Security Index: A Russian Journal on International Security

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/rsec20

INTERNATIONAL REGULATION OF INFORMATION SECURITY AND RUSSIA'S NATIONAL INTERESTS

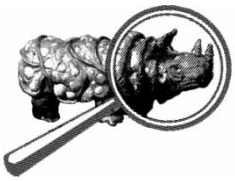
Oleg Demidov

Published online: 23 Nov 2012.

To cite this article: Oleg Demidov (2012) INTERNATIONAL REGULATION OF INFORMATION SECURITY AND RUSSIA'S NATIONAL INTERESTS, Security Index: A Russian Journal on International Security, 18:4, 15-32, DOI: 10.1080/19934270.2012.714597

To link to this article: http://dx.doi.org/10.1080/19934270.2012.714597

Routledge
Taylor & Francis Group



Oleg Demidov

INTERNATIONAL REGULATION OF INFORMATION SECURITY AND RUSSIA'S NATIONAL INTERESTS

In 2011 cyberspace obtained recognition at the highest level—first and foremost, in terms of its importance for international security. This is evidenced by several events and processes which may look unrelated, but which are actually rooted in the same problem.

First, in the global discourse between experts, politicians, and the media, the revolutionary events of the so-called Arab Spring have been inextricably linked with information technology. There has been a lot of wild speculation and a tendency to exaggerate the role of social networks and other Web 2.0 instruments in the revolutionary events in the Middle East and beyond. Nevertheless, that discourse has a solid factual basis. The unprecedented speed and scale of the spread of information in cyberspace—primarily through social networks—have worked against the regimes that were trying to conceal their campaigns of persecution from the international community, but did not have the skills to conduct global information campaigns of their own in cyberspace.

Second, the United States has adopted, in quick succession, two cyberspace security strategies. The first, the International Strategy for Cyberspace, was released on May 16, 2011. It was soon followed by the Pentagon's Strategy for Operating in Cyberspace, parts of which were published in June 2011. The latter document declares cyberspace to be an *operation domain*, i.e. a domain in which the U.S. Armed Forces may have to conduct military operations, just like they already do in the land, maritime, air, and space domains.[1] In essence, cybersecurity has for the first time been equated by the world's only military superpower to military security in terms of its importance.

Last but not least, Russia and the Shanghai Cooperation Organization (SCO) have unveiled their own important initiatives aimed at building a global regime of regulating security in cyberspace (defined more broadly by the Russian authors of the initiatives as ''infospace''). The most prominent of these initiatives is the Russian concept of a UN Convention on International Information Security. A somewhat less high-profile but equally ambitious proposal is for a Code of Conduct on International Information Security. For the first time the international community has been invited to discuss draft pieces of legislation, one or both of which answer the following descriptions:

- Proposes a comprehensive and universal approach to international information security (IIS);
- aims for universal adoption by the international community via UN mechanisms;
- is legally binding;
- is positioned as a more or less finished and workable draft which its authors believe can be approved via UN mechanisms in a matter of two or three years.

These draft pieces of international legislation raise the debate about global regulation of cybersecurity to a whole new level. On a practical level, their adoption would have radical legal, political, social, economic, and even military repercussions for the international community.

ISSN 1993-4270 (print)/ISSN 2151-7495 (online) http://dx.doi.org/10.1080/19934270.2012.714597

Table 1. **Key Pieces of Legislation and Regulation (by Areas and Levels of Cybersecurity Regulation)**

Type of cyber threat/level of regulation	Cybercrime (Citizens Vs. Citizens)	Cyber espionage	Aggressive actions by states in cyberspace		Cyber terrorism (Citizens vs. States)
			States vs. Citizens	States vs. States	
Global	UN CONVENTION (RUS, SCHJOLBERG) CE CONVENTION SCO UN CODE	UN CONVENTION (RUS, SCHJOLBERG)	UN CONVENTION (RUS, SCHJOLBERG) SCO UN CODE	?	UN CONVENTION (RUS, SCHJOLBERG) SCO UN CODE
Regional	SCO 2009 AGR CE CONVENTION	SCO 2009 AGR	SCO 2009 AGR		SCO 2009 AGR

Notes:
UN CONVENTION RUS— Russian concept of the UN Convention on International Information Security.
UN CONVENTION SCHJOLBERG— draft Global Treaty on Cybersecurity and Cybercrime by Stein Schjolberg and Solange Ghernaouti-Helie.
SCO UN CODE— draft Code of Conduct in Cyberspace proposed by the SCO member-states.
SCO 2009 AGR— Agreement between the Member States of the SCO on Cooperation in International Information Security of June 16, 2009 (Yekaterinburg Agreement).
CE CONVENTION— Council of Europe Convention on Cybercrime of November 23, 2001.

This is why the Russian and SCO proposals require detailed analysis, which this article will undertake to provide. The two initiatives are the main subject of this research, which aims to assess their potential impact as far as Russian national interests are concerned.

Table 1 offers a general classification of the two initiatives and of the existing pieces of international legislation by the following criteria: level of regulation (from national to global) and specific areas of cybersecurity being regulated.

This research will focus on two key questions:

1. What is the outlook for the Russian and SCO initiatives in the international arena? How do they sit with the national interests of Russia itself and its key international partners?
2. What effects will these initiatives have on Russian policy with regard to the Council of Europe Convention on Cybercrime? Should Russia continue to avoid joining the Convention?

It must be emphasized that this paper analyzes the aforementioned documents and initiatives mostly from the international-political rather than legal point of view. It focuses primarily on assessing them from the point of view of Russian national interests in the area of international information security as opposed to analyzing their merits as pieces of legislation.

Finally, a few words on terminology. This analysis uses the terms ''information'' (as in information security) and ''cyber'' (as in cybersecurity)—depending on the context. ''Information'' is used when speaking about the official titles of the Russian and SCO initiatives on IIS regulation, or about the corresponding concepts which are different from the concepts dealing with cybersecurity. In all other cases this paper uses the ''cyber'' root.

THE RUSSIAN CONCEPT OF THE UN CONVENTION AND THE SCO CODE OF CONDUCT

For a long time Russia has been making energetic efforts at the UN to promote international cooperation in the area of cybersecurity. The most detailed review of Russia's participation in establishing mechanisms of cyberspace regulation at the UN platform can be found in an article by Andrey Krutskikh.[2] Dr Krutskikh is one of the leading Russian diplomats specializing in IIS;

in March 2012 he was appointed as the Russian Foreign Ministry's special coordinator on issues of political uses of information and computer technologies. On several occasions he led the Russian delegations and UN international expert groups set up as part of the initiatives on promoting international cooperation in countering various cyber threats.

''Russia has been promoting the idea of international cooperation to strengthen IIS since 1998,'' Dr Krutskikh writes in his article. Since mid-1998 ''coordination of specific steps to strengthen IIS has been conducted mainly through UN mechanisms.''[3] Also since 1998 Russia has submitted to the UN General Assembly several resolutions calling for an intergovernmental agreement on countering ''information terrorism.'' On December 8, 2003, in accordance with UN General Assembly Resolution N56/16 of November 29, 2001, the UN set up a group of government experts tasked with studying and assessing the most serious threats to international information security, measures to counter those threats, and concepts of ensuring security of the global information and telecommunications sector. The group prepared its first report in 2005, but the document was not approved owing to the opposition of the American delegation. In May 2010, in response to a Russian initiative, the UN Commission on Crime Prevention and Criminal Justice resolved to set up an open intergovernmental group of experts to conduct a comprehensive study of the problem of cybercrime. One of the new group's priorities is to develop and formulate proposals for improving international legislation and regulation in the area of countering cybercrime and cyberterrorism.[4]

At the 65th Session of the General Assembly in July 2010 a group of government experts from 15 countries (including India), led by Andrey Krutskikh, submitted a report on information security to the UN Secretary-General. The report, which was unanimously accepted by the General Assembly, stresses the need to develop common approaches to countering cyber threats and fighting cybercrime and cyberterrorism. It represented a real breakthrough for the group, which had hitherto worked to little effect since it was established in 2005.

Russian diplomacy has been making increasingly energetic efforts in this area over the past three or four years. But these efforts reached a whole new level in 2011, when Russia proposed a concept of the *Convention on International Information Security*. The concept was unveiled on November 1, 2011 at the London Conference on Cyberspace. Russian Telecommunications Minister Igor Shchegolev delivered a speech which focused on the drafts of the concept and of the Code of State Conduct in Cyberspace.

Shortly before the London conference the concept was presented to heads of secret services and law-enforcement agencies of 52 countries at a meeting behind closed doors in Yekaterinburg on September 22, 2011.[5] The concept of the proposed convention details the infospace (cyber-space) regulation norms, which are designed to counter such threats as cyberterrorism, cybercrime, military-political challenges, and cyber espionage. The concept bans the use of the internet (information and telecommunication networks) for military purposes and for deposing regimes in other countries, while at the same time leaving national governments sufficient freedom of maneuver within their national segments of cyberspace. Shortly before that, on September 12, 2011, permanent representatives of four SCO states—Russia, China, Uzbekistan, and Tajikistan—sent a letter to the UN Secretary-General. Attached to the letter was a draft Code of Conduct on International Information Security. In contrast to the concept of the Convention on International Information Security, the proposed Code of Conduct is not legally binding. On the whole, however, it echoes the ideas of the convention, albeit without such a clear emphasis on the military-political component of cyberspace.

International reaction to Russia's ambitious initiatives has been, for the most part, limited to polite but detached interest, without any active steps or counter-initiatives. According to the information available to the PIR Center, the proposed convention and code of conduct met with a rather mixed reaction in Asia Pacific, where Russia is making energetic efforts in many areas in the run-up to the 2012 APEC summit in Vladivostok. For example, PIR Center experts report that in the second-track format of the Council for Security Cooperation in the Asia-Pacific (CSCAP), which brings together 22 countries, including India, the United States, Japan, China, and Russia, the Russian and SCO initiatives were met with interest—but also with some mistrust and skepticism. The most enthusiastic response came from India; the country aspires to become an IT superpower and is increasingly worried by aggressive activities being undertaken in cyberspace by China, India's main rival in Asia. However, many regional organizations which have a say on matters of security—such as APEC, the East Asia Summit (EAS), ASEAN, and ARF—tend to view the Russian

and SCO initiatives as rather contradictory or even counterproductive for the international cybersecurity agenda.

One of the reasons for such a state of affairs is the opposition of many influential countries, especially the United States. They argue that advertising the problem of cyber threats which are politically motivated or linked to the behavior of state actors only causes discord and hampers regional cooperation, encouraging countries to gang up on their neighbors. In their view, politicizing cyber threats (by talking about cyber wars or cyber conflicts) distorts the international agenda in the area of cybersecurity and distracts partners from a constructive search for the *lowest common denominator*. Also, the United States is especially opposed to those sections of the Russian initiatives which propose a ban on disseminating information ''which inspires terrorism, separatism and extremism, or which undermines the political, economic, and social stability of other countries.'' The absence or vagueness of definitions of such information gives the American diplomats a reason to suspect that these rules will become an instrument of legitimized state censorship and control over cyberspace. For example, after the November conference in London, U.S. Assistant Secretary of State Michael Posner said that the proposed code of conduct was an unacceptable solution because it would turn the internet, which is now a space governed by a multitude of stakeholders, into a system controlled by central governments.[6]

In Europe the reaction to the proposed convention and code of conduct was also mixed and cautious, and for similar reasons. Another factor was that the two documents propose new rules regulating measures to counter cross-border cybercrime. That makes the proposed convention look like an alternative to the existing international mechanism—namely, the 2001 Council of Europe Convention on Cybercrime (the Budapest Convention), which has already been signed by 43 European nations. But it has been less that a year since the two initiatives were announced, so it is too early to view the international reaction they have received so far as final and definitive. These initiatives and the approaches to international information security they propose still deserve detailed analysis, which this piece of research aims to undertake.

TERMINOLOGY: THE ACHILLES' HEEL OF RUSSIAN PROPOSALS?

Analysis of the proposed IIS convention and code of conduct should begin from terminology, which sets the tone of these proposals. The first distinctive feature of the two documents, as well as the Yekaterinburg Agreement, is that their terminology is radically different from that used in Europe, the United States and most of the developing countries. These differences signal two entirely different approaches to the very idea of cybersecurity.

Let us compare, for example, the definition of an information system contained in the proposed convention with the definition used in existing European legislation. The latter can be found in Paragraph (A) Article 1 of the EU Council Framework Decision 2005/222/JHA of February 24, 2005:

> . . . information system means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.[7]

Article 2 (Terms and Definitions) of the proposed IIS convention contains a significantly different definition: ''information system is a complex of information contained in data bases and of the information technologies and technical means necessary for the processing of that information.''[8] That definition was first used in the Russian Doctrine of Information Security of 2000 (hereafter referred to as the Doctrine), and then re-used in key pieces of legislation on information security, including Law No 149-FZ ''On information, information technologies and information security'' of July 27, 2006.[9] A comparison of the Russian definition with the one used by the European Council highlights the fact that the former is ambiguous and too narrow. Its main flaw is that the whole construct centers on *databases*, which are not necessarily a part of information systems in real life. Besides, the second part of the definition introduces a partially recursive idea of information technologies as a means of supporting the operation of information systems.

One other distinctive feature of the Russian Doctrine of Information Security is that it completely avoids any mention of the internet. Instead, it contains terms such as ''open information and telecommunication systems'' and ''global information networks.'' This peculiarity of the doctrine was also inherited by the Russian information security legislation, including the already mentioned Law No 149. The law mentions the internet only once, and then refers to it as merely one of the

''information and telecommunication networks.''[10] In and of itself such wording may be acceptable, but adapting it to European legislation will be difficult because most Western laws in this area specifically refer to the internet.

Some of the most difficult problems with concepts and terminology result from attempts by the authors of the Russian draft to propose terms and definitions which are new in international law. That is especially true of the sections dealing with the conduct of sovereign states in cyberspace. The best (but not the only) example of this is the definition of ''information warfare,'' which is something completely unheard of in international law. The definition used in the proposed IIS convention has already been used in various Russian policy documents. The very idea of ''information warfare'' first appeared in the 2000 doctrine, but it was not fleshed out in any great detail. In 2009 the definition of ''information warfare'' appeared in a legally binding international document—namely, the intergovernmental agreement of SCO member states on cooperation in international information security, signed on June 16, 2009 at the 6th SCO summit in Yekaterinburg (the Yekaterinburg Agreement).

The Agreement defines information warfare as ''hostile action between two or more countries in the information space, with the goal of inflicting damage on the adversary's information systems, processes and resources, critically important and other structures; undermining the adversary's political, economic or social system; mass brainwashing of the adversary's population in order to destabilize its society and state; and forcing a state to make decisions in the interests of its adversary.''[11]

The definition has several potential vulnerabilities:

- First, it discounts the possibility of non-state actors waging information warfare, which is at odds with events in the real world. We can use the examples such as a series of massive and well-coordinated cyberattacks during the August 2008 crisis in Georgia, or during the diplomatic crisis over a Russian war memorial in Estonia in 2007. In both cases it is impossible to trace or demonstrate the link between the perpetrators of those attacks and government agencies. A 2011 report by the PIR Center[12] argues that the only way of reliably establishing a connection between the groups waging attacks in cyberspace and government agencies is with the help of undercover agents working for secret services. But no intelligence service is likely to have the required resources any time soon.[13]

- The definition lumps together several different and unrelated phenomena. On the one hand, it defines information warfare as what essentially amounts to cyberattacks against information and telecommunication networks and infrastructure. On the other, the definition also includes attacks which any Western analyst would describe as classic psychological warfare. As a result, the Russian definition of information warfare applies to such things as the Stuxnet attack and the cyberattacks against the websites of Estonian government agencies (provided of course that both attacks were perpetrated by governments, which many international experts believe was the case). But it applies equally well to Finnish television broadcasts to Soviet territory in the 1980s. The question is, what do all these things really have in common?

- The definition is not entirely correct in describing the goals and objectives of the processes to which it applies. According to Vitaliy Kobernik, a cybersecurity expert with the Russian Foreign Ministry's MGIMO (U) university, cyberattacks do not necessarily aim to damage the information systems, resources, etc. The example of the Stuxnet virus demonstrates that the purpose of such attacks may be to damage the industrial, logistical, energy or other infrastructure; the attack merely uses the information infrastructure as a medium, and cannot succeed if that infrastructure is absent or not functioning. The paradox is that for the attacker to be able to inflict any significant damage on the adversary's national infrastructure via cyberspace, the target nation must have advanced computer networks and rely on these networks to operate its infrastructure, industry, military facilities, and logistics.

- In typical Russian fashion, the definition does not distinguish cybersecurity as a separate branch of information security. This is radically at odds with the existing practice in most foreign countries, especially in the West. The difference here is crucial. The ''information'' adjective, on which the entire Russian legislation and initiatives in this area are based, does not have the same meaning as the ''cyber'' adjective, which is used in Western concepts.

The terminology and classification used in Russian legislation, with its broad understanding of information security, is shared to a greater or lesser extent by most of the post-Soviet countries (Ukraine, Belarus, Moldova, the Central Asian states, Armenia, and Azerbaijan), as well as China. But they represent less than 6 percent of the 193 UN members. Georgia and the Baltic states have already adopted the terminology based on the ''cyber'' root, or on the closely related concepts of computer security and digital security. In May 2008 Estonia adopted a comprehensive national cybersecurity strategy, which is entirely in line with the approaches used by NATO and the EU.[14] Georgia aims to adopt a similar strategy in the near future. In essence, the Russian *extended* approach has been adopted only by China. That approach therefore risks becoming endemic to Russia and China, whereas the Western paradigm of cybersecurity is increasingly being adopted by the developing countries, including the Asia Pacific nations, and becoming the global standard.

The Russian initiatives in this area in the international arena are being hampered not just by the intrinsic shortcomings of the terms and definitions they rely on, but, more importantly, by the fundamental differences with the Western English-language terminology, which is predominant in most parts of the world. Besides, this contradictory nature and vagueness is characteristic of most of the definitions used in the Russian concept, including the terms ''infospace'' and ''spheres of activity.'' The definition of ''information infrastructure'' has almost unlimited scope; theoretically, it can be applied even to a piece of paper. The shortcomings of the key definitions are then duplicated in later references. For example, the term ''information warfare'' is mentioned in one other definition and three separate articles. As a result, all the shortcomings and vulnerabilities of these terms and definitions undermine the entire document. The situation with the SCO Code of Conduct proposal is very similar, because it relies on the same terms and definitions, for the most part.

STATE-CENTRISM: A HEREDITARY DEFECT OF THE RUSSIAN APPROACH

Unfortunately, the vulnerabilities of the terminology on which the Russian proposals rely are not the only problem with these proposals. According to one expert at the Cybersecurity Department of the MGIMO University, a major weakness which lies at the very heart of the proposed convention is the idea that sovereign states can completely control key components of the information infrastructure. For example, neither the proposed convention nor the SCO Code of Conduct proposal contains a single mention of:

- the private sector, which is the main target of cyberattacks, a key stakeholder in the national segment of the internet and information-based economy, a key partner of governments in countering cyber threats, and the main operator and user of information and telecommunication systems, including the internet;
- expert communities, both national and international, which are a key source of expertise on cyber threats and an important participant in the process of formulating the doctrines and visions of cybersecurity;
- civil society, not-for-profit organizations, and NGOs, which are the initiators of broad discussions on cybersecurity issues, a key element of developing and fostering cybersecurity culture, and the ''auditors'' of national governments in this area.

The authors of the Russian proposals seem to believe that all the non-state participants in the process of global governance of the IT sector simply do not exist. In real life, however, the idea of the state being at the center of all things is not entirely correct—at least that is the case in most of the developed countries, where the larger part of critical information infrastructure is not controlled by governments. One obvious example is the 13 root DNS servers, which are run by various entities, most of them private, in cooperation with ICANN, an international not-for-profit organization. There are many other examples, both in the United States and in other countries. Similarly, the government in Washington does not control the information system of the New York Stock Exchange, where 13.39 trillion dollars' worth of shares were traded as of November 2010, which is half of the capitalization of the global stock market.[15] New York Stock Exchange LLC has a status similar to the Russian open joint stock society, which means that its information system cannot be directly controlled by the state. Trading on the New York Stock Exchange, which is located in the vicinity of the World Trade Center site in downtown Manhattan, was disrupted during the 9/11 attacks. Actions by NYSE representatives to restore the normal work of the exchange and

ensure the security of its information system were coordinated with the Securities and Exchange Commission and the U.S. Treasury at an emergency meeting—but even during the 9/11 crisis government bodies did not take over operational control of the exchange.[16,17]

It is important to emphasize that such examples are not unique or endemic to the United States. To begin with, all of these institutions and systems are elements of the global critical information infrastructure. NYSE is a vital component of the stability of the global financial system, of which the Russian financial system is an integral part. The same is true of the information systems of large industrial facilities, such as hydro or nuclear power plants, gas transit pipelines, or transnational energy grids, which are usually operated by the private sector in the developed world. According to research conducted by Symantec in the United States in October 2010, 85 percent of the critical American infrastructure connected to information systems is controlled by the private sector; this includes energy grids, industrial, transport, financial, and energy infrastructure.[18] In most cases critical infrastructure facilities rely on privately owned information networks. Although the information systems of such facilities are not regarded as critical infrastructure, an attack against those systems can lead to major consequences which go far beyond the national borders, reaching a regional or even global scale.

It is therefore clear that the Russian proposals relying on a model in which the state is an undisputed master of all the key assets of the information domain are entirely unacceptable and unrealistic—at least for the developed countries. Meanwhile, the vision of the state as a universal and absolute regulator in cyberspace defines yet another distinctive feature of the proposed convention and code of conduct. Both of them aspire to the role of comprehensive documents and claim to address all the existing gaps in the regulation of international information security.

As Table 1 demonstrates, the concept of the IIS convention aims to regulate international cooperation in the following areas: cybercrime; cyberterrorism; hostile actions by sovereign states in the information space (cyber conflicts and cyber warfare); the use of information as a psychological weapon by sovereign states.

The scale and scope of the Russian initiatives make them attractive in theory—but also create a number of practical difficulties. To begin with, such a broad area of regulation simply cannot be addressed in any concrete detail by a single piece of legislation. The Russian authors have produced a document which is little more than a declaration and lacks the following key elements:

- specific mechanisms of international cooperation to counter cybercrime;
- concrete procedures of cooperation;
- algorithms of preventive action in the area of cyberterrorism, cyber wars, and cyber conflicts;
- areas and formats of dialogue between experts and cultural/educational contacts in the area of cybersecurity, which are indispensible for comprehensive international security;
- measures to arrive at a single set of terms and definitions, which are obviously required, given the specifics of the terminology used in these proposals.

The proposed convention and code of conduct contain only the general principles. In the absence of clear rules and mechanisms for implementing them, these principles are doomed to remain on paper. Also, the authors of the Russian initiatives propose that governments should speak on behalf of all other cyberspace actors in the international arena. According to Madin Kasenov, a professor at the Russian Foreign Ministry's Diplomatic Academy, the same flaw made impossible the adoption of the UN Code of Transnational Corporations. Various drafts of that code were discussed in the period between 1972 and 1992. In the end, the whole idea was abandoned after UN delegates decided that it was impossible to reach a consensus on the issue.[19] After 20 years of trying, the governments failed to agree a legally binding version of the code which would contain effective implementation mechanisms, and—even more importantly—which would be in the interests of the transnational corporations themselves. The reason for that failure is simple: the state cannot comprehensively and independently regulate the institutions, processes, and phenomena which have developed beyond its own limits, with no regard for national borders, and, in the case of cyberspace, beyond government control.

WHAT TO HOPE FOR?

Nevertheless, Moscow is undertaking energetic efforts to promote these Russian and SCO proposals—and for all the flaws of these proposals, Moscow's efforts are neither illogical nor hopeless.

First, the Russian Foreign Ministry has taken a rational and cautious position, as witnessed by several recent statements and official remarks by Russian officials and diplomats. These include the already mentioned speech by Igor Shchegolev, the telecommunications minister, at the London conference on November 1, 2011, and a speech by Kirill Barsky, the Russian President's Special Representative at the SCO, made at the CSCAP General Conference in Hanoi on November 21, 2011. Russian diplomats are well aware that both the proposed convention and code of conduct have serious flaws and limitations. They are therefore trying to position their proposals as an invitation to dialogue on the problems and challenges the two initiatives aim to address. Speaking at the London conference on November 1, 2011, Minister Shchegolev expressed his hope that the Russian concept of the Convention on International Information Security will ''lay the foundations for drawing up a comprehensive convention under the UN auspices.''[20] A very similar tone was used by the Russian presidential representative at the SCO in his speech at the CSCAP General Conference. In essence, that speech was the first official presentation of the Code of Conduct to the Asia Pacific nations, which are seen by Moscow as the target audience for its initiatives on IIS regulation.[21] The Russian initiative is therefore being presented as a work in progress, a flexible early draft which should be seen as an invitation to further dialogue as opposed to a finished product offered to our foreign partners for their approval. Such an approach is the only workable option for the moment, until the existing problems with the Russian and SCO initiatives have been addressed, whereupon both can be re-launched in a more presentable shape. Even if that re-launch happens after 2012, this would be preferable to any attempts to secure international acceptance of a decision which has not been sufficiently thought out. Such unproductive tactics have already been tried when Moscow attempted to win international support for the recognition of South Ossetia and Abkhazia as independent states after the 2008 conflict.

Second, international law allows certain limitations on the dissemination of information that undermines security. In the opinion of the Russian political leadership, just such information was being spread during the Arab Spring. The Russian initiatives echo the rules set out in Article 19 Paragraph 3 of the International Covenant on Civil and Political Rights, which was adopted by Resolution 2200 A (XXI) of the General Assembly on December 16, 1966. According to that paragraph:

> . . . the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media [carries with it special duties and responsibilities and] may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: for respect of the rights or reputations of others; for the protection of national security or of public order, or of public health or morals.[22]

Obviously, a reference to a provision contained in one of the key pieces of international legislation on human rights lends some weight to the Russian Foreign Ministry's position. The problem is, however, that this provision has never really been applied or enforced in practice. We are not aware of a single instance of governments justifying their actions in the area of controlling the dissemination of information by referring to Article 19 Paragraph 3 of the 1966 Covenant. Even the governments of Mubarak, Ben Ali, Gaddafi, Assad, and Lukashenka have not used that international norm—even though in 2011 (and in previous years) all of them were energetically looking for ways of justifying before the international community their efforts to limit the activity of opposition movements in online social networks.

Third, it would be a mistake to believe that the Russian approach is not shared by any other countries, or that the idea of adopting a piece of international legislation covering all the problems of cybersecurity is marginal. In 2010 and 2011 Stein Schjolberg, a prominent Norwegian specialist on cyber law, and his Swiss colleague Solange Ghernaouti-Helie published two editions of the proposed UN Global Treaty on Cybersecurity and Cybercrime. In 2007–2008 Professor Schjolberg served as chairman of the High Level Expert Group on Cybersecurity, which was set up in 2007 to study various options for international coordination of efforts in the area of cybersecurity.[23] The group was supposed to complement the Global Cybersecurity Agenda of the International Telecommunications Union, which was also launched in 2007.[24]

The central idea of the proposed treaty is to adopt a comprehensive approach to international cybersecurity regulation and legislation. In that sense the proposal and the Russian initiatives are fully in line with each other. The difference between them is that, for obvious reasons, European experts do not include in the list of threats the dissemination of information which can undermine social and political stability. Their emphasis is very much on cybercrime. The authors' ambition is to offer an alternative to the definitions contained in the Budapest Convention, and to that convention as a whole. Their draft lists 11 different types of cybercrime, some of which—such as cyberterrorism—are divided into four or five subcategories. Another clear difference from the Russian approach is that the authors do not want, as a matter of principle, to highlight states as an individual category of actors which can perpetrate cybercrime. Articles 11 and 12 of their proposal classify large-scale and carefully planned attacks against critical infrastructure facilities as cyberterrorism, i.e. actions which are aimed against state and society, and which can be perpetrated by an unlimited range of actors (with states not being highlighted as an individual category of such actors).

On the whole, however, the proposed draft of the treaty is more of an experimental research product. It is overburdened with various regulatory norms and multi-tier classifications, and it is just way too cumbersome to serve as a starting point for international negotiation. As one leading Russian specialist on cyber law has put it, ''the proposal is of academic interest in the context of constructing theories and perfect models—but I don't see it becoming a real piece of international legislation.'' That assessment has been borne out by the fact that since the proposed draft of the treaty was published in late 2010 there has not been any notable reaction to it via the UN channels (even though the authors of the draft were on the UN cybersecurity expert group) or via any other channels. Suffice to say that until recently the Russian Foreign Ministry, which is working hard to find allies to promote its own initiatives, was not even aware of the draft treaty's existence.

Fourth, it is true that the approach to the problem of information warfare and information conflicts between sovereign states proposed in the Russian and SCO initiatives is unlikely to win much support. But it cannot be denied that the actual problem of such warfare and conflicts exists, or that it requires regulation on the global level. I am talking about the parts of the Russian definition of ''information warfare'' which coincide with the English terms ''cyber war'' and ''cyber conflict.'' Some common ground can be found on such goals as preventing these cyber conflicts and putting an end to militarization of cyberspace. These issues are at the center of the proposed convention and code of conduct.

The problem is real and pressing; even the United States, which vehemently opposes the Russian initiatives on regulating state conduct in cyberspace, recognizes that the problem exists. According to various experts, research centers, and reports by government agencies, the United States actually suffers more than any other country from hostile actions in cyberspace apparently perpetrated by state actors. Reports released over the past year by various American analytical centers and institutions allege that Chinese and Russian hackers are systemically attacking the Pentagon's networks, trying to steal information from the servers of U.S. government agencies, etc. A report by the Pentagon says that there were more than 6 million attempts at unauthorized access to its computer systems in 2011; the Americans suspect that most of these attempts were made by Russian and Chinese hackers.[25] On July 14, 2011 Deputy Secretary of Defense William Lynn said that in March 2011 the Pentagon's computer network suffered a large and successful attack by ''foreign aggressors.'' He revealed that the perpetrators had managed to steal 24,000 secret files. Although he refused to name the source of the attack, the Pentagon has been dropping heavy hints that it suspects the Chinese.[26] In November 2011 the Americans said that the hacking of U.S. earth observation satellites which took place in 2007 and 2008 was consistent with the latest Chinese military strategies.[27] There has also been an alarming rise in the number of politically motivated cyberattacks against private computer networks of critical infrastructure facilities. According to Symantec, in 2010 some 53 percent of the operators of critical national infrastructure facilities believed that they had experienced such politically motivated attacks.[28]

Nevertheless, the White House is not always on the receiving end of cyberattacks. In September 2011 it became known that prior to the launch of the operation to establish a no-fly zone over Libya, in March 2011 the U.S. military considered the possibility of initiating a massive cyber-strike against the infrastructure of the Gaddafi regime.[29] American military strategists have officially viewed cyberspace as a combat theater ever since the adoption of the Department of Defense Strategy for Operating in Cyberspace; the document was partially de-classified in June 2011.[30] In November 2011 the Pentagon confirmed that in accordance with the Strategy,

it reserves the right to use ''all necessary means,'' including military, ''to defend our nation, our allies, partners and interests.''[31] In essence, Washington now views cyber threats in the same way that it views traditional military threats. There have been some organizational changes as well to reflect the recognition of cybersecurity as a component of military-political security. Back in 2009 the Pentagon set up the U.S. Cyber Command (USCYBERCOM) to deal with threats to the cybersecurity of the United States, including military threats.

China is moving in the same direction. In May 2011 the People's Liberation Army set up a special unit called the Blue Team, tasked with protecting the Chinese military networks.[32] European states, including Germany, are also fully aware of the threat of cyber wars and cyber conflicts. On November 30–December 1, 2011 Germany held an operation codenamed Luekex 2011, which was nothing short of a simulated cyber-war.[33] It involved at least 3,000 officials and imitated massive attacks against the information networks of federal and regional government agencies. According to media reports, the operation was supervised by the National Cyber Defense Center and the secret services. Preparations for it took almost two years.[34] In June 2012 Germany made the next step by setting up a special cyber warfare unit of the Bundeswehr.[35] In 2010 NATO recognized large-scale cyberattacks as one of the most serious threats to international security. The decision was influenced by the Stuxnet virus attack, which damaged the IT infrastructure of the Bushehr nuclear power plant in Iran.[36] Many experts believe that the Stuxnet virus is too complex and sophisticated to be the product of an independent group of hackers; it must have been created using the resources of a state. The Stuxnet attack is believed to be the first real case of cyber weapons being used against the critical infrastructure of a sovereign state; in this case the state under attack was Iran.

All of this raises a legitimate question: is it right for the international community to ignore the initiatives proposed by Russia and its SCO allies regarding regulation of information security in the military-political field? Obviously, the United States and the NATO countries are not particularly bothered at this stage by the lack of international regulation of these problems. The American position is influenced, among other things, by the approaches adopted in its two national strategies, including the active defense paradigm, as well as Washington's traditional reluctance to limit its own freedom of action by international commitments in the area of defense and national security.

Strange though it may seem, from this point of view Russia's position appears to be more constructive. Further development and improvement of various cyber weapons, including new variants of Stuxnet, as well as preparations for waging cyber wars, constitute a serious challenge to international information security. At some point in the future it could become one of the key threats to international security as a whole. For now, governments prefer to make preparations for conflicts in cyberspace instead of trying to preclude the very possibility of such conflicts breaking out. The United States and China in particular are dangerously close to launching a cyber arms race, i.e. creating increasingly sophisticated software to launch cyberattacks and advanced new technologies to defend against the adversary's cyberattacks. The consequences of a full-blown cyber war between states which possess highly developed information and computer technologies are difficult to predict. Damage to critical infrastructure caused by such a war could lead to devastating consequences, especially if the attackers target the computer networks of nuclear and hydro power plants, large industrial facilities, oil and gas pipelines, and strategic transport and logistics operations. Given the globally interconnected nature of information networks, a cyber war will not be limited by national borders. The entire internet could be affected; that is why preventing wars in cyberspace is in the national interests of every country, including Russia.

The fact that the proposed convention has a section which deals with international cooperation in fighting cybercrime, as well as Russia's continued refusal to join the Council of Europe Convention on Cybercrime (the Budapest Convention), gives reason to believe that one of the purposes of the Russian proposal is to offer a global alternative to the existing convention. Moscow will look for allies among the developing countries, in the BRICS bloc, in the Asia Pacific region, etc. Meanwhile, the question of whether Russia should continue to stay out of the Budapest Convention and promote its own initiatives as an alternative requires detailed analysis.

RUSSIA'S POSITION ON THE CE CONVENTION ON CYBERCRIME

At this moment Russia is not a member of the Council of Europe Convention on Cybercrime, which was signed on November 23, 2001 in Budapest. The Budapest Convention is the most well-known

and comprehensive piece of international legislation in this area. Although the convention is open for signature, Russia has refused to join the 43 Council of Europe members and four other states which have signed it.

On November 15, 2005 the Russian president issued a resolution ''On signing the Convention on Cybercrime.'' The resolution authorizes the government to sign the document, but only if Article 32 Paragraph b of the document is revised.[37] The paragraph allows authorized bodies of one member-state to access the computer data stored on the territory of another member-state without securing prior consent from the latter. Specifically, the paragraph reads, ''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.''[38] On March 22, 2008 the president signed another resolution which rescinded the resolution of November 15, 2005. Since then Russia has not shown any interest in the Budapest Convention, focusing instead on its own initiatives in this area. In November 2010 Pavel Livadnyy, an official with the Russian Financial Monitoring Agency (Rosfinmonitoring), had this to say: ''Russia advocates an approach which includes the development of a global convention on fighting crime in the information sphere.''[39] He added that the approach would aim, among other things, ''not to allow any investigations on another country's territory without notifying the law-enforcement agencies of that country.''[40]

The statement reflects the approach to the Budapest Convention that Russia adopted as a matter of principle back in 2010. Representatives of the Russian Cabinet, the Foreign Ministry, and law-enforcement agencies have repeatedly emphasized that the convention would be entirely acceptable were it not for Article 32 (b). As Moscow continued to develop its own initiatives, which propose global regulation of international information security, its policy on the Budapest Convention acquired an element of confrontation. Russia began to position its own proposals as a global alternative to that convention, as opposed to a complementary piece of international legislation. In their criticisms of the convention, Russian officials—especially those representing the Foreign Ministry and law-enforcement agencies—rely on several key arguments. They say that Article 32 (b):

- prevents effective international cooperation by obviating the need for one state party to agree with another state party access to its computer networks;
- undermines the spirit of trust and harmonious coordination;
- provides a cover for unfriendly actions by state parties against each other, and against Russia in particular.

The last point deserves special attention because Russian representatives have never explained their arguments in that regard in any great detail. Based on the existing research and statements by law-enforcement officials, it appears that Russia's main worry is about spying and cyber espionage by European secret services (and since 2007, by American secret services as well—at least in theory). A typical example of such concerns is contained in a statement by Boris Miroshnikov, head of the Interior Ministry's Special Technical Measures Bureau, made on March 1, 2007. Miroshnikov argues that ''the crafty Article 32 pursues purposes which are very different from merely investigating cybercrime,'' adding that ''it is impossible to speak of fruitful and mutually beneficial cooperation if one state party is not even aware of the investigations . . . being conducted in [its] information and communication networks by another party.''[41]

In a more general sense, criticisms of Article 32 (b) boil down to allegations that it violates state sovereignty by allowing uncontrolled intrusion into a state's information networks by third parties. Aleksandr Volevodz, a cyber law expert and professor of the MGIMO (U) University, says that ''in every single country it is possible to find an ISP which has legitimate technical means of accessing computer data stored across the border, or which stores on its own servers some data belonging to a foreign user.''[42] As a result, applying Article 32 (b) to such ISPs enables what amounts to uncontrolled access to computer data in the networks of a foreign state.

There is a certain rational core to these arguments. Nevertheless, they cannot explain Russia's unswerving position, and for a number of reasons. First, such theoretical actions by the Western secret services cannot pose any threat to the information systems and networks of the Russian government agencies, military networks, or critical infrastructure. Therefore, they are no threat to Russian national security. Although the cybersecurity culture in Russia is not all it could be, the

networks of the Russian government agencies—especially those which contain classified information—simply are not connected to the internet. Neither are they maintained by regular ISPs, which would be obliged under the Budapest Convention to grant access to such data.

Second, the practices Mr Miroshnikov hints at in his speech cannot stay undetected forever. In addition, Article 32 (b), just like every other article of the Budapest Convention, applies to all parties, not just to Russia. Of all the parties to the convention, only Germany, Britain, and the United States have about the same level of skills and technical expertise as Russia does as far as cyber-espionage and secret service operations on the Net are concerned. Relying on Article 32 (b) for spying, despite guaranteed retaliatory measures of the same kind, would seem irrational and counterproductive. Besides, theoretically Russia ought to be more interested than anyone else in having access to the Article 32 (b) mechanism—at least that would have seemed to be the case before the United States signed.

There are more rational criticisms of the Budapest Convention; for example, some argue that it has already become obsolete and is no longer up to date with the latest trends in the area which it is supposed to regulate. Critics point out that the convention cannot effectively cope with the new types and methods of cybercrime which have evolved over the past 10 years. These include:

- ❑ phishing;
- ❑ creating and using botnets;
- ❑ advanced spamming technologies;
- ❑ identity theft;
- ❑ crimes committed in the ''virtual worlds'', including such online communities as Second Life;
- ❑ cyberterrorism and the use of cyberspace to glorify violence, extremism, and terrorism.

Some researchers and experts, including Stein Schjolberg and Solange Ghernaouti-Helie, also include in that list large-scale and well-organized cyberattacks against critical and information infrastructure facilities; they view such attacks as a type of cybercrime as opposed to putting them into a separate ''cyber conflicts'' category.[43] It is true that the Budapest Convention has long required some amendments and adjustments. So far there has not been any progress in that direction; that may suggest that the convention is undergoing a certain crisis—or perhaps the parties simply have not realized the need for any amendments. Be that as it may, the practical value of the convention as an instrument for maintaining international cybersecurity will begin to devalue unless the required changes to it are made within the next two or three years.

One final argument in favor of Russia not joining the Budapest Convention is that the document has a regional scope and cannot serve as a truly international piece of legislation. From the practical point of view, that argument is not very meaningful; it can only be taken seriously from a narrow geopolitical point of view. It has to be said that the Council of Europe itself has never aimed to turn the convention into a global piece of legislation—it has simply opened the convention for signature by any country, irrespective of the geographic criteria. Nevertheless, the Council of Europe certainly would not mind at all if more countries joined the convention; the document serves as a conduit of Europe's soft power, and that is something every country in Europe wants to promote.

So far, the Budapest Convention has not become a genuinely global piece of legislation; some of the key international actors on which the state of affairs in the area of cybercrime depends in a major way (including Russia and China) have not signed. The same is true of India, Indonesia, Nigeria, Mexico, Vietnam, and many other densely populated developing countries with a rapidly growing IT sector. For now they play a less significant role in global cybersecurity, but they have a colossal growth potential (which could also translate into growing cybercrime), so the importance of their involvement will grow as well.

There are, however, several indicators which suggest that the Budapest Convention still has a future and a clear potential to acquire new members. In a very important development, the United States ratified it in August 2006 after long and heated debates; the convention entered into force on U.S. territory on January 1, 2007. But for Russia, a far more important fact is that Belarus also decided to join in the spring of 2012. To add insult to injury, the Belarusian authorities did not even

notify their Russian partners and allies of their decision. The application to join the convention submitted by Minsk in May 2012 therefore came as a complete shock to Moscow. The situation clearly illustrates how fragile Russia's positions are as far as promoting its initiatives is concerned. In this particular case the country which has spurned these initiatives is not simply a close Russian ally and a fellow member of the SCO. Worse, Minsk has always been one of the most committed and eager supporters of the ideas of turning the Collective Security Treaty Organization (CSTO) into a ''shield against internet revolutions,'' and an instrument for erecting national cyber borders. Belarus has always argued that proposals to limit the dissemination of information which undermines national sovereignty should be put on the international information security agenda. It may well be, of course, that the decision by the Belarusian president does not signal some new strategic course in the area of cybersecurity; it could be merely part of his constant maneuvering between the EU and Russia. But that does not really change anything. If even Russia's closest allies can spurn Russian initiatives for some small and short-term benefit, at the very least it means that the initiatives themselves require some serious improvement.

Meanwhile, Kazakhstan, another Russian ally and fellow member of the SCO and the CSTO, may also be thinking about joining the Budapest Convention. According to PIR Center sources, Astana intends to sign the convention, although the final decision has yet to be made. Such a decision by Kazakhstan, Moscow's second most important ally in the SCO after China, would be another blow for the Russian initiatives on international cybersecurity regulation.

Still, in deciding whether Russia should join the Budapest Convention, all these considerations are secondary. A far more important question is whether Russia's own national legislation on fighting cybercrime is up to the task. At this moment the situation gives little cause for optimism; some serious and systemic changes are obviously required.

First, cybercrime is growing very rapidly in Russia; all the measures now being taken have failed to contain that growth. According to ESET, the maker of anti-virus software, the number of unique copies of malicious software in the Russian segment of the internet was expected to grow from 40 million to 50–55 million in 2011. The company also estimates that cybercriminals made about 2–2.5 billion euros in the Russian segment of the internet in 2010.[44] A report by Group-IB estimates that ''Russian'' cyber-criminals made about 2.5 billion dollars in 2010; it says the figure will grow to an estimated 3.7 billion dollars in 2012 and 7.4 billion dollars in 2013.[45] In other words, the losses caused by cybercrime are expected to double every year; in two years' time, Russian cybercriminals will probably make about as much as the whole world's cybercriminals made in 2010 (7 billion dollars). Meanwhile, the number of cyberattacks in the Russian segment of the internet rose by an estimated 80 percent in 2010.

The state of the Russian legislation on spam and child pornography on the internet is best demonstrated by the case of a spammer known under the nicknames ''Leo Kuvayev'' and ''Bad Cow.'' In 2005–2010 he was in the Top 5 of the world's most prolific spammers. According to Ilya Sachkov,[46] CEO of Group-IB, for several years Leonid Kuvayev, who was born in Russia, lived mainly in the United States. During that time he developed a very sophisticated automated system of spamming, in addition to selling porn and malicious software via the internet. Every day the system automatically created up to 1,000 new websites for these purposes; the sites were also used for cyber fraud. The spamming network created by Mr Kuvayev continues to earn him about 30 million dollars every year. After the Americans began to investigate him, he returned to Russia on May 11, 2005, where he remained out of reach of the U.S. authorities, including the FBI. Worse, he continued his fraudulent schemes with impunity because he could not be brought to account under Russian laws. It took the Russian authorities five years finally to arrest him—but the charges he faced had nothing to do with cybercrime. He was nabbed under Article 134 of the Russian Criminal Code.[47] According to Mr Sachkov, ''the reality of the Russian legislation is such that achieving a guilty verdict on cybercrime charges of that nature is next to impossible.''[48]

Equally alarming is the situation with the Russian laws on the prevention of internet fraud. Russian law-enforcement agencies have very little experience of bringing cases of internet banking fraud to trial, let alone securing a guilty verdict. The number of such crimes committed in Russia tripled in 2011; a single attack brings the hackers 600,000 to 2 million roubles, on average.[49] Under the existing Russian legal system, only a handful of such cases can be brought to trial, although there are 10–20 successful attacks every month in Moscow alone. In 2009 the Interior Ministry registered more than 15,000 cases of e-banking fraud. In other words, less than 0.1 percent of such cases end in a conviction. In addition, even when cybercriminals are convicted, it is often under articles which are not directly related to cybercrime. One recent example is the case of

Yevgeny Anikin, a hacker who on February 8, 2011 was found guilty of breaking into the RBS WorldPay payment system in 2008, causing 10 million dollars' worth of damage. His accomplices had been extradited to the United States, where they were charged with e-fraud and now face up to 20 years in jail.[50] Mr Anikin, however, got away with a suspended five-year sentence; he was found guilty of grand theft under Article 158, Section B, Part 4 of the Russian Criminal Code.

There is a similar situation in Russia with DoS and DDoS attacks. In 2011 the targets of such attacks, which rely on botnets, were online social networking sites (such as Live Journal), news websites, and interactive communities built on the Ushahidi platform. Especially alarming is the fact that based on the specific nature of these attacks—i.e. their timing and simultaneous attacks against several websites using very formidable resources—experts suspect that they were politically motivated. On the day of the elections to the Russian Duma, December 4, 2011, there were several major DDoS attacks against the websites of news outlets which covered the elections; the Violations Map, an interactive service which gathered information about electoral irregularities in real time; *LiveJournal*, a blogging service popular with the Russian liberal opposition; and other websites. The surprisingly tolerant attitude to such incidents demonstrated by the Russian law-enforcement agencies is compounded by the relative weakness of the Russian laws on DDoS attacks. Speaking in an interview in December 2010, Aleksandr Lyamin, an expert with the Telecommunications and Technologies Center of the Moscow State University, had this to say:

> Most of the articles [of the Russian Criminal Code] dealing with information security cannot be applied to DDoS cases. In all the known cases of people being brought to account, they were convicted under Article 273.[51] But creating, using and disseminating malicious software, which is what this article deals with . . . is not quite the same thing.[52]

As a result, the weakness of the legislative mechanisms and the passivity of the law-enforcement agencies create a climate of impunity for the organizers of such attacks.

There are many other areas in which the situation in terms of fighting cybercrime in Russia is alarming and even threatening. But it has to be said that the weakness of Russian laws is not the only cause of such a situation. Another important reason why cybercriminals can so easily evade the law is the transnational nature of cybercrime itself. It is standard practice for cybercriminals to form groups which include people residing in different countries. Not so long ago criminals living in Russia targeted primarily foreign financial and banking institutions. But that is now a thing of the past thanks to the rapid rise of banking (including e-banking), electronic payment systems, and payment terminals in Russia itself, coupled with the general growth of the Russian economy and the rising incomes of ordinary Russians. The Russian domestic market is now rich enough to attract both Russian and foreign cybercriminals. In 2011 the proceeds generated by cybercrime in Russia rose by 95 percent to 60 billion roubles, making up a third of the global figure.[53]

Taking all of this into account, I believe that the Russian position on the Budapest Convention should be either reviewed, or, at the very least, made the subject of a broad debate within Russia. I also think that the last word in that debate should belong to the business and expert communities rather than the government. For now, there is little reason to expect the Russian government to make a U-turn and join the Budapest Convention instead of promoting its own proposals regarding the Convention on International Information Security. It is therefore up to the expert community, the private sector and the public in general to help form a consensus on this issue.

Another important argument in favor of Russia making a U-turn and joining the Budapest Convention is that time is working against Moscow. Such a conclusion obviously follows from the rapid growth of various types of cybercrime in Russia (by 80–200 percent every year). Another thing to remember is that Russia's proposals regarding the IIS Convention were unveiled less than a year ago; for now we have only an early draft of the possible future piece of UN legislation. Russian cybersecurity experts reckon that it would take at least three to five years for the text of the convention to be agreed at the UN; more time will be required to actually implement the convention's provisions if and when it is adopted. Russia does not have that time; the rapid growth in cybercrime must be reversed within the next two or three years at the very most; otherwise a substantial portion of the Russian IT sector will end up under the control of Russian and foreign cybercriminals.

Of course, joining the Budapest Convention will not be a magic bullet. Besides, the convention itself must be modernized and brought up to date with the current nature of cybercrime, which has changed greatly since the convention was signed 11 years ago. In the short term, however,

Russia cannot afford to wait any longer, and has no alternative to using the opportunities which are offered by the international cooperation mechanisms stipulated in the convention. The recent decision by Minsk, made despite Belarusian support at the SCO and CIS platforms for the ideas of electronic borders and Cyberpol, is a signal to Moscow that it must be realistic in assessing the prospects of its global initiatives.

CONCLUSION

The threats being posed by cyber wars, cyber conflicts, and other aggressive actions by states and actors representing state interests in cyberspace constitute one of the greatest challenges to international information security. Understanding of that fact is increasingly being reflected in the conceptual documents and military doctrines, structural reforms, and policies of many countries all over the world. It is also being discussed by leading politicians and experts. The Russian initiatives are trying, in a perfectly rational and timely manner, to fill the existing regulatory vacuum in international cooperation to defeat that threat. It is right and proper for Russia to propose new international legislation which addresses these goals; the proposed Convention on International Information Security and the Code of Conduct are in line with Russian national interests.

Nevertheless, in their current form, the Russian proposals on global regulation of IIS are unlikely to win sufficient support in the international arena to become a new piece of UN legislation. These proposals have too many systemic flaws and major deficiencies in terminology. Their greatest vulnerabilities are as follows:

- They attempt to build a system of international norms on the basis of Russian national laws on information security. These laws, however, have gaping holes in them; they lack a systemic approach, and are often obsolete. Besides, they run counter to some of the basic principles of the political and legal systems of most of the developed countries.
- They fail properly to take into account the network-centric nature of the information space. As a result, they ignore the fact that cyberspace is governed by many stakeholders, and make an unrealistic assumption that information space can be completely controlled by states.
- They are dominated by bureaucratic interpretations of information security, which seem to have been formulated by law-enforcement agencies. As a result, they often misuse various pieces of terminology and misidentify the areas and the subjects which require international regulation.
- The regulation principles and initiatives they contain are at odds with the interests of key foreign countries whose support is indispensible for any proposed piece of international legislation.
- They assume that the complex and multi-faceted cybersecurity agenda can be addressed in a single, global, and comprehensive piece of international legislation. This assumption is not shared by most of our foreign partners; it is also at odds with the decentralized nature of cyberspace.

To prevent its initiatives from fading into obscurity, Russia needs to retrace its steps back to the level of institutions which formulate coherent national policy on cybersecurity—otherwise all efforts by the Russian Foreign Ministry will be doomed to failure.

The question of whether Russia should join the Budapest Convention must be reopened. The objections being mounted against Article 32 (b) of the convention by the Russian law-enforcement agencies are not sufficiently convincing and may in fact be based on questionable assumptions. Russia needs to revise the practice whereby these agencies have a decisive say in the formulation of the official Russian position in this area. Given the weakness of the national mechanisms for fighting transnational cybercrime, and the absence of any workable alternatives, signing the Budapest Convention may well be in Russian national interests—even if official Russian diplomacy does not share this point of view.

The Russian position on the Budapest Convention must be revised; at the very least, it must become the subject of a broad debate in which the Russian secret services do not have the decisive say. For now, however, there is little reason to expect that the Russian political leadership

will make a U-turn on its current policies on international cooperation in fighting cybercrime, including the question of signing the Budapest Convention. It is therefore up to the expert community, the private sector, and the public in general to help form a consensus on this issue. 

NOTES

[1] ''Department of Defense Strategy for Operating in Cyber Space,'' Department of Defense Official Website, July 2011, <http://www.defense.gov/news/d20110714cyber.pdf>, last accessed June 26, 2012.

[2] Andrey Krutskikh, ''Political and Legal Basis of Global Information Security,'' *Mezhdunarodnyye Protsessy*, No. 1 (13), 2007, <http://www.intertrends.ru/thirteen/003.htm>, last accessed June 25, 2012.

[3] Ibid.

[4] John Markoff, ''Step Taken to End Impasse Over Cybersecurity Talks,'' *New York Times*, July 16, 2010, <http://www.nytimes.com/2010/07/17/world/17cyber.html>, last accessed June 26, 2012.

[5] Yelena Chernenko, ''Russia Enters the Internet Forum with its Own Rules,'' *Kommersant*, No. 205 (4746), November 1, 2011, <http://www.kommersant.ru/doc/1807713/print>, last accessed June 26, 2012.

[6] Ibid.

[7] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (Acts adopted under Title VI of the Treaty on European Union), *Official Journal of the European Union*, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF>, last accessed June 26, 2012.

[8] The Convention on International Information Security (Concept), Russian Ministry of Foreign Affairs, <http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument>, last accessed June 21, 2012.

[9] Russian federal law of July 27, 2006, No 149-FZ, ''On Information, Information Technologies and Protection of Information,'' *Rossiyskaya Gazeta*, Federal edition No 4131. Published on July 29, 2006, <http://www.rg.ru/2006/07/29/informacia-dok.html>, last accessed June 23, 2012.

[10] Ibid.

[11] ''On the Ratification of the Agreement between the Governments of Member-states of the Shanghai Cooperation Organization on Cooperation in International Information Security,'' Law of the Republic of Kazakhstan of June 1, 2010. No 286-IV, <http://e.gov.kz/wps/wcm/connect/62b81c00433164d5bac4be06acaf12a7/Z100000286_20100601.htm?MOD=AJPERES&CACHEID=62b81c00433164d5bac4be06acaf12a7&useDefaultText=0&useDefaultDesc=0>, last accessed June 26, 2012.

[12] Oleg Demidov, ''Social Networking Services in the Context of International and National Security'' (report), Security Index, No. 1 (98), Winter 2012.

[13] Ibid.

[14] ''Cyber Security Strategy,'' Cyber Security Strategy Committee, Ministry of Defence, Estonia, Tallinn 2008, <http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf>, last accessed June 26, 2012.

[15] World Federation of Exchanges, NYSE Euronext—New York, <http://www.world-exchanges.org/member-exchanges>, last accessed June 25, 2012.

[16] NYSE Euronext, September 8, 2004: Testimony of Robert G. Britz, President and Co-COO, New York Stock Exchange, Inc. on ''Protecting our Financial Infrastructure: Preparation and Vigilance,'' before the Committee on Financial Services U.S. House of Representatives Washington, DC, Serial No. 108–108, 163 pp.

[17] ''Critical Infrastructure Protection, Efforts of the Financial Services Sector to Address Cyber Threats,'' report to the Subcommittee on Domestic Monetary Policy, Technology, and Economic Growth. Committee on Financial Services, House of Representatives, January 2003, <http://www.gao.gov/new.items/d03173.pdf>, last accessed June 26, 2012.

[18] ''Critical Infrastructure Protection Study,'' Symantec, 2010. <http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=CIP_survey>, last accessed June 26, 2012.

[19] R. Alan Headley, ''Transnational Corporations and Their Regulation: Issues and Strategies. Abstract,'' CSULA Instructional Web Server, <http://instructional1.calstatela.edu/tclim/S09_Courses/HEDLEY-tncs.pdf>, last accessed June 26, 2012.

[20] Statement by Igor Shchegolev at the London Conference on Cyberspace, London, November 1, 2011, Russian Ministry of Communications and Mass Media Official Website, <http://minsvyaz.ru/ru/speak/index.php?id_4=42975>, last accessed June 24, 2012.

[21] Kirill Barsky, Special Representative of the President of the Russian Federation on the Shanghai Cooperation Organization, ''The International Information Security as a Global Challenge: The Shanghai Cooperation Organization's Vision,'' text of the statement available from the PIR Center.

[22] International Covenant on Civil and Political Rights, adopted by Resolution 2200 A (XXI) of the General Assembly on December 16, 1966, United Nations official website, <http://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml>, last accessed June 25, 2012.

[23] The High-Level Experts Group on Cybersecurity (HLEG), International Telecommunication Union official website, <http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html>, last accessed June 25, 2012.

[24] Stein Schjolberg and Solange Ghernaouti-Helie, ''A Global Treaty on Cybersecurity and Cybercrime. Second edition, 2011,'' <http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf>, last accessed June 26, 2012.

[25] The Pentagon's New Cyber Command. ISN ETH Zurich. December 20, 2010, <http://www.isn.ethz.ch/isn/Digital-Library/ISN-Insights/Detail/?lng=en&id=125768&contextid734=125768&contextid735=125766&tabid=125766>, last accessed June 27, 2012.

[26] ''Pentagon Admits Suffering Major Cyber Attack in March,'' BBC News, July 14, 2011, <http://www.bbc.co.uk/news/world-us-canada-14157975>, last accessed June 26, 2012.

[27] Tony Capaccio and Jeff Bliss, ''Chinese Military Suspected in Hacker Attacks on U.S. Satellites,'' Bloomberg, October 27, 2011, <http://www.bloomberg.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html>, last accessed June 25, 2012.

[28] ''Half of Critical Infrastructure Providers Have Experienced Perceived Politically Motivated Cyber Attacks,'' Symantec, Press Release, October 6, 2010, <http://finance.yahoo.com/news/Half-of-Critical-iw-478930509.html?x=0&.v=1>, last accessed June 26, 2012.

[29] Eric Schmitt and Thom Shanker, ''U.S. Debated Cyberwarfare in Attack Plan on Libya,'' *New York Times*, October 17, 2011, <http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1>, last accessed June 24, 2012.

[30] ''Department of Defense Strategy for Operating in Cyberspace,'' U.S. Department of Defense official website, July 2011, <http://www.defense.gov/news/d20110714cyber.pdf>, last accessed June 26, 2012.

[31] David Alexander, ''U.S. Reserves Right to Meet Cyber Attack with Force,'' *Reuters*, November 15, 2011, <http://www.reuters.com/article/2011/11/16/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116.>, last accessed June 25, 2012.

[32] ''Chinese Military Sets Up Special Cyber Warfare Unit,'' *The Economic Times*, May 28, 2011, <http://articles.economictimes.indiatimes.com/2011-05-28/news/29594039_1_cyber-attacks-cyber-warfare-cyber-defence>, last accessed June 26, 2012.

[33] ''Simulated Cyber-war Begins in Germany,'' Lenta.ru, November 30, 2011, <http://lenta.ru/news/2011/11/30/lunex/>, last accessed June 23, 2012.

[34] Ibid.

[35] ''Bundeswehr bedingt bereit für den Cyberkrieg,'' *Financial Times Deutschland*, June 5, 2012, <http://www.ftd.de/politik/deutschland/:elektronische-aufruestung-bundeswehr-bedingt-bereit-fuer-den-cyberkrieg/70046056.html>, last accessed June 26, 2012.

[36] ''Germany's Cyber Defense Center Goes Fully Online,'' *Deutsche Welle*. June 16, 2011, <http://www.dw-world.de/dw/article/0,,15161387,00.html>, last accessed June 27, 2012.

[37] Council of Europe, Convention on Cybercrime, Budapest, 23.XI.2001, Council of Europe official website, <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm>, last accessed June 24, 2012.

[38] Ibid.

[39] ''Russia Refuses to Ratify the CE Convention on Cybercrime,'' *Vzglyad.* November 9, 2010, <http://www.vz.ru/news/2010/11/9/445958.html>, last accessed June 25, 2012.

[40] Ibid.

[41] Boris Miroshnikov, head of the Russian Interior Ministry's Bureau of Special Technical Measures, ''Prospects for International Cooperation on Criminal Cases,'' report at a conference as part of the Project on International Cooperation on Criminal Investigations, headlined, March 1, 2007, Russian Ministry of Internal Affairs, <http://www.mvd.ru/reform/interview/show_83370/>, last accessed June 26, 2012.

[42] Alexander Volevodz, ''Convention on Cybercrime: Innovations of Legal Regulation,'' *Legal Issues in Telecommunications*, No. 2 (2007), pp. 17–25, <http://www.mgimo.ru/files/113908/113908.pdf>.

[43] Stein Schjolberg and Solange Ghernaouti-Helie, ''A Global Treaty on Cybersecurity and Cybercrime,'' Second edition, 2011, Article 11—Massive and Coordinated Cyberattacks against CriticalCommunications and Information Infrastructures, <http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf>, last accessed June 26, 2012.

[44] ESET, ''Cybercrime Market in Russia, Results of 2010,'' ESET, <http://www.esetnod32.ru/.company/news/?id=35865&year=2011#>, last accessed June 25, 2012.

[45] ''Russian Cybercrime Market in 2010: Current State and Trends,'' Moscow, 2011, Group-IB, <http://www.group-ib.ru/wp-content/uploads/2011/03/GIB-Issl-rynka_2010.pdf>, last accessed June 22, 2012.

[46] Ilya Sashkov, ''Legal Aspects of Fighting Cybercrime,'' report as part of the Special Program RIW-2011, Russian Internet Week, October 18, 2011, <http://2011.russianinternetweek.ru/program/>, last accessed June 26, 2012.

[47] Intercourse or other sexual acts with a person under 16 years of age.

[48] Ilya Sashkov, ''Legal Aspects of Fighting Cybercrime,'' report as part of the Special Program RIW-2011, *Russian Internet Week*, October 18, 2011, <http://2011.russianinternetweek.ru/program/>, last accessed June 26, 2012.

[49] ''Number of E-banking Fraud Cases Triples,'' DIGIT, a RIA Novosti project, October 28, 2011, <http://digit.ru/internet/20111028/385602315.html>, last accessed June 25, 2012.

[50] ''Russian Hacker Receives a Suspended Sentence for Stealing 10m Dollars,'' BFM.Ru, February 8, 2011, <http://www.bfm.ru/articles/2011/02/08/za-krazhu-10-mln-rossijskomu-hakeru-dali-uslovnyj-srok.html>, last accessed June 26, 2012.

[51] Russian Criminal Code of June 13, 1996, No 63-FZ (approved by the Russian Duma on May 24, 1996) (current edition), Article 273, ''Creating, Using and Disseminating Malicious Software,'' <http://www.consultant.ru/popular/ukrf/10_38.html#p4556>, last accessed June 23, 2012.

[52] ''Internet Conference: DDoS Attacks in Russia as an Instrument of Dishonest Competition,'' IA Klerk.ru, December 16, 2010, <http://www.klerk.ru/buh/articles/205822/>, last accessed June 26, 2012.

[53] ''Russia is One of the World Leaders in Terms of Cybercrime—Main Interior Ministry Department,'' RIA-Novosti news agency, April 4, 2012, <http://ria.ru/incidents/20120404/617989613.html>, last accessed June 28, 2012.