CONFLICT STUDIES RESEARCH CENTRE

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МГУ ИМЕНИ М.В.ЛОМОНОСОВА

Russia's "Draft Convention on International Information Security"

A Commentary

April 2012

Conflict Studies Research Centre
PO Box 86 Watlington Oxford OX49 5XE UK
www.conflictstudies.org.uk

Institute of Information Security Issues
Moscow State University
www.iisi.msu.ru

Russia's Draft Convention on International Information Security – A Commentary

Introduction

In September 2011, a "Draft Convention on International Information Security" was released at an "international meeting of high-ranking officials responsible for security matters" in Yekaterinburg, Russia.

This commentary, produced jointly by the Institute of Information Security Issues (IISI) of Moscow State University and Conflict Studies Research Centre, an independent research group based in the UK, seeks to explain key provisions of the draft Convention and the reasoning behind them – particularly in those areas where this reasoning may be at odds with the Western consensus on basic concepts of internet security.

The key provisions of the document have been condensed into a list of 23 fundamental issues of concern to Russia in information space by IISI, whose staff members were closely engaged in developing the draft Convention. Of these 23, 20 have been used by IISI in the text of this commentary to group concepts and ideas expressed in the draft. Part I of this document comprises a parallel commentary on each of these principles, and the citations from the draft which embody them, by both IISI and CSRC. Part II consists of additional commentary by CSRC on specific sections of the draft which are not explicitly referenced in Part I; this is because CSRC identified many more points of contention and possible disagreement in the document than are explicitly listed by the Russian commentary. Finally, two appendices cover translation and linguistic issues in the draft, and potential scope for confidence and security building measures based on the text.

It should be noted that the translation into English cited in this commentary, provided by IISI, differs in some areas from official translations provided publicly[1] and from the bilingual printed version distributed by IISI. Minor variations of translation have therefore been disregarded for this commentary, and comment has only been made on those instances where a mistranslation, or use of contentious terminology, could convey an impression in English which appears at odds with the authors' intentions.

Part I. Joint IISI-CSRC Commentary

This section lists each key principle of information security put forward by IISI, notes the section of the draft Convention which is pertinent for that principle, and then offers parallel commentary by IISI and CSRC.

It will be noted that in some cases, the two commentaries differ so widely as to appear completely unrelated despite proceeding from the same text. This is illustrative of the disparity between the concepts and assumptions of Russian and Western views, which provides a fundamental obstacle to agreement on some of the provisions of the draft Convention. At the same time Part I does not constitute an exhaustive list of the points of difference between the Russian proposals and generally accepted views in the USA, UK and other states: examples of further important divergences are listed in Part II.

[1] For example as available on the website of the Russian Embassy to the UK, at http://rusemb.org.uk/policycontact/52

1. Acknowledgement of the triad of threats originating from cyberspace

Draft Convention reference:
Article 4. Major threats to international peace and security in the information space
The following threats causing disruption of international peace and security in the information space are considered to be major ones:
1) the use of information technologies and other means in order to carry out hostile actions and acts of aggression;
2) an intentional destructive impact produced upon critically important structures or frameworks of another nation in the information space;
4) activities in the information space with the object to undermine the political, economic, and social systems of another nation, a meticide destabilizing the public;
5) the use of the international information space by government and non-government entities, organizations, groups, and individuals for extremist, terrorist, and other criminal purposes;

IISI commentary

The triad is not fundamentally criticized; most countries acknowledge its existence in the cyberspace to a greater or lesser extent (although, we need to distinguish the triad in the cyberspace and the triad in the information space). Almost nobody speaks of threats in the information space. Probably, a separate notion is needed for the threats in the information space, and the "threat of malicious content" shall be included in each of the threat triads. It is generally agreed that there is the problem of attribution, as determining the source of a threat takes certain time and till then the malicious content shall be isolated and eliminated. On the international level selective blocking of malicious content is widely accepted and used. The main requirement here is that such blocking shall correspond to the goals and objectives so as not to limit the rights and freedoms of information space users.

A number of states allocate the cyber-espionage, financial fraud and intellectual property theft to a separate category. Those elements, to our mind, quite correspond to the extended interpretation of the term "cyber-crime" that includes not only crime existing in the physical world and using information technologies as a tool, but also crime that has been enabled

CSRC commentary

The existence of a “triad of threats” is a repeated theme in Russian commentary on information security, yet is not defined in any official documentation. It would be helpful therefore, since it is suggested that “acknowledgement of the triad” is a main principle behind the draft Convention, if a clear definition were attached, since this is not a commonly-used phrase elsewhere.

The principle refers to “threats arising from cyberspace”, yet the cited draft Convention text refers to “information space”, which may or may not be the same thing depending on interpretation of the definition given in the draft Convention. Understanding what precisely is meant by “information space” is key to assessing the viability of the Article cited, and in fact essential to the entire draft Convention, yet at present this term is imperfectly defined and inconsistently applied throughout the text. (For further discussion of this and of “meticide”, see Appendix A.)

by information technologies. Cyber-espionage can be classified by goal. If it involves industrial espionage such act falls under the category of cyber-crime. If the actor is a state then it is classified as use of information space for military or political goals.

"At the present time terrorists mostly rely on these technologies to communicate, collect information, recruit, organize, promote their ideas and actions, and solicit funding, but could eventually adopt the use of ICTs for attack. Thus far, there are few indications of terrorist attempts to compromise or disable ICT infrastructure or to execute operations using ICTs, although they may intensify in the future."[2]

The US criticism aimed at decreasing the significance of the threat of cyber-space use by states for military and political goals turns out to be not quite appropriate as the United States themselves actively create cyber-troops, increase their presence in cyber-space, and, furthermore, consider cyber-space as another area of confrontation. Meanwhile, the concept of collective defense in cyber-space is actively promoted at the level of NATO allies, along with the idea of applying Article V of the North Atlantic Treaty in case of attacks in cyber-space.

2. Threat of using content in order to influence the social and humanitarian sphere

Draft Convention reference:
Article 4. Major threats to international peace and security in the information space
The following threats causing disruption of international peace and security in the information space are considered to be major ones:
4) activities in the information space with the object to undermine the political, economic, and social systems of another nation, a meticide destabilizing the public;
7) the use of the information infrastructure in order to disseminate information inciting inter-ethnic, inter-racial, and inter-religious hatred; to distribute written

[2] {Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.|Report of the Group of Governmental Experts on Developments in the Field of Information and. Telecommunications in the Context of International Security. }{Одобрен на 65 сессии Генеральной Ассамблеи ООН 30 июля 2010 года.|Approved at the 65th session of the UN General Assembly on 30 June 2010.}

materials, images, or any other representations of racist and xenophobic ideas or theories which promote, support, or incite hatred, discrimination or violence against any individual or a group of individuals when such factors as race, the color of skin, national or ethnic origin, or faith are used as a pretext;
8) manipulating information flows within the information space of other nations, disseminating disinformation and withholding information in order to distort the psychological and spiritual environment of the public, eroding traditional, cultural, moral, ethical, and esthetical values;

IISI commentary

The countries that have taken a liberal approach towards content (primarily the US) show anxiety and claim that nobody has the right to control the content as that would "hinder the free flow of information on the net, lower the intensity of innovations", etc. However, the US acknowledge the existence of content that should not be present in real life, and, therefore, should not be present on the Internet. Specific US criticism presented by Michele Markoff (article in Kommersant of 8 February): “Authorities of some states consider the free exchange of ideas on the Internet as inacceptable from the political and cultural point of view or perceive it as a threat to political stability." Therefore, they try to picture this Convention as a document infringing on human rights in favor of establishing government control over content.

The question of using content in order to influence the social and humanitarian sphere covers the integrity of ethical ideas, norms and traditions of a single state as applied to the information space. A state, basing on its sovereignty and acting on behalf of its citizens, determines that specific content carries some negative elements and limits its spread at the legislative level. Bans and restrictions on information inciting inter-ethnic, inter-racial, and inter-religious hatred or promoting hatred, discrimination or violence against any individual or a group of individuals when such factors as race, the color of skin, national or ethnic origin, or faith are used as a pretext, are quite legitimate and are practiced by the international community. Article 19 of the International Covenant on Civil and

CSRC Commentary

Much of the activity described in the text cited is already covered by the International Covenant on Civil & Political Rights and European Convention on Human Rights, to both of which Russia is a signatory. There is no clear explanation why in this case any new legal instrument is required covering the same ground.

Language has been borrowed from this and other international legal documents, including the Budapest Convention, but without the coherence provided by the original full text. This is indicative of the fact that the fundamental principles referred to are already governed by international legal obligations which cover all areas of life, including use of ICT. Furthermore, the obligations described in the text appear only to apply to states, which neglects the multi-stakeholder nature of cyberspace and the key role of individuals, civil society and corporations.

Paragraph 8 is problematic because in US and UK concepts and definitions, it appears to be referring to a different category of state activities than cyber security.

Although protection of traditional cultural, moral and other values is a concern expressed in other Russian documents, for example the Information Security Doctrine (2000), in international terms this belongs more in a convention of protection of cultural heritage rather than a document which appears to deal primarily with cyber security.

The Western consensus, as expressed for instance in Organisation for Economic

Political Rights states that "the exercise of human rights may be subject to certain restrictions: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order, or of public health or morals."

Cooperation and Development (OECD) recommendations on principles for internet policy making, recognises the threat from hostile code, but generally discounts the issue of hostile content. Instead, a basic principle is of: "free flow of information and knowledge, the freedom of expression, association and assembly, the protection of individual liberties, as critical components of a democratic society and cultural diversity".[3]

The definition of "information space" requires clarification. (For more detail on this and "meticide", see Appendix A.)

3. Threats to human rights and freedoms

Draft Convention reference:
Article 4. Major threats to international peace and security in the information space
The following threats causing disruption of international peace and security in the information space are considered to be major ones:
9) the use of information and communications technologies and other means to the detriment of the human fundamental rights and freedoms realized through the information space;

IISI commentary
This Convention is depicted as a document infringing on human rights in order to establish government control over content.

At the same time, freedom doesn't mean anything goes. One man's freedom ends where another person's freedom begins. In accordance with the US International Strategy for Cyberspace, the fundamental human rights and freedoms on the Internet are: freedom of expression and association; privacy; free flow of information. However, censorship and restrictions on the freedom of expression are recognized: there are "exceptions to free speech in cyberspace". Certain content "has no place in any society, and thus, it has no place on the Internet". "Our commitment to freedom of expression and

CSRC commentary
The explicit support for human rights commitments is to be welcomed. It would be helpful if this section were to be developed further, in order to understand more fully the nature, extent and limits of this support.

For instance, the Preamble to the draft Convention refers to "the necessity of ensuring the appropriate balance between maintaining law and order and protecting fundamental human rights, as foreseen in the 1966 International Covenant on Civil and Political Rights". This provision is echoed in Article 5, Paragraph 18, which reads: "each State Party aims to maintain a balance between fundamental human rights and the effective counteraction of terrorist use of the information space;" – thus omitting a reference to the Covenant

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

association is abiding, but does not come at the expense of public safety or the protection of our citizens." The right to privacy can also be limited, in case of investigation by law enforcement authorities.

Article 19 of the International Covenant on Civil and Political Rights states that "the exercise of human rights may be subject to certain restrictions: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order, or of public health or morals."

Article 10 of the EU Convention for the Protection of Human Rights (Freedom of expression)[4] also states that "everyone has the right to freedom of expression", yet "the exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary".

and instead "balancing" human rights with effective CT measures.

Two key treaties form the basis of international human rights law and are widely ratified: the International Covenant on Civil and Political Rights (ICCPR)[5] and International Covenant on Economic, Social and Cultural Rights (ICESCR) 1966[6]. Civil rights include the rights to freedom of expression and assembly. The UK and Russia (amongst others) are parties to the European Convention on Human Rights, which essentially contains the same civil and political rights as the ICCPR, occasionally formulated slightly differently.

The "balancing" act and the issues it is necessary to balance are clearly set out in existing legal instruments, to which Russia and others are party, and these apply equally in a cyber context.

4. Threats of abuse of dominant position in cyberspace

Draft Convention reference:
Article 4. Major threats to international peace and security in the information space
The following threats causing disruption of international peace and security in the information space are considered to be major ones:
3) an illegal use of information resources of another nation without a permission from the nation whose information space houses such resources;
10) opposing the access to the latest information and communications technologies by other nations or creating conditions for a technological dependency of other nations in the field of informatization;
11) information expansion, obtaining the control over national information resources of other states.

[4] http://conventions.coe.int/treaty/en/Treaties/Html/005.htm
[5] http://www2.ohchr.org/english/law/ccpr.htm
[6] http://www2.ohchr.org/english/law/cescr.htm

IISI commentary

There is no criticism of the Convention in this area, as those issues are not covered in documents on cyber-security of other countries.

Domination in cyberspace is generally regarded from the point of view of military presence, creation of cyber-weapons and capability to conduct operations in cyberspace. The US consider cyber-space as another area of confrontation. Meanwhile, the concept of collective defense in cyber-space is actively promoted in NATO, along with the idea of applying Article V of the North Atlantic Treaty in case of attacks. While the defense objective is declared, nothing seems to hinder creation of offensive cyber-weapons for counter-attack.

CSRC Commentary

The citations provided raise several issues, including the stated desire for technological equality between nations. Article 5, Paragraph 3 chimes with this concept by stating that “each State Party must strive to overcome the disparity in the level of equipment of national information systems with modern information and communication technologies, to bridge the ‘digital divide’ with the purpose of lowering the general threat level in the information space”. This appears to be calling for technologically advanced states to share ICT with those less well advanced. Yet for the US, UK and similar countries, given the degree of commercialisation of information and technology infrastructure, this would appear to be far more a business issue than an inter-governmental one – all commonly used ICT technology is commercial, and innovation takes place in the private sector, so any restrictions on the transfer of technology would be far more likely to arise from commercial considerations and protection of the competitive advantage of a corporation than from government policy. The ICT boom in developing countries has been accelerated by private companies, and as a result most ICT technology is available nowadays for all actors in global information society.

In this case, how precisely do States Party address the issue in the terms set out in this paragraph? It would also be helpful if it were set out more clearly where, even if this were possible, the obligation arises for them to facilitate technology transfer to less advanced states, and how precisely this would “lower the general threat level”.

In so far as the ambitions of this section are realisable, they are already enshrined in international obligations, for example, target 8F of the UN’s Millennium Development Goals, which calls on states to “in co-operation with the private sector, make available the benefits of new technologies, especially information and

communications".[7]

Yet at the same time transfer of some strictly limited technologies falls squarely in the dimension of national security. Control of specific security-sensitive technologies has historically been the prerogative of states, a fact which has not, hitherto, been treated as a threat in and of itself. In effect, the draft, as it stands, if it were applied to all technologies indiscriminately would compel states to act against their own security interests, which may be unrealistic.

Use of the word "illegal" is problematic without a clear explanation of which jurisdiction or legislation is to determine legality.

5. Principle of indivisibility of security

Draft Convention reference:
Article 5. The basic principles of the international information security
The information space is in the public domain. Its security makes the foundations for the sustainable development of the global civilization.
In order to create and maintain the atmosphere of trust within the information space, the member states must adhere to the following principles:
2) the member states, while forming the international information security system, will be governed by the principle of indivisibility of security which means that the security of each of the member states is inseparable from the security of all other states and the international community as a whole, the member states will not strengthen their security at the expense of the security of other states;

IISI commentary
The principle of indivisibility of security was adopted and legally drawn during the Budapest summit of OSCE in 1994. It is recognized by many countries, but is not yet observed as conceived. For example, in response to Russian concerns regarding the US deploying its missile defense shield in Europe we received only verbal assurances of its not being directed against Russia. It is unlikely that countries that have the capabilities and resources will reduce their level of security to the level of the weaker

CSRC commentary
The mention of indivisibility of security is problematic. This is because shared usage of this common phrase by Russia and its partners hides fundamental disagreement over its meanings - which are entirely different in Russian and in English. Despite recognition and patient explanation that use of the identical phrase to refer to widely differing concepts leads to misunderstanding and frustration,[8] the phrase continues to occur in both Western and Russian discourse leading to each side embarking on their own separate

[7] http://www.un.org/millenniumgoals/global.shtml
[8] NDC, "The Indivisibility of Security: Russia and Euro-Atlantic Security," NATO Defense College, Rome, 2010.

states.

The principle of indivisibility of security in cyberspace has a slightly different meaning. Most states recognize (and this is confirmed in the report the UN Group of Governmental Experts) that cyber-security cannot be achieved unilaterally. This is prevented by the very nature of cyberspace – the networks and systems are interrelated and interdependent. Therefore, the need for security dictates the need for cooperation between the countries. In addition, states do not oppose the need for developing confidence-building measures, exchange of information on the views on information security, joint investigation of incidents, or creating "hot lines" for emergency situations in the information space.

Thus the thesis on strengthening one's own security to the detriment of others does not work in the open international cyberspace. However, it can be applied in case of collective defense in the cyberspace (for example, collective defense of NATO or CSTO states), when it comes to military information systems and networks.

If the security level can be detected in the physical world (strengthening of borders, movement of troops, weapons testing), in the virtual world it is quite complicated and can only be based on indirect evidence.

conversation.[9] The term should be avoided, or carefully defined.

The concept that "the member states will not strengthen their security at the expense of the security of other states" is a specifically Russian preoccupation, Implicit in it is the zero-sum principle that any improvement in the security of any of Russia's foreign partners necessarily entails insecurity for Russia and is therefore a political problem. This is an approach which does not mesh with the post-nationalist, cooperative approach of Russia's partners in Europe and North America, and its inclusion in the draft Convention would therefore be problematic.

Furthermore it is unclear what precisely "forming the international information security system" means – is this a reference to states subscribing to this draft Convention?

Finally, the text as it stands is too state-centric and does not reflect the multi-stakeholder reality of cyberspace, its threats and targets.

6. Network sovereignty

Draft Convention reference:
Article 5. The basic principles of the international information security
The information space is in the public domain. Its security makes the foundations for the sustainable development of the global civilization.
In order to create and maintain the atmosphere of trust within the information space, the member states must adhere to the following principles:
1) the activities of each member state within the information space must promote social and economic development and be implemented in such a way as to be

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

compatible with the goals of promoting international peace and security and align with the generally recognized principles and norms of international law, including the principles of peaceful settlement of disputes and conflicts, the non-use of force in international relations, the nonintervention in the internal affairs of other nations, the respect for national sovereignty and fundamental human freedoms and rights;
4) within the information space all member states enjoy a sovereign equality, have the same rights and obligations and are the equal subjects of the information space regardless of economic, social, political, or other differences;
5) each member state is entitled to set forth sovereign norms and manage its information space according to its national laws. The information infrastructure located in the territory of a member state or otherwise existing under its jurisdiction is subject to the sovereignty and laws of such member state. The member states must strive to harmonize their respective national legislations, the existing differences shall not make barriers to the formation of a reliable and secure information environment;
8) each member state, while taking into account the legitimate security interests of other states, may freely and independently determine its own interests in respect to ensuring information security as based on the principle of sovereign equality and be free to choose its own methods of information security in conformity with international law;

IISI commentary

There is indirect criticism of the Convention provisions on network sovereignty. First of all, this concerns the ability of states to determine what content is allowed and how it can be filtered. The US believe that it harms interoperability and accessibility of information in the cyberspace. Yet, de facto national sovereignty over cyber-infrastructure is recognized. If the notion of sovereignty is defined for the information space, a state can use all available legal mechanisms within its jurisdiction to work with proxy servers located in its information space to identify the true source of the attack. Otherwise, the state has no right to take actions against the source of the attack on the basis of its lack of sovereignty in the information space. If we allow the submission of claims against a state "for" proxy servers located in its information space, the state shall have the right to use its administrative law in this space, i.e. possess sovereignty in its segment of the Internet.

The essence of the definition of network sovereignty consists in avoiding intervention into "networks" of other

CSRC commentary

The term “network sovereignty” is not defined elsewhere and requires clarification. It is particularly confusing because the first text quoted from the draft Convention refers to “information space” being “in the public domain”, which appears to contradict the notion of it being the object of sovereignty. In any case, there can be no such thing as absolute sovereignty in the context of an international network, because then it is not an international network. This is because being part of an international network entails obligations and responsibilities, and the observance of other nations’ legitimate interests within your own cyberspace; for example, to ensure the unimpeded flow of information and communications between states.

The first section of paragraph 5 refers to “information infrastructure”, which suggests that there is a difference between this and the “information space” referred to elsewhere – yet in other Articles the two concepts appear to overlap. (See detailed discussion of “information space” in Appendix A.) The final sentence echoes the provisions of the

countries. Perhaps we should focus on the subject of such "intervention in the information space", i.e. actions in the information space aimed at undermining the political, economic and social system of another state, imposing psychological influence on the population, or destabilizing society.

Council of Europe Convention on Cybercrime (Budapest Convention), and could therefore be considered redundant.

It is not immediately clear what value paragraph 8 adds, since the text holds little specific meaning. Further explanation of what this implies would be welcome.

Overall, the paragraphs cited here repeat in several sentences the same idea that existing laws apply in cyberspace as in any other domain. It would be easier to say just once that the principles established in the UN Charter and which govern the use of force, International Humanitarian Law, and Human Rights Law apply also in cyberspace. As seen elsewhere in this commentary, the Budapest Convention could be added here as a useful legal instrument for international cooperation on cybercrime investigation, and as a document providing for harmonisation of domestic legislation – both of which are aspirations expressed elsewhere in the draft.

As exemplified here, it is noteworthy that the draft Convention borrows language from different international treaties and legal principles, but does not always loyally reflect existing language. This is unhelpful as it could confuse the law as it stands and could not provide any useful guide for States, who would not know the scope of their new obligations and how they fit in with, or replicate, existing obligations.

7. Right to self-defense

Draft Convention reference:
Article 5. The basic principles of the international information security
The information space is in the public domain. Its security makes the foundations for the sustainable development of the global civilization.
In order to create and maintain the atmosphere of trust within the information space, the member states must adhere to the following principles:
11) each member state shall have the inalienable right to self-defense in the information space against aggression aimed thereat, provided that the aggressor has been identified beyond all doubt and the retaliatory measures are adequate;

IISI commentary

The position of Russia regarding the right to self-defense can be argumented by the fourth (potential) rule for NATO - "the Territoriality Rule"[10].

Everyone has the right to self-defence in face of obvious and imminent danger.

The concept of self-defence is part of both criminal and international law.

In principle, everyone has the right to self-defence, subject to the proportionality and necessity of such action.

In criminal law, if victim reasonably believes that unlawful force is about to be used against him, there is no liability for what would otherwise be wrongful acts in self-defence. This is not say that every cyber 'hack-back' can be justified under the concept; it should be a remedy of last resort.

On the international level, the criteria for invoking individual and collective self-defence are based on custom, the UN charter and international case law.

A cyber attack invokes individual and collective self-defense if it rises to the threshold of an 'armed attack'. The assessment of whether a cyber attack is, by its effects, consequences or nature, equivalent to such an attack will be made by national authorities or, for collective action, by international partners (the North Atlantic Council invoking Article V of the NATO Treaty, for example).

So far no cyber attack has crossed this threshold and no military response has yet been made to a cyber attack. A kinetic response in self-defence against a cyber attack can be legal if it is necessary to reach the goal (e.g. put an end to the attack) and the response is proportionate to the method and impact of the attack.

...

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations

CSRC commentary

Here again it would be more useful to apply the rules already established which govern the use of force, including Articles 2(4) and 51 of the UN Charter. Work exploring how existing legislation can be applied to cyberspace has already been carried out, as in for example the 'Ten Rules for Cyber Security' produced by the NATO Cooperative Cyber Defence Centre of Excellence, which explain how interpretation of existing law can avoid the necessity for new regulation.

The text of paragraph 11 as translated for published versions of the draft Convention is sufficiently different (and closer to the Russian version) to be worth quoting in full for comparison: "each State Party has the inalienable right to self-defense against aggressive actions against it in the information space, if the source of aggression can be reliably located and the retaliatory measures are appropriate".

This introduces the concept of "aggressive actions", also described as "aggressive 'information warfare'" in paragraph 9 previously: "the States Parties acknowledge that aggressive 'information warfare' is a crime against international peace and security". The insertion of the word "aggressive" needs further explanation. Is it suggested that there is a form of information warfare which is not considered aggressive, and therefore not a crime? If so, what is it?

In addition, it is unclear whether the "retaliatory measures" referred to would be restricted to cyber domain or the "information space" – greater precision is necessary in order to understand the potential consequences of this provision.

As there is a major issue of identifying the aggressor in cyberspace beyond all doubt – it is possible, but difficult - this argument could be turned into a positive argument of

[10] Tikk, E. Ten Rules for Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence, Estonia, 2011.

[...].
Article 51 of the UN Charter
The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked […].
Article 5 of the North Atlantic Treaty

what states could undertake to diminish the risk of miscalculation, misperception and uncertainty in case of cyber conflicts. Another important question is what constitutes aggression in cyber terms. There is no agreed definition of aggression in cyberspace, any more than there is of armed attack, and thus it will be difficult to predict how states are going to use cyber tools that are equivalent to conventional weapons. See also Appendix B, "Confidence and Security Building Measures".

In the UNGGE report on cyber security in 2010 referenced above, all participating countries agreed to the right for self-defence in cyberspace. In fact the general right to self-defence is established and defined in Article 51 of the UN Charter, and it ought not, therefore, to be necessary to reestablish it here. What is necessary is for aggression in cyberspace to be described, and for it therefore to be possible to compare or measure this aggression against the "armed attack" stipulated in Article 51.

For the issue of placing defined terms within quotation marks, see Appendix A.

8. All states are equal subjects of the information space

Draft Convention reference:
Within the information space all member states enjoy a sovereign equality, have the same rights and obligations and are the equal subjects of the information space regardless of economic, social, political, or other differences.

IISI commentary
For example, the US recognize in their International Strategy for Cyberspace that the benefits of ICTs should not be reserved to a privileged few nations, or a privileged few within them.

CSRC commentary
The rights and obligations of states may differ based on several factors such as the condition of their information society or information infrastructure. As there is no globally acknowledged common information space due to regimes covering inter alia protection of intellectual property and personal data, this principle remains distant from current reality.

9. Non-intervention in the cyberspace of other nations

Draft Convention reference:
The purpose of this Convention is to oppose the use of information and communications technologies to disturb international peace and security and also to introduce special measures in order that activities of nations in the information space are aligned with the generally recognized principles and norms of international law, including the principles of peaceful settlement of disputes and conflicts, the non-use of force, the nonintervention in the internal affairs of other nations, the respect for human rights and fundamental freedoms.
In order to create and maintain the atmosphere of trust within the information space, the member states must adhere to the following principles… the nonintervention in the internal affairs of other nations, the respect for national sovereignty…
…states shall refrain from any actions aimed at a complete or partial breach of the integrity of the information space of another State.
... states shall refrain from using information and communication technology to interfere with the internal affairs of another State.
... states shall refrain, in international relations, from threatening to use or using force against the information space of any other State with the purpose of breaching it or as a means of resolving conflict.
... states shall refrain from organizing or encouraging the organization of any irregular forces with the purpose of carrying out unlawful activities in the information space of another State.

IISI commentary

The position of Russia regarding the sovereignty of a state over the information infrastructure located on the state's territory can be "over-argumented" by the first (potential) rule for NATO - "the Territoriality Rule"[11].

Information infrastructure located within a state's territory is subject to that state's territorial sovereignty.
In view of the global nature of cyber threats, there is on-going debate over whether territoriality-based legal frameworks can cope, but the lessons of Estonia, Georgia and other major cyber incidents show that nations can and must make better practical use of the legal remedies and concepts available under national law by fine-tuning their national regulations.
The territoriality principle empowers nations to impose their sovereignty on information infrastructure located within their territory or otherwise subject to their

CSRC commentary

The text cited above, from Article 1 of the draft Convention, contains phrases which would require substantial elucidation (for example, "to disturb international peace and security"). In fact this version of the text, which matches printed copies of the draft Convention distributed by IISI, differs substantially and materially from the version made available by the Russian Ministry of Foreign Affairs (as per the citation above from the website of the Embassy of the Russian Federation in London). This poses obvious difficulties in assessing the draft Convention for non-Russian speakers who are unable to access the original text, and it is therefore suggested that translations of any possible future versions of the draft are coordinated and harmonised before being distributed.

The text calls for "special measures" to ensure that activities of nations are in accordance with international law, but does not specify why these are needed,

[11] Tikk, E. Ten Rules for Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence, Estonia, 2011.

jurisdiction. Through effective updating of the national law, strategy and politics regarding cyber security the nations expand the cyber security paradigm to include cyber-incidents that threaten national security.

In addition, implementation on the national level is required for entering into effect of most international norms. Electronic communications, criminal sanctions, investigative authority, cooperation with ISPs and many other essential elements of successful cyber defense depend on the quality of the national law.

Until the options for implementation and interpretation of national legal instruments are exhausted, it is difficult to determine what, if any, remedies need to be agreed upon on the international level, given the modern cyber threats.

The territoriality principle motivates the states to use all possible advantages of their legal framework. The responsibility of a state for securing its own networks is supported by the internationally recognized concepts of non intervention and sovereignty. Every government can exercise effective control over the IT infrastructure located on its territory, for example by ensuring the availability and quality of logs, maintaining an overview of the providers of electronic communications, developing an understanding of threats and capabilities existing within its jurisdiction to cope with and manage incidents, and balancing the development of the information society with the interests of national security.

since states are already subject to international legal obligations which cover many of the areas of activity illustrated in the cited paragraphs. The principle of non-intervention, specifically, is reflected in both Article 2(7) and 2(4) of the UN Charter; and the International Court of Justice in the case of Nicaragua confirmed that aspects of 1970 UN General Assembly Friendly Relations declaration (enshrining and elaborating on the content of the principle) were customary international law.[12] It is thus unclear what value would be added by the draft Convention in this field.

The concept of “breach” in “information space” needs to be defined as it does not have a meaning in English (see Appendix A for more on this). Also, “use of force against information space” requires clarification, since it is not possible to use force against space – against countries, individuals, or infrastructure, yes, but not against space.

With the last paragraph cited, difficulty lies with implementation and enforcement. The absence of encouragement for irregular forces would be impossible to verify, and “unlawful activities” is a meaningless phrase as long as it is unclear under which jurisdiction the activities are unlawful – that of the perpetrators or that of the victims. Since the principle is a broad one, this stipulation perhaps belongs in another, more general and more enforceable, document rather than one dealing with information security.

The “territoriality rule” included in the proposed “Ten Rules for Cyber Security” cited above is pertinent here. Under this rule, the notion of territoriality has been proposed as a factor enabling nations to exercise control over the information infrastructure subject to their jurisdiction in order to avoid harm to other countries. The right to exercise such control would not be absolute in cases where other nations’ cyber security concerns are involved.

[12] http://www.un-documents.net/a25r2625.htm

Thus, although the “Ten Rules” introduce sovereignty as an element supporting such control, it does not, per se, conclude that this right is or ought to be unrestricted. Therefore the concepts of territoriality, sovereignty and non-intervention cannot be used interchangeably.

10. Limitation of rights and freedoms only in the interests of security

Draft Convention reference:
The list of actions, which allow limitation of rights and freedoms only in the interests of security is given in Chapter 4, “Main Measures For Counteracting Illegal Activity In The Information Space”.

IISI commentary
The US do not recognize existence of "national Internets” and do not consider measures for breaking their censorship barriers as an intervention into their internal affairs. Internet access in the US is included in the set of universal human rights that cannot be limited under any circumstances.

At the same time the International Strategy for Cyberspace states that the US “recognize that exceptions to free speech in cyberspace must be narrowly tailored”. Thus, they do recognize that there can be exceptions.

The draft US Stop Online Piracy Act (SOPA) clearly states that the virtual space will fall under definite jurisdiction of one particular state. The specifics of the procedure that can be imposed by the SOPA consists in the ability to block not only the sites that are hosted on servers located on the US territory, but any resources to which the citizens of the country have access. And that is 99% of the Internet.

CSRC commentary
Clarification is needed as to whether paragraphs 3-6 of Article 11, relating to investigative measures, have territorial or sovereignty limitations. Paragraphs 5 and 6 include the phrase “in its territory”, which is absent from paragraphs 3 and 4, implying that the activities described there can be extra-territorial. This is significant when considering the applicability of the Budapest Convention (see elsewhere in this commentary for discussion of other provisions in the draft which mirror the already existing Budapest Convention).

The widespread opposition to the USA’s proposed Stop Online Piracy Act (SOPA), including as officially voiced by the European Parliament and Commission,[13] clearly illustrates the difficulties entailed in attempting to legislate against internet content held internationally using law which is specific to one country (the USA). The same difficulty would apply to any nation seeking to dictate what is and is not acceptable for another nation to hold in its “information space”.

Use of the word “illegal” is problematic without a clear explanation of which jurisdiction or legislation is to determine legality.

[13] J Baker, "European Parliament Joins Criticism of SOPA". PC World, 18 November 2011
G. Steinhauser, "EU Internet czar tweets against SOPA". The Sacramento Bee, 20 January 2012

Information exchange on threats and early warning are good practices that should be used in cyber security globally (see Appendix B).

11. Cooperation in order to locate the source of computer attacks, to repel these attacks and to eliminate their consequences

Draft Convention reference:
... states shall take all necessary steps to prevent any destructive information action originating from their own territory or using the information infrastructure under their jurisdiction, as well as cooperate to locate the source of computer attacks carried out with the use of their territory, to repel these attacks and to eliminate their consequences ...
The States Parties shall, on the basis of voluntariness and reciprocity, exchange best practices on the prevention, legal investigation, and the liquidation of consequences of crimes, including those related to terrorism, involving the information space.

IISI commentary
INTERFAX.RU, 10 December 2011 – Russia and the US plan to establish regular exchange of data on cyber-threats that can come "from computers" located on the territories of both states, said Caitlin Hayden, US National Security Council spokeswoman. "This will include “regular exchanges on technical threats that appear to emanate from one another's territory as well as no-fail communications mechanisms to help prevent crisis escalation and build confidence”, she said.

CSRC commentary
Despite the difficulty posed by the phrase “destructive information action”, which requires definition, the cited paragraphs contain the basis of potentially beneficial CSBMs (see Appendix B).

12. Taking necessary steps to prevent any destructive information action originating from the territory under jurisdiction of the state

Draft Convention reference:
... states shall take all necessary steps to prevent any destructive information action originating from their own territory or using the information infrastructure under their jurisdiction.

IISI commentary
According to the directives signed by Barack Obama (June 22, 2011), the Pentagon is forbidden to conduct cyber-attacks from the territory of other states without their prior consent. At the same time, these same directives allow the US to conduct cyber attacks and cyber espionage against other countries. These

CSRC commentary
This provision envisages states ensuring that information infrastructure within their own jurisdiction is not used for “hostile” activity – cooperation in order to identify the source of such activity is also described above. Consideration of the practical implications of a stipulation of this kind, and the obligations it entails, leads

directives of the White House, for example, allow the military to send computer codes to other countries to test interoperability between the their networks. The digital code will be passive and will not contain viruses or "worms" that can cause damage. But if the US enter into a military conflict with such other country, then this code will help to pave the way for future cyber attacks, which would be authorized by the President in person.

quickly to the realisation of an enormous legislative and administrative burden on states which might wish to subscribe to the draft Convention. Not only must they supervise the legality of content within their own jurisdiction, but also ensure that it is considered inoffensive and non-hostile in the jurisdictions of all other signatories – otherwise, they can immediately be accused of permitting hostile activity in breach of the Convention. The multiplicity of mutual obligations for content checking would be unmanageable.

Again, the phrase “destructive information action” requires definition or clarification as it does not carry meaning in English.

13. Refrain from using information and communication technologies to intervene in internal affairs of other states

Draft Convention reference:
... states shall refrain from developing and adopting plans or doctrines capable of increasing threats in the information space, straining relations between States or provoking “information wars”.

IISI commentary
Today the political reality demonstrates a lot of facts that could be described as attempts to use ICTs to achieve political goals. We observe "forced" violation of the operation stability of separate fragments in the global information infrastructure, or manipulation of content distributed through it.

The application of fundamental rights and freedoms in cyberspace is not absolute, it is limited by the interests of ensuring internal order and public safety, and non-interference in enjoyment of other fundamental human rights. Such limitations are clearly stated in the International Covenant on Civil and Political Rights and other fundamental treaties on human rights. Actions, sometimes quite severe, of the authorities of the United States and a number of other

CSRC commentary
This principle is sufficiently close in wording to Principle number 9 that it is unclear why they have been separated into two different sections.

The reference to use of ICT for intervention in the internal affairs of other states may be linked at the time of writing to the idea that political change in North Africa in 2011, and the campaign of protest against election results in Russia in 2011-2012, were both caused or at the very least facilitated by information operations carried out by the USA.[14] Since most people outside Russia will not be aware that this view exists, it may be worth providing more detail on what kind of “intervention” the drafters have in mind.

For problems with putting defined terms in quotation marks, see Appendix A.

[14] Among many other references, see President Medvedev speaking at a meeting of Russia’s National Anti-Terrorist Committee (NAK) in February 2011. http://www.kremlin.ru/transcripts/10408

Western countries with regard to protests show that at home they do not forget about the limits of democratic freedoms. And double standards here are pretty evident.

14. Non-proliferation of information weapons and the technology for their creation

Draft Convention reference:
.. states shall take action aimed at limiting the proliferation of "information weapons" and the technology for their creation.
... states shall refrain from using information and communication technology to interfere with the internal affairs of another State.

IISI commentary

One of the arguments supporting the position of Russia[15]: "The UK is developing a cyber-weapons programme that will help to counter growing threats to national security from potential attackers on the Internet and in the virtual space…[16] The armed forces minister, Nick Harvey, told the Guardian that "action in cyberspace will form part of the future battlefield" and though he said cyber-weapons would not replace traditional weapons, he admitted he now regards them as "an integral part of the country's armoury". The Guardian notes, that it is the first official acknowledgment that such a programme exists in the UK, which tacitly implies creation of computer viruses and other malicious software. In response to the question regarding when such weapons would be used and who would sanction it, N. Harvey said they would be governed by the same rules that apply to the deployment of other military assets such as special forces. According to the Guardian, though the nature of the weapons being developed remains top secret, it is understood that the Cabinet Office and the Cyber Security Operations Centre at GCHQ have taken the lead on the issue, and recently the Ministry of Defence has joined in the creation of new "weapons".

CSRC commentary

"Information weapons", according to the draft definition, are "designed for the purposes of information warfare". The definition for "information warfare", in turn, depends on the concept of "information space" and "meticide". For detail on difficulties with both of these, see Appendix A.

However the definition is interpreted, it is unclear how the "technology for the creation" of "information weapons" can be distinguished from technology for creation of any other computer program, internet process, or even media output.

As elsewhere, the draft states an aspiration which is unfortunately unverifiable and unenforceable.

[15] However, this concerns creation of cyber weapons rather than their proliferation.
[16] Guardian, 31 May 2011.

15. Refrain from organizing or encouraging the organization of any irregular forces with the purpose of carrying out activities in the information space of another State

Draft Convention reference:
Article 6. Main Measures for Averting Military Conflict in the Information space
Guided by the principles laid out in Article 5, the States Parties shall take steps to anticipate and expose potential conflicts in the information space and take joint action to avert them and resolve crises and disputes peacefully.
To this end, the States Parties shall:
2) take all necessary steps to prevent any destructive information action originating from their own territory or using the information infrastructure under their jurisdiction, as well as cooperate to locate the source of computer attacks carried out with the use of their territory, to repel these attacks and to eliminate their consequences;
3) refrain from developing and adopting plans or doctrines capable of increasing threats in the information space, straining relations between States or provoking "information wars";
4) refrain from any actions aimed at a complete or partial breach of the integrity of the information space of another State;
5) refrain from using information and communication technology to interfere with the internal affairs of another State;
6) refrain, in international relations, from threatening to use or using force against the information space of any other State with the purpose of breaching it or as a means of resolving conflict;
7) refrain from organizing or encouraging the organization of any irregular forces with the purpose of carrying out unlawful activities in the information space of another State;

IISI commentary
According to the UN General Assembly resolution on "Definition of Aggression" adopted in 1974, the sending (i.e. "use") of irregulars or mercenaries, which carry out acts of armed force against another state qualifies an international delinquency.

It shall be recognized that the states are unlikely to abandon the concealed use of irregular forces in the information space, i.e. the actions themselves are illegal, but the irregular forces are controlled by the government bodies.

CSRC commentary
For the difficulty of enforcing the "irregular forces" principle, see the commentary on principle 9 above.

The content of the references cited could be summarised as saying that the UN Charter also applies in cyberspace.

16. Refrain from threatening to use or using force in the information space

Draft Convention reference:
Article 6. Main Measures for Averting Military Conflict in the Information space
Guided by the principles laid out in Article 5, the States Parties shall take steps to anticipate and expose potential conflicts in the information space and take joint action to avert them and resolve crises and disputes peacefully.
To this end, the States Parties shall:

refrain, in international relations, from threatening to use or using force against the information space of any other State with the purpose of breaching it or as a means of resolving conflict;
refrain from organizing or encouraging the organization of any irregular forces with the purpose of carrying out unlawful activities in the information space of another State;

IISI commentary
There is no direct criticism of this part of the Convention.

The US criticism aimed at decreasing the significance of the threat of cyber-space using by states for military and political goals turns out to be irrelevant as the United States themselves actively create cyber-troops, increase their presence in cyber-space, and, furthermore, consider cyber-space as another area of confrontation. Meanwhile, the concept of collective defense the cyber-space is actively promoted at the level of NATO allies, along with the idea of applying Article V of the North Atlantic Treaty in case of attacks in cyber-space. Given the possibility of reaction in cyberspace, the clause on the refrain from using force in the draft Convention seems justified.

CSRC commentary
An understanding of what force in information space can be depends on a clearer definition of “information space”. For difficulties with this definition, as with the concept of “breaches”, see Appendix A. See above for discussion of “irregular forces”.

At the same time, international legal obligations already clearly state when the use of force is forbidden, and this, therefore, does not need to be re-established or redefined. As stated in Article 2(4) of the UN Charter, for example, “All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”

17. Working-out uniform approaches to disabling Internet resources of a terrorist nature

Draft Convention reference:
Article 8. The Use of the Information space for Terrorist Purposes
The States Parties acknowledge the possibility of the information space being used for carrying out terrorist activities.
Article 9. Main Measures for Preventing the Use of the Information space for Terrorist Purposes
To prevent the use of the information space for terrorist purposes, the States Parties shall:
1) take action to prevent the use of the information space for terrorist purposes and acknowledge the necessity of decisive joint efforts to this end;
2) strive to work out uniform approaches to disabling Internet resources of a terrorist nature;
3) acknowledge the need for establishing and expanding the exchange of information on possible computer attacks, on the signs, facts, methods, and means of using the Internet for terrorist purposes, and on the goals and activities of terrorist organizations in the information space, as well as the need for the exchange of experience and best practices on monitoring Internet resources, finding and monitoring the content of websites of a terrorist nature, carrying out criminal investigations by computer experts in this sphere, and legal regulation

and the organization of activities for preventing the use of the information space for terrorist purposes;
4) take such steps of legislative or other nature as may be necessary to allow law enforcement authorities to carry out investigative and other relevant activities aimed at preventing and suppressing terrorist activities in the information space and at the elimination of the consequences thereof, as well as at punishing persons and organizations guilty of conducting them;
5) take necessary steps of legislative or other nature which will guarantee lawful access to specific parts of the information and communication infrastructure in the territory of the State Party, which are legally implicated in being employed for the perpetration of terrorist activities in the information space or involved in such activities elsewhere, for the perpetration of activities conducive to terrorist acts, or for the activities of terrorist organizations or groups, or individual terrorists.

IISI commentary

Given the scale of possible consequences of actions of Internet resources (and terrorist activities in the information space) the adoption of this provision is essential. This raises the question of developing approaches to monitoring and filtering the content of the corresponding Internet resource (for searching and collecting evidence). Criteria shall be developed to classify an Internet resource as a resource of a terrorist nature.

CSRC commentary

The repeated references to terrorism throughout the draft give rise to severe problems of interpretation. Conceptual differences in the understanding of the nature of "terrorism" between Russia and other states provide an additional layer of complexity and indeterminacy to the already muddied picture of what constitutes "terrorism in the information space", or as it would be referred to elsewhere, cyberterrorism. As described by Anna-Maria Talihärm[17], Alex Michael[18] and others, "there is a great abundance of different definitions of the idea of 'terrorism'... the addition of the prefix "cyber" has only extended the list of possible definitions and explanations".

Thus without consensus with Russia on what precisely is covered by "perpetration of terrorist activities in information space", this clause remains unusable. Such consensus is unlikely to be achieved given the fundamental and unresolved differences between the two sides on what constitutes both terrorism and counter-terrorist activity.[19]

In the meantime, this formulation would permit governments to declare undesirable internet content "terrorist" or "extremist" at

[17] A.-M. Talihärm, "Cyberterrorism: in Theory or in Practice?," Defence Against Terrorism Review, Vol. 3, No. 2, pp. 59-74, 2010
[18] A. Michael, "Cyber Probing: The Politicisation of Virtual Attack," Defence Academy of the United Kingdom, Shrivenham, 2010
[19] A. Monaghan, "The Moscow metro bombings and terrorism in Russia," June 2010. [Online]. Available: http://www.ndc.nato.int/research/series.php?icode=1

will, and therefore subject to suppression by all other potential signatories to the draft Convention

18. Taking steps of legislative or other nature as may be necessary to carry out investigative and other relevant activities in the information space

Draft Convention reference:
Chapter 3. MAIN MEASURES FOR PREVENTING THE USE OF THE INFORMATION SPACE FOR TERRORIST PURPOSES
Article 9. Main Measures for Preventing the Use of the Information space for Terrorist Purposes
To prevent the use of the information space for terrorist purposes, the States Parties shall:
4) take such steps of legislative or other nature as may be necessary to allow law enforcement authorities to carry out investigative and other relevant activities aimed at preventing and suppressing terrorist activities in the information space and at the elimination of the consequences thereof, as well as at punishing persons and organizations guilty of conducting them;

IISI commentary
Given the scale of possible consequences (primarily, of terrorist activities in the global information space) the adoption of this provision is essential. The adoption of some of these measures is provided for in the Budapest Convention on Cybercrime (see Preamble and Section 2 - Procedural law). It should be noted that the Budapest Convention contains no rules regarding terrorist activities.

CSRC commentary
The Budapest Convention includes key rules for law enforcement cooperation in any investigation, be it into criminal activities, terrorist activities or even state-sponsored proxy activities in cyberspace. It is not necessary to add specific provisions for actions to be taken in a counter-terrorist situation when all-encompassing rules are already in place. It is hard to see how the draft Convention adds value in this area when a suitable instrument is already available for signature.

In the meantime, this formulation would permit governments to declare undesirable internet content “terrorist” at will, and therefore subject to suppression by all other potential signatories to the draft Convention.

An explanation would be useful of why current law enforcement agreements (e.g the Council of Europe instruments) are not considered sufficient to provide the desired standard of cooperation.

19. Take necessary steps of legislative or other nature which will guarantee lawful access (when justified) to specific parts of the information and communication infrastructure in the territory of the State Party

Draft Convention reference:

Chapter 3. MAIN MEASURES FOR PREVENTING THE USE OF THE INFORMATION SPACE FOR TERRORIST PURPOSES

Article 9. Main Measures for Preventing the Use of the Information space for Terrorist Purposes

To prevent the use of the information space for terrorist purposes, the States Parties shall:

take necessary steps of legislative or other nature which will guarantee lawful access to specific parts of the information and communication infrastructure in the territory of the State Party, which are legally implicated in being employed for the perpetration of terrorist activities in the information space or involved in such activities elsewhere, for the perpetration of activities conducive to terrorist acts, or for the activities of terrorist organizations or groups, or individual terrorists.

Chapter 4. MAIN MEASURES FOR COUNTERACTING ILLEGAL ACTIVITY IN THE INFORMATION SPACE

Article 11. Measures on Organizing Criminal Procedures

To organize criminal procedures, the States Parties shall:

take legislative or other steps which may be necessary to empower the law enforcement authorities of the State to search or gain similar access to information and communication systems and their parts and the data stored therein, as well as to storage media which may contain the data in question, in its territory, and to other data and information and communication systems of their information space which are reasonably implicated in storing the data in question;

IISI commentary

The need for the development and adoption of these measures is obvious. The adoption of some of such measures is provided for in the Budapest Convention on Cybercrime (see Chapter II – Measures to be taken at the national level). From the position of States which have ratified the Budapest Convention, trans-border access to stored computer data with consent or where publicly available *without consent of the other Party* is legitimate (Article 32 of the Convention).

CSRC Commentary

Besides the difficulty with the definition of terrorist activities as described above, a further query over Article 9 Paragraph 4 cited is that it does not appear to include any territorial limitation. This implies that one State could pursue investigations in the “information space” of another nation. Yet it is this principle which appears to be Russia’s main objection to the Budapest Convention, which aims to assist cross-border investigations. Does the presence or allegation of terrorism provide an exception to this Russian objection, making the stipulations of the Budapest Convention acceptable under these circumstances?

The subsequent Paragraph 5 reads: “take necessary steps of legislative or other nature which will guarantee lawful access to specific parts of the information and communication infrastructure in the territory of the State Party, which are

legally implicated in being employed for the perpetration of terrorist activities in the information space or involved in such activities elsewhere, for the perpetration of activities conducive to terrorist acts, or for the activities of terrorist organizations or groups, or individual terrorists". If the "lawful access" referred to provides access for one state to another state, then this appears to be a cross-border investigation as provided for by the Budapest Convention. As above, does "terrorism" provide a waiver to Russia's objections to this part of the Convention?

Use of the word "illegal" is problematic without a clear explanation of which jurisdiction or legislation is to determine legality.

20. Criminalization of the use of information resources and/or the manipulation of them in the information space for unlawful purposes

Draft Convention reference:
Chapter 4. MAIN MEASURES FOR COUNTERACTING ILLEGAL ACTIVITY IN THE INFORMATION SPACE
Article 10. Main Measures for Counteracting Illegal Activity in the Information space
To counteract illegal activity in the information space, the States Parties shall:
1) strive to criminalize the use of information resources and/or the manipulation of them in the information space for unlawful purposes, which include the unauthorized dissemination of information, breaches of confidentiality, and damaging the integrity or accessibility of information, and also take legislative or other steps to stipulate the responsibility and hold responsible persons for perpetrating, attempting, being accomplices in or instigating criminalized and socially dangerous actions in the information space;
2) take legislative or other steps to ensure that offenders in the information space receive effective, proportional, and convincing punishment.
Article 11. Measures on Organizing Criminal Procedures
To organize criminal procedures, the States Parties shall:
take legislative or other steps to stipulate powers and procedures for the purposes of conducting individual criminal investigations or court trials in cases of the perpetration of criminalized and socially dangerous actions in the information space;
take legislative or other steps to establish its jurisdiction over any criminalized and socially dangerous action in the information space perpetrated in the territory of the State, on board a vessel flying the flag of that State, and on board a plane or any other aircraft registered under the laws of that State.
If jurisdiction over an alleged offence is claimed by more than one State Party, the interested parties hold consultations to decide on the most suitable jurisdiction for prosecution.

IISI commentary

There is no principal criticism of this provision of the Convention. On the contrary, most countries believe that criminalization is needed, and that the law should keep pace with the development of computer crime. They also confirm the need for joint struggle against cybercrime and the need for harmonization of national legislations. However, not all states recognize the limitations of the draft Convention on Cybercrime, they stand for expansion of the circle of its participants. Other countries such as India acknowledge the need for continued criminalization of cybercrime.

CSRC Commentary

Use of the word "illegal" is problematic without a clear explanation of which jurisdiction or legislation is to determine legality.

The Budapest Convention already provides for harmonisation of legislation between signatories, which would include bringing into line those states where legislation for online activity is insufficiently developed as described here.

In order to justify the stated principle, a more thorough discussion of the limitations of the Budapest Convention would be useful, with critical assessment as to what would be needed in addition to or in comparison with the Budapest instrument. This would enable a clearer understanding of why it is considered insufficient or unsatisfactory.

Part II. Additional Comments by CSRC

This section discusses a number of specific issues arising from specific parts of the text of the draft Convention not covered in Part I above, presenting them in the order in which they appear in the text (as it is not a qualified legal opinion, it does not claim to be a comprehensive list of all potential issues). In many cases it is noted that additional information, explanation or definition would be necessary in order to understand the obligations which the draft Convention entails. Comment of this nature takes the form of open questions below. Citations from the text are presented boxed.

General Observations

- From the UK perspective, the presumption is that treaties and international agreements evolve from already established norms and principles, rather than being established from scratch in an attempt to prescribe behaviour, as the draft Convention appears to seek to do.

- In international security, there are long traditions of enhancing transparency and building confidence between states, which have been formulated as Confidence Building Measures. Development of CBMs in cyberspace would be the efficient international response to overcome perception issues between state actors. See Appendix B for examples of potential CBMs which have been extracted from the text of the draft Convention.

- A key distinction between the Russian and Western approaches to the issues

under discussion is that between the focus on “information security” and on “cyber security”. It has been suggested that information security is cyber security plus content control; but in any case a clear definition of information security is essential if the two concepts are usefully to be compared.

- It should not be necessary to reinvent the wheel in cyberspace and/or for information security: existing international law applies in this context as it does elsewhere, and the areas covered by the draft Convention do not constitute a legal exemption justifying special treatment. While the application of existing law and legal principles may require discussion, given that it is being applied in a novel sphere, CBMs and discussion of how existing principles apply in this new context will produce a clearer, more coherent and useful approach.

- A treaty between States is unsuitable as a means of regulating the domain of cyberspace, given the key role of non State actors- corporations, ISPs, civil society and so on.

- This draft Convention borrows language from different international treaties and legal principles, but does not always loyally reflect existing language. This is unhelpful as it could confuse the law as it stands and could not provide any useful guide for States, who would not know the scope of their obligations and how they overlap with or duplicate existing undertakings.

- As this is the case, it is questionable in which international forum the draft Convention should be presented for negotiation. There is no evident reason why the United Nations, for example, would wish to negotiate another treaty when its content duplicates that of already existing UN documents.

Commentary on Specific Articles

acknowledging the necessity of preventing possible uses of information and communication technology for purposes not compatible with ensuring international stability and security, and capable of having a negative effect on the integrity of governmental infrastructures, causing damage to their security,

It is hard to discern any concrete meaning in this paragraph. The abstract introductory phrase is followed by a concept which is at once extremely broad and extremely vague. It would be preferable to rephrase this to convey a specific meaning.

3) correspond to generally accepted principles and norms of international law, including principles of peacefully regulating conflicts and disagreements, abstaining from the use of force, not interfering in internal issues, and respecting fundamental human rights and freedoms;

It is unclear how the principle of non-interference in internal issues can be defined in a medium like the internet, which crosses borders effortlessly and at random. It would also need to be specified where precisely it is decided what constitutes “interference”.

4) be compatible with the right of each individual to seek, receive, and distribute information and ideas, as is affirmed in UN documents,

This appears to be a reference to Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. The first part of the text is correct: “right to seek, receive and impart”. It is the second part on restrictions that has not been reproduced correctly, and it does not refer to the need for the restrictions to be necessary and proportionate, as well as legal.

5) guarantee the free exchange of technology and information, while maintaining respect for the sovereignty of States and their existing political, historical, and cultural specificities.

This indirect reference to the establishment of sovereignty in cyberspace overlooks the fact that nations have already subscribed to specific legal obligations and norms which override and trump national laws (which usually are the embodiment of the “political, historical and cultural specificities” referred to).

“**threat to the information space (threat to information security)**” - factors that pose a danger to individuals, society, and the state, and their interests, in the information space.

It is not clear why these two titles are listed together. The definitions of information space and information security are different, so is it correct to conflate the two into a single definition for the threat to them?

Article 3.
This Convention will not apply in those cases when the actions in question are taken within the information infrastructure of one State, citizen, or corporation under the jurisdiction of that State, and the effects of those actions are only felt by citizens and corporations under the jurisdiction of that State, and no other State has grounds to assert its jurisdiction.

It would appear that this could only apply to a small proportion of activity or data exchange taking place on the internet – since so much crosses international borders, even if the originator and target are within one country. The conditions listed above are extremely restrictive, even if there is no intention for information to cross between notional jurisdictions.

Article 4.
6) the dissemination of information across national borders, in a manner counter to the principles and norms of international law, as well as the national legislation of the government involved;

Once again, there is a tacit assumption in this paragraph that (a) flows of information respect national borders, and that (b) there is any real control over via which routes data may flow. Since neither of these is the case, this paragraph appears unworkable.

Additional factors increasing the danger of the aforementioned threats are:….

It would be useful to find out why these four points are separated out from the preceding 11. Is it that these are considered “technical” challenges while the others are more “political”?

Article 5.

1) the activities of each State Party in the information space must promote social and economic development and must be consistent with the goals of maintaining world peace and security, and conform to the universally recognized principles and norms of international law, including the principles of peaceful reconciliation of strife and conflict, of the non-use of force in international relations, of non-interference into the internal affairs of other States, and of respect for the sovereignty of States and the major human rights and freedoms;

A subtlety of translation in this paragraph carries the potential for misunderstanding by inserting a reference to “major human rights”. Human rights are human rights, and are not separated into major and minor. In fact the Russian version reads “основных прав и свобод человека”, which is rendered more clearly in other translated versions as “fundamental human freedoms and rights”.

Elsewhere, a similar phrase has been translated as “basic human rights”. There is no hierarchy of human rights and freedoms, so an apparent reference to “basic” rights will be problematic.

In any case, the principle of respect human rights and freedoms is universal and trumps any calls for non-interference in the internal affairs of other states.

6) each State Party must observe the principle of responsibility for its own information space, including responsibility for its security and the nature of information it holds;

It would be useful to know more on where this “principle of responsibility” is established and what precisely it entails. Would it, for example, make any nation liable for any e-crimes or hacktivism that originated from its territory?

10) the information space of States Parties should not be the object of acquisition for other States as a result of threats of force or the use of force;

Does this imply that a state should have a monopoly over whatever it deems to be its “information space”? Further explanation (or indeed an example of a scenario) would be useful to illustrate what is actually meant here.

12) each State Party will determine its military potential in the information space on the basis of national procedures, with consideration for the lawful interests in security of other States, as well as the necessity of working to strengthen international peace and security. No State Party will make an attempt to achieve dominance in the information space over other States;

Even if the provisions elsewhere in this drafts for advanced states to share their technologies were enforced, it seems implausible that all nations will ever be at an identical level of technological development. In this case, how will “not making an attempt to achieve dominance” be measured and enforced? This seems to be another example of a stipulation put in place by the draft with no prospect of it being actionable.

13) a State Party may locate its forces and means of ensuring information security on the territory of another State in accordance with an agreement, developed by both parties on a voluntary basis through negotiations, and in accordance with international law;

The text of this paragraph is reminiscent of the "Conceptual Views" on the information space published by the Russian Ministry of Defence, which also provide for deployment of information security forces on the territory of other states. But in the context of information or cyber security this could imply having offensive-capable IT capacity located in another nation state. Who then has responsibility for actions conducted by that capability? Is the host nation obliged to take action to stop any improper activities by the "guest" capabilities? This provision seems at odds with other stipulations of the draft requiring nations to take responsibility for activity and content in their own jurisdiction.

14) each State Party will take the measures necessary to ensure that the activity of international information systems for the management of the flow of transport and finance, means of communication, means of international information exchange, including the exchange of information for scientific and educational purposes, continues without interference, based on the understanding that such interference could negatively affect the information space as a whole;

This appears to be a very specific list of information systems. Is there a reason why these specific systems have been chosen, and what has been excluded as a result – to take just one example, healthcare information systems? Also, given the unavoidable interconnectedness of these and other systems, how is a distinction to be drawn between these systems which are to continue without interference, and other systems with no such protection?

19) States Parties do not have the right to limit or interrupt the access of citizens to the information space, except when acting to protect national and social security, or when preventing the illegal use of an unsanctioned interference into their national information infrastructure;

For the problem of "social security", see Appendix A. In addition, the exception stipulated here appears dangerously wide-ranging in scope. Greater precision is clearly essential.

20) States Parties stimulate the partnership between business and civil society in the information space;

This paragraph seems out of place and out of context, and provides no explanation as to why it has been included – apart from making some recognition of the multi-stakeholder approach accepted elsewhere in the world.

9) have the right and duty to take action against the proliferation of untruthful or distorted messages which could be considered as a means of interfering in the internal affairs of other States or as damaging world peace and security;

It is unclear how and where this provision could or should be interpreted. It is a state's obligation to uphold freedom of expression - even if there is doubt about the veracity of some information. Slander and libel laws already exist to counter gross distortions, so in this respect it is unclear what this paragraph adds.

Article 7. Measures for Resolving Military Conflict in the Information Space

Article 6 focuses on averting conflict in the information space, and Article 7 looks at resolving conflict in the information space. Yet although the notion of "information war" is introduced, there is no mention of conduct during an information war, nor of defining when a state of information war exists or has been declared.

Article 9.

2) strive to work out uniform approaches to disabling Internet resources of a terrorist nature;

There are two key conceptual problems in this paragraph.

First, there cannot be "internet resources of a terrorist nature". Internet resources are neutral: it is how and by who they are used that matters. If the definition of "internet resources" used here is one that implies that these resources in and of themselves can possess intent or attitude, then that definition needs to be made explicit.

Second, as there is no universally agreed definition of terrorism, interpretation would be down to nation states. See Appendix A for further discussion of the problem of use of "terrorism" in the draft.

4) take such steps of legislative or other nature as may be necessary to allow law enforcement authorities to carry out investigative and other relevant activities aimed at preventing and suppressing terrorist activities in the information space and at the elimination of the consequences thereof, as well as at punishing persons and organizations guilty of conducting them;

Appendix A

Concepts, Definitions and Linguistic Considerations

This appendix lists a number of problematic terms and definitions used in the draft Convention and not discussed elsewhere in this commentary, which will give rise to confusion and/or convey a meaning different to what appears to be intended in the Russian-language original.

Security

> *affirming* the necessity for a common understanding of Internet security issues and further cooperation on the national and international level,

The term “internet security” does not appear to be repeated elsewhere. It would be helpful to know whether its inclusion is deliberate, and if so what precisely it is taken to mean (as opposed to “information security”, which is the subject of the draft).

Meanwhile the definition of “information security” itself is problematic:

> **Article 1. Subject and aim of the Convention**
> *The subject* that this Convention seeks to regulate is the activity of governments to ensure international information security.

This is the basis of this entire draft Convention, but the definition provided (see Article 2, Paragraph 6) rests on a definition of “destructive and negative actions” which is not spelt out – the phrase itself is so vague as either to be meaningless or all-encompassing.

> “**information security**” - a state in which personal interests, society, and the government are protected against the threat of destructive actions and other negative actions in the information space;

In addition the draft calls for information security in the “information space”, which as discussed below is a concept applied inconsistently throughout the text.

Information Space

The usage of the phrase “information space” appears at times to be at variance with the definition given in Article 2, Terms and Definitions:

> “**information space**” - the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself;

This initial definition calls the “space” a “sphere of activity”. Yet when the phrase is used later in the document, it appears to refer to infrastructure, as in:

> 3) the illegal use of the information resources of another government without the permission of that government, in the information space where those resources are located;

or as in:

> **Article 5**
> 5) each State Party has the right to make sovereign norms and govern its information space according to its national laws. Its sovereignty and laws apply to the information infrastructure located in the territory of the State Party or otherwise falling under its jurisdiction

It is thus not clear whether information space is a concept that captures also the content of information, or simply means ICT services. Whichever interpretation is used, it remains unclear how it is possible to describe or define an "information space" specific to one country, when by the very nature of the internet, information can be hosted anywhere in the world.

Further, references are made to a "breach" of the "information space", as in Article 6:

> 4) refrain from any actions aimed at a complete or partial breach of the integrity of the information space of another State;
> 6) refrain, in international relations, from threatening to use or using force against the information space of any other State with the purpose of breaching it or as a means of resolving conflict;

It is unclear what precisely a "breach" would be. This needs explanation.

Terrorism

The definition of "terrorism in the information space" provided in Article 2 is unusable without a definition of terrorism itself:

> "**terrorism in the information space**" - the use of information resources and/or activity affecting them in the information space for the purposes of terrorism;

This renders the many significant references to terrorism in the text of the draft (including as a "main threat to international peace and security") also unusable; as for example in:

> 5) the use of the international information space by governmental and non-governmental structures, organizations, groups, and individuals for terrorist, extremist, or other criminal purposes;

International agreement on what constitutes a terrorist or extremist purpose is demonstrably far from achieved. In the meantime, as noted above, this formulation would permit governments to declare undesirable internet content "extremist" at will, and therefore subject to suppression by all other potential signatories to the draft Convention.

Social Security

The Russian phrase общественная безопасность has in places been translated in this version as "social security" – the English phrase which conveys the intended meaning is

"public safety". "Social security" tends to refer instead to welfare and benefits provided by the state.

Cybersecurity

There is one mention of the term "cybersecurity" in the draft. It is not listed in the definitions, and is not a term used elsewhere in Russian official documentation. It would be interesting to know if its inclusion is deliberate, and if so what precisely it is taken to mean.

> **Article 5**
> 15) States Parties should support and stimulate scientific and technical developments connected with the exploration of the information space, as well as educational activity, aimed at forming a global culture of cybersecurity;

Socially dangerous actions

This phrase provides an interpretative minefield, and surely can be made more precise:

> **Article 11**
> 1) take legislative or other steps to stipulate powers and procedures for the purposes of conducting individual criminal investigations or court trials in cases of the perpetration of criminalized and socially dangerous actions in the information space;

Linguistic Trivia

In more than one location in the English-language text, previously-defined terms have been placed in quotation marks, raising the question of whether that definition applies in that instance. If the use of the terms is as per the initial definition, the quotation marks should be simply removed in order to avoid doubt.

For example:

> **Article 6**
> 3) refrain from developing and adopting plans or doctrines capable of increasing threats in the information space, straining relations between States or provoking "information wars";
> 10) take action aimed at limiting the proliferation of "information weapons" and the technology for their creation.

and others.

References to "breeches" should be replaced with "breaches" throughout, as in English breeches are knee-length trousers.

> *convinced* that this Convention is necessary in the fight against breeches of the confidentiality, integrity, and accessibility of computer systems and networks and computer information, as well as the misuse of such systems, networks, and information by ensuring the punishment of such actions, detailed in this Convention, and in the granting of sufficient authority to effectively fight such offenses through the tracking, exposure, and investigation of such offenses on an internal and international level, and

through the development of agreements on efficient and reliable international cooperation,

Finally, the draft uses the term “meticide” in all translations seen to date (see citation below). It is likely that the intention was to use “menticide”, but this is not a widely recognised word in English: perhaps an alternative could be found. In any case “meticide” should be amended in the English-language versions since this refers to a form of pesticide.

Article 4.

4) activities in the information space with the object to undermine the political, economic, and social systems of another nation, a meticide destabilizing the public;

Appendix B

Scope for Confidence- and Security-Building Measures (CSBMs)

The draft Convention contains suggestions which could be usefully developed into initiatives to foster international security and trust in cyberspace, regardless of whether any state adopts the draft. But it would be essential to recognise that any such measures must, because of the nature of the subject, include non-state actors such as business and civil society as well as the state.

Article 5

21) States Parties acknowledge their responsibility to ensure that citizens, public and state bodies, other States, and the global community are informed about new threats to the information space and about known methods of increasing the level of their security.

This is an interesting proposal, and more information on how it could be implemented would be welcome.

Article 6

2) take all necessary steps to prevent any destructive information action originating from their own territory or using the information infrastructure under their jurisdiction, as well as cooperate to locate the source of computer attacks carried out with the use of their territory, to repel these attacks and to eliminate their consequences;

Cooperation to locate the source of attacks constitutes another potential CSBM, where more detail on possible mutually beneficial implementation would be welcome. An exchange of expertise in mitigating technical threats on a national or international level could only be of benefit.

Article 13. Confidence-Building Measures in the Sphere of the Military Use of the Information space

Each State Party must strive to promote confidence-building measures in the sphere of the military use of the information space, which include:

1) the exchange of national security concepts in the information space;

2) timely exchange of information on crises and threats in the information space and on the steps taken to deal with them;

3) consultations on activities in the information space which may raise concerns of States Parties and cooperation on resolving conflicts of military nature.

It is unclear why this provision is limited to military use. Surely all forms of CSBMs should be used to deescalate any tension when a nation experiences a cyber attack – since at the time of attack there is no way of knowing whether a nation's military has been involved or not.

At the same time, excellent state-to-state political-military CSBMs are already in place through the auspices of, for example, the OSCE. There is no reason why this should not be expanded into direct military-to-military contact to establish CSBMs – to take just one example, exchange of doctrines on use of force or on structures of cyber commands.

If the phrase “information space” were to be removed from sub-paragraph 1, then this would be achievable. At the same time, if “information space” is not removed from sub-paragraph 2, then this mechanism could very readily become overloaded as under the terms of this draft every complaint about unflattering media reports or other trivia could lead to a call for information exchange.

Sub-paragraph 3, unfortunately, is so vague as to be meaningless.

Published by
Conflict Studies Research Centre

and

Institute of Information Security Issues
Moscow State University