. (2011). *NATO and Russia: Resuscitating the Partnership.* [Online] Available at http://www.nato.int/docu/review/2011/NATO_Russia/EN/index.htm.

Monaghan, A. (2010). *The Moscow Metro Bombings and Terrorism in Russia*. [Online] Available at http://www.ndc.nato.int/research/series.php?icode=1.

NDC (2010) *The Indivisibility of Security: Russia and Euro-Atlantic Security.* Rome: NATO Defense College.

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

OECD (2011). *OECD Council Recommendation on Principles for Internet Policy Making*. [Online] Available at http://www.oecd.org/dataoecd/11/58/49258588.pdf

Panarin, I. (2011). *December 2011: Information War Against Russia*. [Online] Available at http://rt.com/politics/information-war-russia-panarin-009/.

Panarin, I. (2009). *Russian pundit interviewed on US information operations conference*. [Interview] 27 April 2009.

Panarin, I. (2004). *Informatsionnaya voyna i diplomatiya (*Information Warfare and Diplomacy*)*. Moscow: Gorodets.

Russia Today (2012). *Social networks – a threat for Russia?*. [Online] Available at http://rt.com/news/social-networks-bullying-russia-695/.

Russia Today (2011). *Stallman: Facebook Is Mass Surveillance*. [Online] Available at http://rt.com/news/richard-stallman-free-software-875/.

Russian Ministry of Defence (2011). [Online] Available at http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

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

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

Sharikov, P. A. (2009). "Evolyutsiya gosudarstvennoy strategii v sfere informatsionnoy bezopasnosti" (Evolution of state strategy in the sphere of information security). *SShA – Kanada. Ekonomika, politika, kul'tura*, December, pp. 95-108.

Shavayev, A. G. and Lekarev, S. V. (2003). "Spetssluzhby i informatsionnoye prostranstvo" (The Special Services and the Information Space). *Razvedka i kontrrazvedka*, pp. 350-354.

Shchegolev, I. (2011). s.l., s.n.

Shcherbakov, V. (2010). "Prostranstvo virtual'noye, bor'ba real'naya" (Virtual Space, Real Combat). *Voyenno-promyshlennyy kur'yer*, 13 October.

Sherstyuk, V. P. (2011). *Presentation.* Brussels: s.n.

Sheynis, V. L. (2010). "Natsional'naya bezopasnost' Rossii. Ispytaniye na prochnost'" (National Security of Russia. Testing for Strength). *POLIS. Politicheskiye issledovaniya*, Issue 1.

Sidorov, V. (2008). "Kibervoyny: ot dozhdya k uraganu" (Cyber War: From Rain to Hurricane). *Krasnaya zvezda*, 26 March.

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

State Duma (1996). *Proceedings.* s.l.:s.n.

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

Thomas, T. (2011). *Recasting the Red Star.* Fort Leavenworth: Foreign Military Studies Office.

Thomas, T. (2010). "Russian Information Warfare Theory: The Consequences of August 2008". In S. Blank and R. Weitz eds., *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald.* Carlisle, PA: US Army War College Strategic Studies Institute.

Thomas, T. (2002). *Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?.* Fort Leavenworth, KA: Foreign Military Studies Office (FMSO).

Thomas, T. (2000). *The Russian View Of Information War.* Fort Leavenworth, KA: Foreign Military Studies Office (FMSO).

Tsymbal, V. (1995). *Concept of Information Warfare.* Moscow: s.n.

UNIDIR (2008). [Online] Available at http://www.unidir.org/audio/2008/Information_Security/en.htm.

US Department of Defense (2011). *Strategy for Operating in Cyberspace.* [Online] Available at http://www.defense.gov/news/d20110714cyber.pdf.

Zeenews (2011). *Russian website publishes vote monitor's e-mails*. [Online] Available at http://zeenews.india.com/news/world/russian-website-publishes-vote-monitor-s-e-mails_746183.html.