2011 3rd International Conference on Cyber Conflict
C. Czosseck, E. Tyugu, T. Wingfield (Eds.)
Tallinn, Estonia, 2011 © CCD COE Publications

"Information Troops" – a Russian Cyber Command?

Keir Giles
Conflict Studies Research Centre
Oxford, UK
keir.giles@conflictstudies.org.uk

***Abstract*- Appraisals of Russian military performance during the armed conflict with Georgia in August 2008 noted, among other deficiencies, poor performance in Information Warfare (IW). This led to calls in informed commentary for the creation of dedicated "Information Troops" within the Russian armed forces, whose duties would include what we would define as cyber operations. This stemmed from a perception in parts of the Russian Armed Forces that the "information war" against Georgia had been lost.**

No such entity has appeared in the Russian order of battle, but the public discussion and military comment is informative. Prospects for the appearance of "Information Troops" have been discounted both officially by the FSB and privately by Russian military officers. Arguments put forward against a unit of this kind include the unsuitability of servicemen for advanced cyber operations, and the ready availability and deniability of talented civilian volunteers. But at the same time Russia's EW troops are seeing their role and profile evolve in a manner which suggests they may be acquiring at least some IW capability.

The Russian approach to IW differs from our own, and there are specific perceived internet vulnerabilities which further affect the Russian approach to cyber operations, and prompt Russian pushes for treaty arrangements governing cyberspace.

This paper draws on unclassified open-source media and interviews with serving Russian military officers to consider the Russian military view of cyber operations as a subset of information war, and the prospects for creation of "information troops" (whether given this name or not) in the context of ongoing Russian military transformation. Informal links with volunteer and co-opted cyber forces are also considered.

Keywords: Russia; military; information warfare; doctrine;

I. “Information War” with Georgia

The brief war with Georgia in August 2008 prompted critical reviews of all aspects of Russia’s performance and capabilities in armed conflict. For the most part, this criticism focussed on clear and unambiguous shortcomings in the conduct of kinetic military operations [1], giving impetus to the fundamental transformations which at the time of writing continue to grip the Russian Armed Forces. But one aspect of the conflict provoked far more nuanced and uncertain assessments; this was how Russia had acquitted herself in “information war” with Georgia.

Debates in the West over the nature of cyber conflict are followed with interest in Russia [2], but are not mirrored in the Russian public narrative. Considerations of whether cyberspace is the “fifth domain” for warfare, or simply is a common factor to the other four, do 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 tends to use the term only to describe US or Chinese activities [3]. 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.

In other words, “Russia views cyber-capabilities as tools of information warfare, which combines intelligence, counterintelligence, maskirovka, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, and destruction of enemy computer capabilities [4].” At a time when the term has been written out of US information operations doctrine [5], “information war” is still alive and thriving in Russian security considerations [6].

Yet Russian analyses of the “information war” with Georgia failed to arrive at a consensus on whether that war was actually won or lost [7]. The rapid development of the portrayal of the conflict in Western media, and the mixed success of penetration of the Russian narrative of forced intervention in response to intolerable “genocide”, were cited as evidence by both sides in the debate [8]. In addition, while cyber “campaigns” before and during combat operations in South Ossetia and Abkhazia were not alluded to as a component of Russian overall strategy, it was noted that their contribution to the Russian strategic aims was limited to the information domain – in other words, while elements of Georgian strategic communications were effectively suppressed, broader attacks (for instance on critical national infrastructure) were not in evidence [9][10]. Regardless of the final conclusion, the common perception among those writing in open sources about the information aspect of the conflict was that the performance of the Russian military in this area badly needed to improve.

II. VULNERABILITY

Specific historical factors relating to the Russian adoption of the internet and information and communications technology (ICT) give rise to a sense of vulnerability in this field, which serves only to exacerbate what British expert James Sherr called Russia's habitual "conspiratorial view about absolutely everything" [11].

For instance, failure to develop indigenous ICT and communications networks technology has led to extensive reliance on foreign-built systems – so a writer on information security can note that:

"The information security of the Customs Service of Russia is under the control of Slovenia and Germany (Iskratel), Russian power engineering enterprises and Gazprom have their security looked after by Germany (Siemens) and Sweden (Ericsson), Slovenia and Germany (Iskratel) and the USA (Avaya) make sure there are no accidents on the Russian railways, and now the USA and France (Alcatel) are to guarantee civic safety for us with the MVD... As for our defensive capabilities, it must be noted that the Russian Ministry of Defence does not have its own fixed communications network as in other countries but leases communications systems from Rostelekom. But the Rostelekom long-distance communications network is... wide open to the world."

In other words, "'Caution, The Enemy is Listening' is not just a warning you find on old telephones, but an objective reality. Their ears are in every home, every workplace, every military unit [12]."

The vast majority of Russian writing on cyber conflict is defensive in tone, and focussed on information security and information assurance. Although official Russia now views the activities of NATO and the USA with less alarm than during peaks of tension in the first decade of the 21st century, 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 [13]" – 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 the Information Security Doctrine of the Russian Federation. This document, not updated since 2000, emphasises:

"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 unauthorised access to them [14]".

This defensive theme to public statements from Russia contrasts with US and British official discussion of cyber issues, where reference to defence against hostile cyber operations is balanced with references to considering *offensive* cyber operations within a range of tools available to respond to attacks – as for example with British Minister of State for the Armed Forces Nick Harvey referring to "exploiting cyberspace to enhance our defence – including the capability to exploit the weaknesses of our opponents. Cyber capabilities may provide the kind of precise and tailored effects which a conventional attack cannot [15]." Mention of offensive cyber activity by the state is strikingly absent from Russian open sources.

Another distinctive aspect of consideration of information warfare in Russia is preoccupations in other spheres of information competition, such as the vulnerability of national culture to outside influences – perhaps understandable in a nation which, as Timothy L. Thomas 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')" [17]. This is another facet of the holistic approach to information security in Russia, and this too is reflected in the Information Security Doctrine, 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 [17]."

Thus in the Russian view, the information threat to be countered is a holistic one consisting of both hostile code and hostile content, and the threat is real and current – Russian doctrine emphasises the constant role of IW in peacetime as well as during hostilities.

The view of Dmitriy Rogozin, Russia's Permanent Representative to NATO, of recent NATO pronouncements on cyber defence is predictably colourful: "in spite of all of the Russian side's initiatives, questions having to do with cyber-security were not added to the list as a review of the Russia-NATO Council's common threats. This means that this topic was closed for Russia - they do not want to discuss it with us." Rogozin uses Stuxnet as an example to suggest that those countries whom he considers Russia's adversaries are "developing systems to suppress the cyber-nets of a potential enemy or to introduce to the software of civilian production (mobile telephones, for example) harmful programmes that can be activated at moment necessary for the West... It comes as no surprise, then, that the US has no strong motivation to sign any global treaties on not using cyber-weapons, especially not with Russia, which potentially could be the object of cyber-attacks [18]."

President of the Academy of Military Sciences Army Gen Makhmut Gareyev refers to "subversive information technologies of the West" being the root cause of disorder in the Middle East and North Africa in early 2011. "Internet networks were implanted in Egypt, Tunisia and Libya over a two-year period. It started with systematic training for communication checks, without direct calls for unlawful actions. At the right moment, a centralized order was issued across all networks for people to take to the streets." Gareyev pointed to a full-spectrum information threat consisting of both code and content. “You know how this was done in Georgia, Ukraine and Kyrgyzstan and is now being done in the Middle East,” he continued, adding that the main instigator is the US National Security Agency, which “controls the radio-electronic situation and internet structures across the world... It has open and secret branches in many countries…Any attempt of relevant national structures to counteract these actions is immediately portrayed as violation of freedom of expression and human rights, causing various sanctions [19]."

Given their role and history, both Rogozin and Gareyev could reasonably be expected to take a conservative view on the immediate IW threat posed by the West to Russia. But the view that political change in North Africa came about as a result of a Western IW/cyber conspiracy, which could now be implemented against Russia, has also been expressed by President Medvedev. Speaking at a meeting of the National Anti-Terrorist Committee in February 2011, Medvedev 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 [20].”

III. “PLAYING CATCH-UP”

In keeping with a common perception that Russian security bodies moved from a very recent standing start in operations via the internet, the official history of the Institute for Cryptography, Communications and Information Technology (IKSI, originally training specialists for the FSB, SVR and other bodies, and now part of the FSB Academy) says that “test use of the Institute’s connection to the global Internet network” did not begin until February 1996 [21]. This was not long before, at parliamentary hearings entitled "Russia and the Internet: The Choice of a Future," FAPSI First Deputy Director General Vladimir Markomenko characterised the internet as a whole as a threat to Russian national security [22].

Certainly Russia’s first real exposure to “information war” involving public internet resources - countering Chechen information sources during the first Chechen war - was a sobering experience, and in the words of Paul Goble, “forced... Vladimir Putin to focus ever more closely on the role of the Internet in deciding the outcome of conflicts... Putin openly acknowledged that Moscow was playing catch-up on this battlefield: ‘We surrendered this terrain some time ago,’ he said, ‘but now we are entering the game again [23].’

After computer crime was defined for the first time in Russia’s 1997 Criminal Code, “combating crimes of this type became something entirely new for the law enforcement bodies. There were a lot of problems... the absence of practical experience or methods for investigating these crimes, or of a forensic system [24].”

Concerns about IW and cyber vulnerability continued to be expressed even before the armed conflict in Georgia. The then Deputy Chief of the General Staff, Lt-Gen Aleksandr Burutin, noted in January 2008 that "Russia should be ready for a global information war". "Leading states are now actively developing forms and methods of struggle in the information sector", since "the development of information technology transforms the idea of a state's military might and political potential, changes the traditional forms of power struggle... In the foreseeable future, the final aims of wars and armed conflicts will be achieved not so much by destroying the troops and forces of an adversary, as by suppressing its state and military command, navigation and communication systems, influencing other information facilities on which the stable government of a state depends [25]."

On the same day, Burutin said that information weapons which could be "used in an efficient manner in peacetime as well as during war pose great danger" for Russia. He voiced the Russian preoccupation with "the destruction of spiritual values, by targeting individual, group and mass conscience", noting that this was the area of activity of "a number of non-government organizations supported from abroad, to form a negative image of Russia [26]".

Despite the head of US Cyber Command, Gen Keith Alexander, describing Russia as a "near peer" to the USA in capability [27], this perception of vulnerability and sense that Russia may be lagging behind in development of official capacity for computer network operations (CNO) is reinforced by the dogged Russian emphasis on treaties or agreements to restrain the activities of states in cyberspace, and so-called arms control treaties for information weapons [28].

These efforts also involve the Ministry of Foreign Affairs of the Russian Federation (MFA) and Directorate K of the Ministry of Internal Affairs (MVD) [29]. Professor Igor Panarin of the MFA's Diplomatic Academy, the author of one of the standard works on Russian theory of information war [30], advocates "using 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 [31]". It is argued that the 2009 agreement between Shanghai Cooperation Organisation (SCO) states on "cooperation in ensuring international information security", including provision for military cooperation, should be used as a template and extended [32]. Meanwhile, CSTO Secretary-General Nikolai Bordyuzha has said that his organisation too must "create a joint system to counter information threats", since: "a number of Western countries and international institutions, the first to step over the threshold of the information era, have stepped up the structural reconstruction of national and security systems on the basis of joining their information potentials into one to achieve political, economic, military and ideological dominance at the regional and global levels... Developing a common information space become particularly important. There is a need to create a joint potential for countering information threats, to secure information resources and communications of the CSTO bodies and the member states' national authorities [33]."

Taken together, this offensive on a broad front suggests strongly that Russia feels the need to complete its “catch-up” with foreign states, while further development by those states should ideally be limited by international binding agreements.

Some of the proposed treaty limitations make interesting reading when compared with anti-social behaviour in cyberspace which has emanated from the Russian Federation: Aleksandr Burutin backs “a mutually acceptable multilateral mechanism” which would bind states to “taking responsibility for what is happening in their information space” – a responsibility conspicuously absent in the case of Russia [34].

In treaty proposals as well as in doctrine, Russia conflates the threat from hostile bits with the threat from hostile content, which according to the Information Security Doctrine can "distort the perception of the political system, social order, domestic and foreign policy, important political and social processes in the state, spiritual, moral, and cultural values of citizens." It is for this reason, among others, that Russia is dissatisfied with initiatives proposed overseas - as uncompromisingly put by Khatuna Mshvidobadze of the Georgian Foundation for Strategic and International Studies (GFSIS), “Moscow refuses to sign the only promising agreement, the European Convention on Cybercrime, which has been open for signatures since 2001. The Kremlin does not want to cooperate with foreign law enforcement officials looking into something like the 2007 cyberattacks on Estonia, and it is surely does not want to risk exposure of its links” to cyber crime syndicates [35].

IV. “INFORMATION TROOPS”

When reviewing the military’s performance in Georgia, deficiencies were noted in both the information-technical and information-psychological domains, the two main strands of information warfare in Russian thinking [36]. The answer, in the view of several informed critics, was the creation of “Information Troops” within the Russian Armed Forces, who would meet the military’s need for full-spectrum information operations.

One of the most clearly developed arguments for an entity of this kind was put forward by Igor Panarin, referred to above. Panarin called for “Information Special Forces” who would “prepare for effective operations under potential crisis conditions [37]”. These operations would cover all aspects of information operations, including CNO: as he noted elsewhere, “the objective is... certainly, to create centres which would envisage so-called hacker attacks on enemy territory [38].”

The holistic nature of the tasking for these new units, and the way in which the Venn diagram of the Russian information war concept includes much that we might categorise under entirely different headings, was illustrated by further extensive and detailed descriptions of the desired new capability, which inter alia stated:

"The personnel of the Information Troops should be composed of diplomats, experts, journalists, writers, publicists, translators, operators, communications personnel, web designers, hackers, and others... To construct information countermeasures, it is necessary to develop a centre for the determination of critically important information entities of the enemy, including **how to eliminate them physically**, and how to conduct electronic warfare, psychological warfare, systemic counterpropaganda, and net operations to include hacker training [39]."

Persuasive press commentaries were followed in due course by Aleksandr Burutin noting at the National Information Security Forum that it was "essential to move from analysing the challenges and threats... to reacting to them and pre-empting them [40]". At the same time the Ministry of Defence acquired a new deputy minister specifically for information and telecommunications technologies, Dmitriy Chushkin [41].

V. COMPETITION

But when Col-Gen Anatoliy Nogovitsyn followed up by suggesting that the General Staff should be working on defence against information-technical attack, this military ambition was immediately criticised by the Federal Security Service (FSB): "It is a strange statement... Such issues are not under the purview of any one department and should be resolved within the framework of the country's Security Council" (a body saturated with serving and "former" FSB officers). "At the same time, the military cannot but know that we have already created information-protection mechanisms, and they are constantly being improved [42]."

This is indicative of the fact that this capability, which the military seems to feel it lacks, is already well-established in other of Russia's "power ministries" with permanent seats on the Security Council. The regulations on use of SORM, Russia's official monitoring system installed (and paid for) by ISPs, state that it is the FSB that accesses information on internet use on behalf of all other interested parties, or if they do not have sufficient technical means to do so, the MVD takes over [43]. The MVD has its "Directorate K" dealing with information crime in the broadest sense, and with a perceived ambiguous role in which kind of cyber crime it will prosecute and which it will leave in peace. Russia did at one point have a dedicated information security agency, the Federal Agency for Government Communications and Information (FAPSI) – described by one leading expert as "the unofficial Ministry of Information Warfare of the Russian Federation [44]". Although the life-span of FAPSI as an independent entity was relatively short, its components were not disbanded but absorbed into two other agencies – the Federal Protection Service (FSO) and the FSB [45].

While the FAPSI directorate dealing with government communications was transferred to the FSO [46], the FSB received the Main Directorate for Radio-Electronic Reconnaissance on Communications Networks (*Glavnoye upravlenye radioelektronnoy razvedki sredstv svyazi*, GURRSS). The influence of this body in directing policy today could be inferred from the fact that the former chief of FAPSI and of the GURRSS, Vladislav Sherstyuk, holds the information security portfolio on the Security Council and is also the head of the Department of Information Security at Moscow State University [47]. This department is particularly active in Russia's drives for international agreements on information and cyber conflict [48], referred to above. So a proposal for a new component of the Russian Armed Forces dealing with information warfare would have to contend with the fact that it would be launched onto a stage already crowded with other actors, who might be less than entirely willing to share space with a newcomer [48].

VI. THE REB TROOPS

Opinions on the prospects for "Information Troops" among senior Russian serving military officers interviewed for this paper vary widely. One dismissed the idea out of hand [50]; another expressed the view that although media chatter about "Information Troops" might be misguided, if a place were to be found for carrying out functions of the kind described within the Russian Armed Forces, it would be in the *Voyska radioelektronnoy bor'by, Voyska REB* – the Russian military's electronic warfare branch, to be translated here as REB Troops [51]. This was one of the few elements of the Russian forces whose performance did not suffer intense criticism after the armed conflict in Georgia (although as always, it is hard to distinguish Georgia's claims of effective enemy counter-measures from complaints that friendly communications systems simply didn't work in the first place) [52].

The emblem of the REB Troops, a spider astride a globe in the form of a latitude and longitude grid, is rich with temptation for those who would wish to interpret the symbol as meaning that operations using the internet are a key part of their role – even if there has been no explicit mention of formal expansion into cyber activities. (So much so, in fact, that the emblem has been appropriated by the self-styled "Cybernetic Police" for their website on information security and computer crime in Russia [53].)

Much of the upbeat material in open sources written about future plans for the REB Troops blends easily into the background noise of puff pieces about Russian military capability: they are not immune from the standard regular promises of new and improved equipment "which has no world equivalent". But at the same time, change does appear to be taking place there. Declaring a "REB Troops Day" alongside similar days for border guards, paratroopers etc. suggested a boost in status for the branch, even before a promise of reorganisation into an independent service arm in its own right [54], which if true would be a remarkable development. The REB Troops are currently part of the "Special Troops" (not to be confused with “special-purpose troops” or Spetsnaz), i.e. troops with specialised functions which are not part of a force or service arm (*vid* or *rod voysk*).

At the same time the main role of the REB Troops has been re-defined as “winning and retaining superiority in command and control of combat actions” (a common phraseology in Russian definitions of information warfare), while “the effect of the actions of EW means are comparable with the use of modern high-precision weaponry”. Furthermore, “in the near future fundamental changes in the development of EW means and materiel should allow it to develop into a specific main form of combat action, which in many ways will determine the course and outcome of armed conflict [55].” In short, although there is no direct evidence to support the suggestion that the REB Troops will be the locus of CNO for the Russian Armed Forces, the coloratura of official statements suggests that their role and prominence is developing in a new direction.

VII. DIY Cyber War

Another serving Russian interviewee was sceptical about the prospects for creation of effective “Information Troops”, whatever their formal title might be, because of the difficulty of finding and retaining appropriate personnel within the military – in fact, he noted, the military was the wrong place for capabilities of this kind, since servicemen under orders could never compete in flexibility and creativity with civilian enthusiasts [56]. The tension between qualities desirable in servicemen and qualities desirable in “information warriors” may well be a universal problem - in the phrase of Brig-Gen Charles Shugg, Deputy Commander US 24th Air Force, it is hard to find people who are “military minded but still competent to be cyber professionals [57]”. Just as with their counterparts overseas, the Russian REB Troops too report retention difficulties due to competition from civilian employers [58]. And in Russia, an additional constraint is imposed by reliance on conscription for a significant part of military manpower: it remains the case that those young males with an interest in, aptitude for, and access to ICT are the ones who are least likely to be conscripted, and therefore available for manning “Information Troops”, because they are precisely the ones who have access to the vast wealth of online information explaining the best possible ways of avoiding the draft [59].

Yet according to one counter-argument, much of what the “Information Troops” would seek to achieve in terms of CNO need not be sited within the military at all. The cyber component of confrontation with Estonia in 2007 and Georgia in 2008, and the online assault against Kyrgyzstan in January 2009 [60], showed how little encouragement large sections of the Russian online community need to join in with furthering Russian state goals. A Russian survey of “actors in cyberspace” defines “Net NGOs” as “internet combatants who as a rule declare the absence of any link with State bodies but which as a rule are financed by them, or by other entities [61]”. But with a light management touch ensuring that plausible (or even implausible) deniability is maintained, a nudge in the right direction is enough for campaigns rapidly to take on a viral nature. As suggested in one Russian report on the cyber attacks on Georgia, "there is no need for the state machine in modern cyber warfare [62]". When considering a loose network of highly technically capable individuals working towards a common goal, there is an obvious parallel with the Russian Business Network (RBN) cybercrime organisation [63].

With an overlap of tactics, techniques and procedures (TTPs) between cyber crime, cyber activism, and cyber aggression, from a Russian perspective the synergies are clear. As Alex Klimburg puts it, "the differences between these categories of cyber activity are often razor thin, or only in the eye of the beholder. From the perspective of a cyber warrior, cyber crime can offer the technical basis (software tools and logistic support) and cyber terrorism the social basis (personal networks and motivation) with which to execute attacks on the computer networks of enemy groups or nations." Furthermore, "states have an interest in maintaining or tolerating proxy organisations that could be implicated in this type of activity and other forms of attack, such as distributed denial of service, which can be conducted by an average computer user with the right tools [64]". Khatuna Mshvidobadze goes further and states that "the FSB's 16th Directorate is believed to control Russia's reserve force of hackers [65]." And in the words of the head of the Federation Council's Defence and Security Committee, Viktor Ozerov, briefing foreign military attaches on 18 March 2011, "there is still no special structure for countering cyber in the Armed Forces, but this does not mean that we are not dealing with these problems [66]."

The ready availability of cyber volunteers, or those who can be co-opted, is facilitated by the relatively low barriers to entry to would-be cyber miscreants in Russia. Some of the scripts and instructions distributed to aid those who wanted to attack Estonia in 2007 but didn't know where to start may have been of an extraordinarily basic nature; but there is an impressively broad choice of Russian-language online resources available for the guidance and equipping of those who would like to develop their computer network attack (CNA) and penetration skills further. On the basis of the author's entirely unscientific comparison, it appears a great deal easier (and cheaper) for a Russian speaker to find meaningful instructions, guidance and tools than for somebody seeking to make the same debut in English [67].

The concentrated power of deniable CNA operations from Russia is striking even when it is not directed abroad with hostile intent, as witness the fallout from the concentrated efforts to suppress the blogger Cyxymu in August 2009, when collateral damage meant large parts of Twitter, Facebook and LiveJournal were temporarily taken offline [68]. As David Hollis implies in the study cited earlier in this paper, when drawing lessons for future confrontations, in circumstances of this kind where the objectives of the perpetrators coincide precisely with the interests of the Russian state, is it important whether the aggressor party denies liability or not [69]? Much has changed since Moonlight Maze, when activities directed against US government computer systems reportedly ceased outside Russian office hours [70].

VIII. CONCLUSION

The narrative of “information war” is developing within Russia, but mostly under the influence of initiatives taken overseas. The approach to CNO by the USA and to a lesser extent by its allies is followed closely. The most recent senior comment on the subject at the time of writing came from influential long-term Duma deputy, and former Secretary of the Security Council and Deputy Minister of Defence, Andrey Kokoshin - a long-term proponent of the vital importance of information superiority for Russian security [71], with, intriguingly, a first qualification in radioelectronics from the then Bauman Higher Technical College [72].

Speaking at the launch of a report entitled “’Cyber Wars’ and International Security” published in late January 2011 jointly by the Institute of International Security Issues of the Russian Academy of Sciences and the Faculty of World Politics of Moscow State University, Kokoshin said that “the development of issues of information warfare and ‘cyber wars’ must take place on an interdisciplinary level... the experience of many states shows that information warfare is not just a function of the Armed Forces: other state institutions including the secret services take part in it [73]”. This makes an interesting counterpoint to the FSB statement cited earlier in this paper which appeared to be suggesting that it was not the business of the Armed Forces at all. The “’Cyber Wars’ and International Security” report, according to the Russian Ministry of Defence newspaper *Krasnaya Zvezda*, “examines primarily US and Chinese policy in this area... The study examines issues such as operations in cyberspace as an integral part of information operations [74].” At the time of writing, the report itself appeared to be unavailable in open sources.

Meanwhile, Russian security concerns will continue to be prompted by the fact that “influencing the transfer and storage of data means that the physical destruction of your opponent’s facilities is no longer required [75]” – potentially negating all the benefits of Russia’s hard-won military reforms. Efforts will continue to be “directed at introducing international legal mechanisms that would make it possible to contain potential aggressors from uncontrolled and surreptitious use of cyberweapons against the Russian Federation and its geopolitical allies [76].”

So, Russian statements and initiatives on cyber operations have to be placed in this context of observing rapidly-developing capabilities overseas, and listening to public announcements in the USA and elsewhere of ever-greater potential and willingness to inflict damage on adversaries by means of cyber attack. At present, the urgent arguments for the creation of “Information Troops” within the Armed Forces have not yet given rise to any visible change in tasking or designation of military structures, and visions of Russia’s potential organised cyber warriors range from the heroic and omnipotent [77] to the realms of surreal parody [78]; but there is no doubt that the preoccupation with a perceived lack of capacity to prosecute or defend against CNO within the military will continue to provoke calls for action.

ACKNOWLEDGEMENTS

Thanks are due to Timothy L Thomas of FMSO for exhaustive long-term research on Russian views on IW, extensively cited in this paper; and to Gordon Bennett for historical information on Russian security structures.

REFERENCES:

[1] "Understanding the Georgia Conflict, Two Years On", NATO Defense College, Rome, September 2010. Available at http://www.ndc.nato.int/research/series.php?icode=9

[2] BBC Monitoring: "Russia needs more cyber war specialists - prominent expert and Duma MP", Interfax-AVN, 1430 GMT 26 January 2011. Also Shavayev, A. G. & Lekarev S. V. "*Spetssluzhby i informatsionnoye prostranstvo*", *Razvedka i kontrrazvedka*, Moscow 2003, pp. 350-354, and Sharikov, P. A. "*Evolyutsiya gosudarstvennoy strategii v sfere informatsionnoy bezopasnosti*", *SShA – Kanada. Ekonomika, politika, kul'tura*, No. 12, December 2009, pp. 95-108.

[3] V. Shcherbakov. "*Prostranstvo virtual'noye, bor'ba real'naya*", *Voyenno-promyshlennyy kur'yer,* 13 October 2010; V. Sidorov. "*Kibervoyny: ot dozhdya k uraganu*", *Krasnaya zvezda*, 26 March 2008.

[4] K. Mshvidobadze, "The Battlefield On Your Laptop", Radio Free Europe/Radio Liberty 21 March 2011, available at http://www.rferl.org/articleprintview/2345202.html

[5] The 2006 revision of US Joint Publication 3-13, "Information Operations", "removes information warfare as a term from joint IO doctrine".

[6] T.L. Thomas. "Russian Views on Information-based Warfare", Foreign Military Studies Office (FMSO), July 1996; T. L. Thomas. "The Russian View Of Information War", FMSO, February 2000; T. L. Thomas. "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?", FMSO, 2002.

[7] P. Goble. "Defining Victory and Defeat: The Information War Between Russia and Georgia", in S. Cornell & F. Starr (eds) *The Guns of August 2008: Russia's War in Georgia*, New York 2009.

[8] M. Akhvlediani. "The fatal flaw: the media and the Russian invasion of Georgia", in P. B. Rich (ed.) *Crisis in the Caucasus: Russia, Georgia and the West*, London: Routledge 2010.

[9] A. Tsyganok. "*Informatsionnaya voyna protiv Rossii: kak eto bylo"*. Segodnya, 17 April 2009. Available at http://www.segodnia.ru/index.php?pgid=2&partid=13&newsid=8407.

[10] D. Hollis. "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, 6 January 2011. Available at http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

[11] "Russia: A New Confrontation?" House of Commons Defence Committee Tenth Report of Session 2008-09, 30 June 2009, available at http://www.publications.parliament.uk/pa/cm200809/cmselect/cmdfence/276/27602.htm

[12] A. I. Nogovitsyn. "*Za gran'yu informatsionnoy bezopasnosti*", *Zashchita i bezopasnost'*, No. 1, 2010. For an expression of similar concerns in a UK context, see A. Michael. *Cyber Probing: The Politicisation of Virtual Attack*. Shrivenham: Defence Academy of the United Kingdom, 2010.

[13] US Joint Publication 3-13.1, "Electronic Warfare".

[14] Available on the Security Council of the Russian Federation website at http://www.scrf.gov.ru/documents/6/5.html

[15] Public statement at Chatham House, 9 November 2010.

[16] T. L. Thomas. “Russian Information Warfare Theory”, op. cit.

[17] Information Security Doctrine. See also V. L. Sheynis. “*Natsional’naya bezopasnost’ Rossii. Ispytaniye na prochnost’*”, *POLIS. Politicheskiye issledovaniya*, No. 1, 2010.

[18] D. Rogozin. "The Price of the Issue", *Kommersant*, 16 February 2011

[19] Interfax news agency, 26 March 2011

[20] “*Dmitriy Medvedev provel vo Vladikavkaze zasedaniye Natsionalnogo antiterroristicheskogo komiteta*”, Russian presidential website, 22 February 2011, available at http://www.kremlin.ru/transcripts/10408

[21] *Kompant-dien, posvyashchennyy pyatidesyatiletyu IKSI*, Moscow: Institut Kriptografii, Svyazi i Informatiki, 1999; pp. 195-201.

[22] State Duma proceedings, 17 December 1996.

[23] P. Goble. “Russia: Analysis From Washington -- A Real Battle On The Virtual Front”, RFE/RL 11 October 1999. Available at http://www.rferl.org/content/article/1092360.html

[24] MVD website at http://www.mvd.ru/struct/10000220/10000288/

[25] ITAR-TASS news agency, 31 January 2008

[26] Interfax-AVN news agency, 31 January 2008

[27] “Cyber Threat to Pentagon is Global: China, Russia Near Peers of US”, 1 October 2010, http://www.geostrategy-direct.com/geostrategy-direct/secure/2010/10_06/ba.asp

[28] S. Gorman. “U.S. Backs Talks on Cyber Warfare”, *Wall Street Journal*, 4 June 2010. Available online: http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html

[29] MVD website: http://www.mvd.ru/struct/10000220/10000221/10000740/

[30] I. Panarin. *Informatsionnaya voyna i diplomatiya,* Moscow: Gorodets 2004.

[31] BBC Monitoring: “Russian pundit interviewed on US information operations conference”, *Rossiya TV* 1950 GMT 27 April 2009

[32] S. M. Boyko, I. N. Dylevskiy, S. A. Komov, S. V. Korotkov. “*Voyenno-politicheskiye aspekty obespecheniya informatsionnoy bezopasnosti na prostranstve Shankhayskoy organizatsii sotrudnichestva*”, *Voyennaya mysl’*, No. 7, July 2010.

[33] “CSTO Needs Coordinated Information Policy – Bordyuzha”, Interfax 21 December 2010

[34] *Tsentr parlamentskikh kommunikatsiy*, 30 January 2009, available at http://www.parlcom.ru/index.php?p=MC83&id=27297

[35] K. Mshvidobadze, “The Battlefield On Your Laptop”, Radio Free Europe/Radio Liberty 21 March 2011, available at http://www.rferl.org/articleprintview/2345202.html

[36] T. L. Thomas. “Russian Information Warfare Theory: The Consequences of August 2008”, in S. Blank and R. Weitz. *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, Carlisle: US Army War College Strategic Studies Institute 2010.

[37] OSC: I. Panarin. "The Information Warfare System: the Mechanism for Foreign Propaganda Requires Renewal", *Voyenno-Promyshlennyy Kuryer* 15 October 2008.

[38] BBC Monitoring: “Russian TV highlights hacker attacks on Georgian sites”, *RenTV* 0930 GMT 11 November 2008.

[39] BBC Monitoring: “Russia is underestimating information resources and losing out to the West”, *Novyy Region*, 29 October 2008 (emphasis added). See also Tsyganok, op. cit.

[40] *Tsentr parlamentskikh kommunikatsiy*, 30 January 2009, available at http://www.parlcom.ru/index.php?p=MC83&id=27297

[41] Izvestiya, 27 February 2009

[42] D. Litovkin. “General Staff Prepares for Cyber War”, *Izvestiya*, 27 February 2009.

[43] For a detailed discussion of SORM, with legislative citations, see http://www.cyberpol.ru/sorm.shtml

[44] G. Bennett. *The Federal Agency of Government Communications & Information*, Conflict Studies Research Centre. Sandhurst: August 2000.

[45] G. Bennett. *FPS & FAPSI – RIP,* Conflict Studies Research Centre. Sandhurst: March 2003.

[46] Official history of the FSO, available at http://www.fso.gov.ru/histori/histori7.html

[47] Security Council of the Russian Federation website, http://www.scrf.gov.ru/persons/11.html

[48] See D. Talbot. “Russia's Cyber Security Plans”, 16 April 2010, available at http://www.technologyreview.com/blog/editors/25050/ for an interview with Sherstyuk discussing “cyber arms control” and the nature of cyber weapons.

[49] See also R. Heickerö, “Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations”, Swedish Defence Research Agency (FOI), FOI-R-2970-SE, March 2010.

[50] Private interview, November 2010.

[51] Private interview, December 2010.

[52] R. Hamilton, “The bear came through the tunnel: an analysis of Georgian planning and operations in the Russo-Georgian War and implications for US policy”, in “Crisis”, op. cit.

[53] http://www.cyberpol.ru/

[54] “*Voyska radioelektronnoy bor’by stanut v armii RF samostoyatel’nymi*”, *Vesti.ru*, 15 April 2009, available at http://www.vesti.ru/doc.html?id=275300

[55] “*Sostoyaniye sil REB: interv’yu s nachal’nikom voysk REB VS RF O. Ivanovym*”, *Krasnaya Zvezda*, 15 April 2010.

[56] Private interview, January 2011.

[57] Speaking at “Cyber Warfare” conference, London 28 January 2011.

[58] “*Sostoyaniye sil REB: interv’yu s nachal’nikom voysk REB VS RF O. Ivanovym*”, *Krasnaya Zvezda*, 15 April 2010.

[59] For example the always-busy forum at http://www.antipriziv.ru/forum/ and many more.

[60] http://hostexploit.blogspot.com/2009/01/cyberwar-cyber-iron-curtain-now_28.html

[61] O. V. Kazarin, A. A. Salnikov, R. A. Sharyapov, V. V. Yashchenko. “*Novyye aktory i bezopasnost’ v kiberprostranstve*”, *Vestnik Moskovskogo universiteta*: *Seriya 12, Politicheskiye nauki*, NN 2-3, 2010.

[62] BBC Monitoring: “Russian TV highlights hacker attacks on Georgian sites”, RenTV 0930 GMT 11 November 2008.

[63] For a well-constructed overview of RBN activities, see http://www.bizeul.org/files/RBN_study.pdf

[64] A. Klimburg. “Mobilising Cyber Power”, Survival: Global Politics and Strategy, vol. 53, no. 1, February-March 2011, pp. 41-60

[65] K. Mshvidobadze, “The Battlefield On Your Laptop”, Radio Free Europe/Radio Liberty 21 March 2011, available at http://www.rferl.org/articleprintview/2345202.html

[66] Interfax-AVN news agency, 18 March 2011

[67] For illustration, visit (with appropriate precautions) the fora at http://forum.inattack.ru/Barakholka-f11.html (for initial and advanced training) or http://forum.xakep.ru/forumid_307/tt.htm (for a bustling trade in tools).

[68] A. Michael. (2010) *Cyber Probing: The Politicisation of Virtual Attack*. Shrivenham: Defence Academy of the United Kingdom, p. 15.

[69] D. Hollis. "Cyberwar Case Study: Georgia 2008" in Small Wars Journal, 6 January 2011. Available at http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

[70] B. Drogin. “Russians Seem To Be Hacking Into Pentagon”, San Francisco Chronicle, 7 October 1999. Available at http://sfgate.com/cgi-bin/article.cgi?f=/c/a/1999/10/07/MN58558.DTL

[71] As cited in M. C. Fitzgerald. “Russian Views on Electronic and Information Warfare”, Hudson Institute, December 1996.

[72] Biography available at http://dic.academic.ru/dic.nsf/ruwiki/101812

[73] “Kokoshin: Kibervoyny ugrozhayut natsional’noy bezopasnosti Rossii”, One Russia party website, 26 January 2011. Available at http://er.ru/er/text.shtml?18/2254

[74] Ye. Podzorov. “*Ostorozhno, kibervoyny*”, *Krasnaya zvezda*, 29 January 2011. Available at http://www.redstar.ru/2011/01/29_01/1_02.html

[75] Prof. V. Lisovoy, speaking at Swedish Defence Research Agency, Stockholm 5 October 2010

[76] “Russian Federation Military Policy in the Area of International Information Security”, Moscow *Military Thought* 31 March 2007

[77] O. V. Kazarin, A. A. Salnikov, R. A. Sharyapov, V. V. Yashchenko. “*Novyye aktory i bezopasnost’ v kiberprostranstve*”, *Vestnik Moskovskogo universiteta*: *Seriya 12, Politicheskiye nauki*, NN 2-3, 2010.

[78] I. Koshkin. “*Zapiski o budushchey voyne – informatsionnyye voyska Rossii”. Voyenno-istoricheskiy forum,* 28 September 2009, available at http://vif2ne.ru/nvk/forum/archive/1758/1758322.htm