PIR LIBRARY

REPORT

GLOBAL INTERNET GOVERNANCE AND INTERNATIONAL SECURITY IN THE FIELD OF ICT USE

MOSCOW • GENEVA

2015

Note: The image on the cover shows the HAL 9000 artificial intelligence from the Stanley Kubrick film “2001: A Space Odyssey”.

Original illustration available at: Wikimedia, file “The famous red eye of HAL 9000”, distribution under free license Creative Commons Attribution 3.0 Unported.

Link to the original illustration:
https://commons.wikimedia.org/wiki/File:HAL9000.svg
(last accessed on April 30, 2015)

Oleg Demidov, Consultant at PIR Center, is the author of this Report. Previously, in 2012-2014 Oleg ran the PIR Center's Program "Global Internet Governance and International Information Security".

Oleg Demidov is also a member of the Research Advisory Committee under the Global Commission on Internet Governance (GCIG RAN). He has been involved in research collaboration with ICANN and Russian technical community. Oleg is a regular participant of global conferences and fora on the issues of cybersecurity and Internet governance, including ICANN Conferences, NETmundial summit, Internet Governance Forum, Global Conference on Cyber Space and other formats.

PIR Center is a partner organization of PIR Press and a leading Russian non-governmental think tank conducting research in the field of international security including the issues of WMD nonproliferation and disarmament, arms control and regional security.

In 2011, PIR Center launched the Program "Global Internet Governance and International Information Security". Within the framework of the Program, the PIR Center regularly organizes expert workshops, roundtables and trainings, publishes research papers and reports as well as the bimonthly e-journal *The CyberPulse*.

As the Program evolved, the PIR Center has established itself as a leading Russian nongovernmental think tank conducting research on ICTs in global security context. The PIR Center has been collaborating with technical actors in Russia and abroad, private companies, think tanks, universities, and with intergovernmental organizations including the UN bodies (UNIDIR, ITU, ECOSOC). In 2015, Alexandra Kulikova took over the Program with a mission to continue its further development and expansion.

The Report “Global Internet Governance and International Security in the Field of ICT Use” was prepared by the PIR Center’s Consultant Oleg Demidov with contribution from the Working Group on International Information Security and Global Internet Governance under the PIR Center’s Advisory Board. The PIR Center is a leading non-governmental think tank conducting research in the field of global security, and a partner organization of PIR Press.

The Report aims to identify the key challenges to international security in the field of the use of ICTs at global and national level, and to highlight the interests and goals of the international community including nation states and other relevant stakeholders in the field of Internet governance.

Target audience of the Report includes representatives of organizations engaged in discussions and policy making on the issues of information society, cybersecurity, Internet governance, critical infrastructure protection and cyber governance.

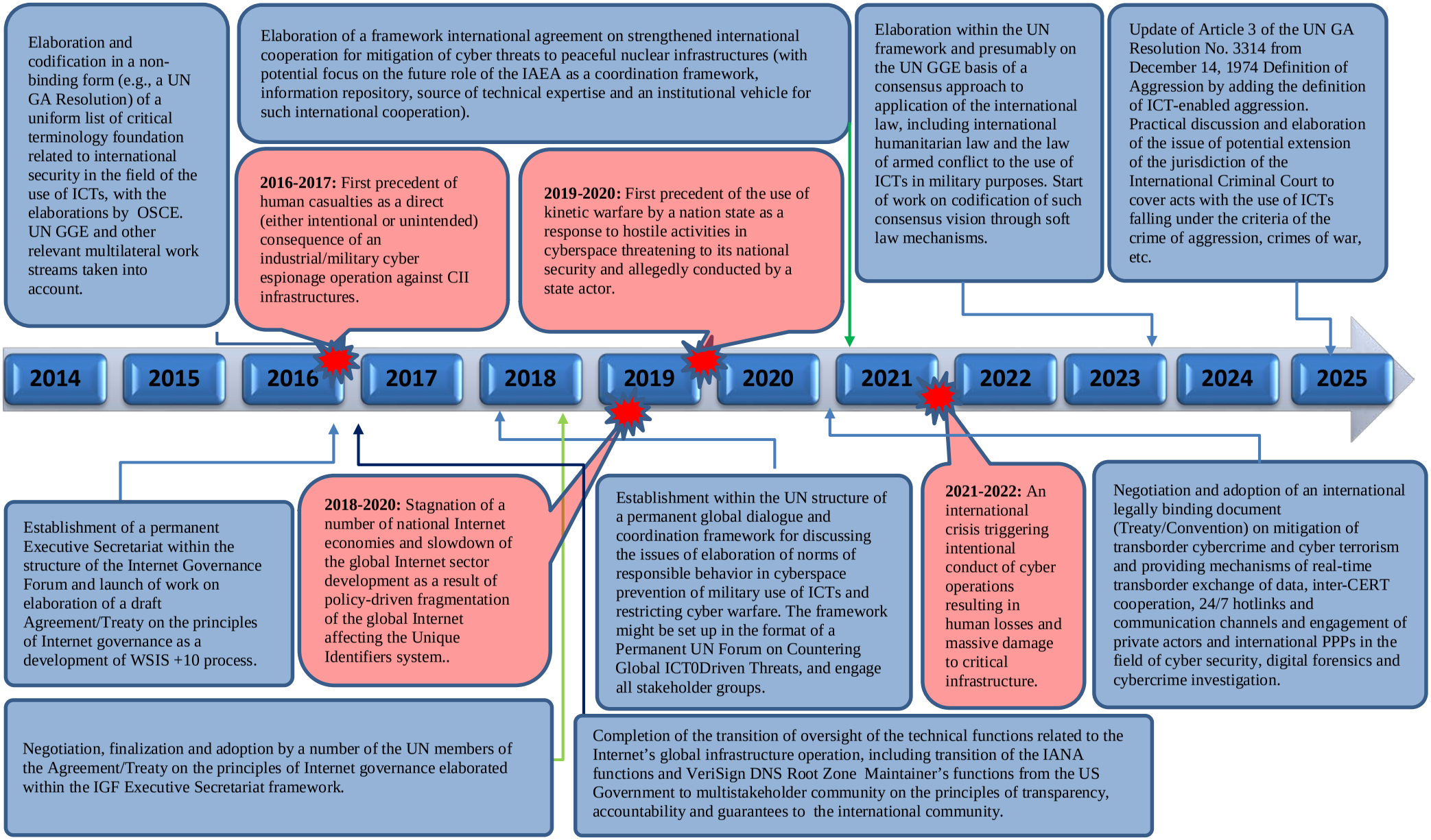
The Report was also designed for and oriented to serve academic institutions, including universities and think tanks with a focus on international law, foreign policy and global security. The Report’s materials could be of interest for graduate and postgraduate students with relevant specialization, as well as for experts from technical organizations.

The report “Global Internet Governance and International Security in the Field of ICT Use” was prepared by the PIR Center’s Consultant Oleg Demidov and published by PIR Press (Moscow) in cooperation with the Centre russe d'études politique (Geneva). The views expressed in this article are those of the author and do not necessarily represent the views of, and should not be attributed to PIR Press, Centre russe d'études politique and their partners.

The Report was prepared with support from the Internet Support Foundation.

TABLE OF CONTENTS

Map of Global Threats and Policy Goals in the Field of ICT Use Up to 2025



"The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had."

Eric Schmidt, Chairman of the Board, Google Inc.

"Information and Communications Technology (IT) is one of the most potent forces in shaping the twenty-first century. Its revolutionary impact affects the way people live, learn and work and the way government interacts with civil society. IT is fast becoming a vital engine of growth for the world economy. It is also enabling many enterprising individuals, firms and communities, in all parts of the globe, to address economic and social challenges with greater efficiency and imagination. Enormous opportunities are there to be seized and shared by us all."

Okinawa Charter of the Information Society, 2000

"We recognize that Internet governance, carried out according to the Geneva principles, is an essential element for a people-centered, inclusive, development-oriented and non-discriminatory Information Society. Furthermore, we commit ourselves to the stability and security of the Internet as a global facility and to ensuring the requisite legitimacy of its governance, based on the full participation of all stakeholders, from both developed and developing countries, within their respective roles and responsibilities."

Tunis Agenda for the Information Society, 2003, Paragraph 31

"ICTs are dual-use technologies and can be used for both legitimate and malicious purposes. Any ICT device can be the source or the target of misuse. The malicious use of ICTs can be easily concealed and attribution to a specific perpetrator can be difficult, allowing for increasingly sophisticated exploits by actors who often operate with impunity. The global connectivity of ICT networks exacerbates this problem. The combination of global connectivity, vulnerable technologies and anonymity facilitates the use of ICTs for disruptive activities."

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly of the United Nations, A/68/98, 24 June 2013, Paragraph 5

I. ICTs: A Critical Factor of Global Development

Global trends of the ICT evolution

Information and telecommunication technologies (ICT) have become one of the most ubiquitous, fundamental, and genuinely global technologies that define the dynamics of the development of the global economy and its individual niches and segments.

The Internet is undoubtedly the central component of the global ICT industry. According to the International Telecommunications Union, by the end of 2014 the global number of Internet users will reach 3 billion people, which is about 40 per cent of the planet's population. Internet penetration growth rates are unprecedented; no other mass user technology has ever spread so rapidly. The number of Internet users in the developing countries doubled in the 2009-2014 period from 974 million people to 1.9 billion.

Map 1: Global Internet penetration in 2012

80–100%
60–80%
40–60%
20–40%
0–20%
No data available

Source: Internet Society, Global Internet Report 2014. Open and Sustainable Access for All, <http://www.internetsociety.org/sites/default/files/>, last accessed 15 on April 2015.

According to various projections, half of the planet's population (3.5billion people) will have Internet access by 2017. OSCE experts reckon that the figure will rise to 5bn by 2020. By 2030, Internet penetration rates in the developed countries will be just below 100 per cent. Almost every demographic and social group, including children, the elderly, and the underprivileged, will be using the Internet on a daily basis.

The markets and transactions that constitute the so-called *digital economy* are already worth trillions of dollars. It is the fastest-growing segment of the global economy. According to various estimates (including those by IDC and IDate), the overall size of

the digital economy, which comprises transactions in the electronic commerce market (the business-to-business and business-to-customer segments), as well as the market for digital products and services, reached $20.4 trillion in 2013. This is more than the GDP of the world's largest economy, the United States, which stood at $15.685 trillion in 2013. The figure is equivalent to 25.57 per cent of global GDP in 2013.

The scale and the intensity of the global information exchange via the Internet and other networks continue to grow at a break-neck rate. In 2012, the global volume of Internet traffic reached 44 exabytes, which is more than the aggregate figure for all the previous years since the dawn of humanity. In late 2013, mobile Internet traffic reached 1.5 exabytes. According to Cisco Systems, by 2016 mobile Internet traffic will reach 1.4 zettabytes (1.4 trillion gigabytes), of which 95 per cent will be mobile video traffic.

This information explosion is going hand in hand with a rapid development of the global cloud infrastructure. Cloud computing is a combination of services and solutions based on the principle of on-demand access to a shared pool of distributed resources. The original concept was largely formulated in 2005 as part of the Amazon EC2 project, but it truly came into its own only in the early 2010s, The advantages of cloud computing include on-demand self-service, the pooling of resources, universal network access, elasticity, and service consumption billing. Thanks to the successful capitalization of these advantages, spending of the IT market on cloud technologies and related research programs could have reached 1 trillion dollars in 2014. It is projected that by 2020, one third of all data will be stored or transmitted in the cloud. But in addition to new possibilities and opportunities, cloud computing also represents new information security risks. The greatest of those risks is the increasing vulnerability of the global cloud storages, and the growing dependence on these storages of individual users (who rely on the cloud to store vast amounts of personal data) and businesses, which use the cloud to optimize and develop their critical processes.

Other *big ideas*, such as the Internet *of Things*, and other major ICT sector growth drivers, also pose challenges to the architecture of the global network, forcing it to expand its size and adapt itself to handling new connected devices whose number is many times greater than the total number of people on this planet.[1]

In addition, numerous private companies, civil society outfits, and the technical community – often supported by governments – are developing and implementing a whole number of projects and technologies that greatly improve access to the Internet and wireless network communications, making it immeasurably more accessible for the developing countries. These projects include:

- Internet.org, a partnership set up by Facebook with the aim of providing Internet connectivity to 5 billion people all over the world;
- Google and Facebook initiatives to deploy fleets of satellites, suborbital UAVs and balloons in order to provide Internet connectivity in remote and inaccessible areas;
- Superfast Internet projects offering connection speeds of 2 Gbps to 10 Gbps (Google Fiber), 1.4 Tbps (BT Group), and faster;

[1] For more details about the Internet of Things, see Chapter V. Global Internet Governance: Legal and Policy Aspects (p. 48).

- Projects to set up data exchange networks on the basis of complementary of alternative technological solutions (mesh networks, P2P, etc.).

Even more revolutionary ideas and solutions are being implemented in areas where the Internet sector meets other sectors of the economy, such as manufacturing or the media.

One example is the rapidly growing market for Augmented Reality services and devices. It includes such segments as visual search, information recognition, product visualization, etc. Augmented reality applications are projected to achieve near-100 per cent penetration ratios by 2021. The entire augmented reality market could be worth about $5.15 billion in 2016, including $209 million in the Russian segment.

There are even more breathtaking projections for the 3D Printing market, which is expected to grow by 62 per cent in 2014. It could be worth up to $2.99 billion by 2018. Even though estimates for the capacity of this market are fairly modest, 3D printing has a nearly unlimited potential of applicability in various segments of the manufacturing industry. The most promising areas include the defense industry (the production of weapons, gear, parts and components, ammunition, and robots), biotechnology (printing of artificial biological tissues), construction, and engineering. The 3D printing technology is still far from mature, but it can already produce huge savings and greatly improve efficiencies. For example, a project to print parts for a turbofan engine in 2011 achieved financial savings of 97 per cent and cut production time by 83 per cent.

The most revolutionary change promised by the 3D printing technology, in combination with the related software and the Internet of Things, is a radical transformation of the current industrial manufacturing model through decentralization and individualization. According to projections by Gartner, the average price of a 3D printer will fall below $2,000 in 2016, making this technology affordable for millions of individual users in the developed countries. Development of the market for 3D printing software and virtual 3D models, improvements in the 3D printing technology itself, and expansion of the range of materials that can be used for 3D printing, will make it possible to manufacture many consumer goods and products at home. Even though companies have been quicker than individual users to take advantage of the opportunities offered by 3D printing, the rapid rise of the market for software-modifiable virtual product templates will inevitably lead to the rise of individual manufacturing.

Naturally, 3D printing can be a double-edged sword, and it gives rise to various new security challenges. The first 3D-printed hand gun was produced in 2013. Assault rifles 3D-printed in 2014 are robust enough to fire several magazines of ammunition before they become unusable. There is an obvious potential for the development of a new market for illegal home-made firearms. Its regulation is not among the challenges we will have to face in the near future (not in Russia anyway), but it could become a real problem much sooner than many people expect. On the one hand, we need to master this particular niche, for reasons that include national security. On the other hand, experts need to assess possible consequences of the 3D printing technology for the global arms market, biotechnology, organized crime, and the black market. So far, there has been only one notable Russian initiative in this area: on February 20, 2013 the MoD announced a tender for a contract to create a bio-engineered liver (Project Prometheus)

- but on March 14, 2014 that tender ended without producing any results. The Future Technologies Fund is currently working on several similar projects.

As a result of the implementation of these and other initiatives, the Internet and other networks will continue to expand their spatial and geographic coverage. The introduction of the fifth, sixth, and subsequent generations of wireless communication technologies will make them ubiquitous and affordable, with very few, if any, areas still left without wireless coverage. It would be no stretch to predict that within the next 10-15 years, there will be some form of wireless network available everywhere on this planet, regardless of the altitude, depth, or terrain. There will be some limited coverage available even in the interplanetary space.

In other words, the social and economic preconditions will soon be in place for Internet access to become a universal and ubiquitous common good.

Rights to Internet access

The universal and ubiquitous Internet coverage that will be achieved in the near future, and the vast significance of the Internet for the economy, social processes, and communications as such, at the level of states, corporations, and individual citizens, produces demand for treating access to digital communications as a basic human right.

This trend has already become clear at the level of international organizations and some nation states (see Table 1).

This trend does not generate any major tensions or conflicts. In fact, it is particularly relevant in the developed countries, where Internet penetration rates are already approaching 90 per cent. In Russia, and especially in the developing countries, where penetration rates are often below 50 per cent, demand for this right is not quite as urgent.

Nevertheless, it must be taken into account when drawing up policies for state regulation of the Internet sector. In the absence of a clearly stipulated right to Internet access in international documents or national legislation, perception of the Internet as a basic common good makes it necessary to keep Internet access available everywhere and at all times. Citizens are increasingly likely to perceive the loss of Internet connectivity in a large territory or across the entire country as a severe national crisis.

The consequences of such situations can be illustrated by one episode during the so-called Arab Spring. On January 27-28, 2011, all the large Egyptian Internet service providers simultaneously switched off their service, leaving 93 per cent of the country’s networks without Internet access. That step, which was thought to have been ordered by the Mubarak government, led to a sharp increase in the intensity of the protests and the numbers of the protesters, who were outraged by the “information blockade”.

Table 1: Access to the Internet as a human right

No	Organization/state	Norms and recommendations
1.	United Nations	A report submitted by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, on August 10, 2011 (A/66/290), reads that "States have a positive obligation to promote or to facilitate the enjoyment of the right to freedom of expression and the means necessary to exercise this right, which includes the Internet."
2.	OSCE	A report headlined "Freedom of Expression on the Internet" by Dunja Mijatović, the OSCE representative on freedom of the media, reads that "every person has the right to participate in the life of information society, which is why states must guarantee citizens' access to the Internet".
3.	Finland	Starting from July 2010, under the terms of Section 60 (3) of the "Universal Service Provision" (the law "On the communications market"), all citizens have a legal right to a broadband Internet connection with a speed of at least 1 Mbps.
4.	Brazil	On April 23, 2014 on the margins of the NETmundial Summit of the Future of Internet Governance the President of Brazil Dilma Rousseff signed Law No. 12.965 also known as Marco Civil da Internet. The law has become of the first comprehensive "Laws on the Internet" to be adopted by a nation state. Marco Civil establishes "establishes principles, guarantees, rights and obligations for the use of the internet in Brazil and provides guidelines for the actions of the Union, the States, the Federal District and the municipalities in this regard". According to paragraphs I-II of Article 4, the discipline of internet use in Brazil aims to promote the right of all to access the internet; and the access to information, to knowledge and participation in the cultural life and in the handling of public affairs. Also, as stated in Article 7 of Marco Civil, "The access to the internet is essential to the exercise of citizenship, and the following rights are guaranteed to the users: <…> – IV – non-suspension of the Internet connection, except if due to a debt resulting directly from its use; – V – maintenance of the quality of Internet connection contracted before the provider".

Even without such radical examples, it would clearly be unwise to introduce any legislation that allows for large-scale and/or long-term restrictions of Internet access for large numbers of users. Citizens have become so reliant on the Internet for their information and communication needs that even at times of crisis, such measures must be avoided at all cost. This must be taken into account when drawing up crisis management and emergency response strategies.

At the same time, the Internet's growing role as a basic common good increases the importance of ensuring stability of the global network and security of its critical infrastructure.

Crypto currencies: challenges and opportunities for the global financial system

ICT and the Internet are opening up radically new technological and infrastructural opportunities for the global financial and economic system. Crypto currencies are a new instrument of liquidity that has no precedent in economic history. As of September 2014, the total value of crypto currencies in circulation was about $7billionn; Bitcoin made up roughly 90 per cent of that constantly growing figure. From the legal point of view, crypto currencies are unchartered territory for the financial system and international law.

Anonymity of transactions and an almost unlimited number of issuers of crypto currencies make such currencies a very flexible and convenient payment instrument. Their other advantages include lack of any linkage to other liquidity instruments or currency standards, perfect divisibility and mobility, and a natural barrier against inflation formed by the very principle of issuing such currencies. As a result, there is a lot of demand for them in the context of the ongoing reform of the financial system. In essence, crypto currencies are more suitable for the role of an instrument of decoupling the global financial architecture from the dollar standard than any other payment instrument currently in existence.

"Virtual currencies are a very interesting international experiment that breaks the very paradigm of currency emission. I definitely believe that they should not be banned. Instead, we should try to understand them, and maybe come up with proper ways of regulating them."

German Gref, Chairman of the Board of Sberbank

Nevertheless, at the current stage crypto currencies cannot be regarded as a credible alternative to the existing payment instruments because their aforementioned virtues and advantages also have major downsides. Anonymity of transactions makes such currencies an attractive instrument of illegal trade, including trade in banned products and services, and of financing crime and terrorism.

- In 2011-2014, the most well-known crypto currency, Bitcoin, was used as a payment instrument by the largest anonymous Internet trading platform, Silk Road, which was hosted in the .onion zone of the Tor anonymous network. At the peak of its rise in 2012-2013, Silk Road was selling up to $14-15 million worth (in Bitcoin equivalent) of weapons, drugs, and other banned products

every month. According to the FBI, 9.5 million Bitcoins worth of goods had been traded via Silk Road since its launch; as of September 2014, that figure was equivalent to $4.55 billion.

- According to Russia's Group-IB, crypto currencies, including Bitcoin, were one of the most popular payment instruments on the Russian cybercrime market (leasing botnets, trading personal data, etc.) in 2012-2013.

Most of the countries in the world, including China, Russia, and the United States, have chosen the strategy of restricting or even banning crypto currencies. For now, however, these legal restrictions are having next to no effect on the emission of crypto currencies, the volume of such currencies in circulation, or demand for them. Bitcoin has appreciated against the dollar by 300 per cent since the arrest of the founder of Silk Road in 2013. In the absence of effective regulation of crypto currencies, legal bans will merely drive such currencies underground and into the black market, further strengthening their role in financing crime. They could also pose a threat to the entire global financial system if the flows of liquidity between the legitimate and shadow segments of that system reach a certain level.

As a consequence, one of the major threats generated by lack of sensible regulatory approach might be gradual erosion of the global financial system resulting from the rise of an unregulated crypto currencies market in the 2019-2020 time horizon.

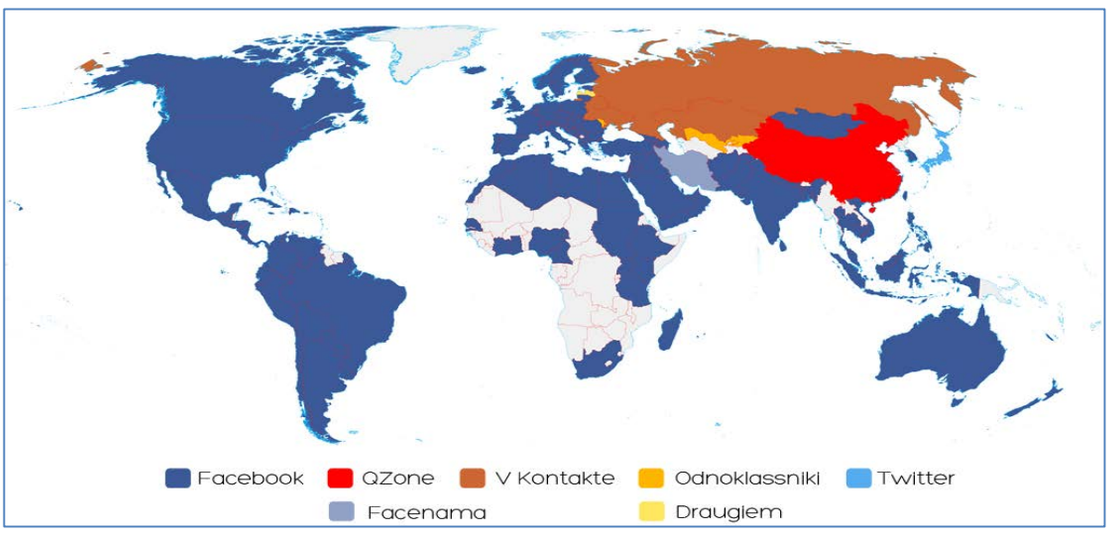
Russia's agenda in the Internet sector

Russia is one of the leading global powers in terms of national Internet sector growth:

- It ranks 7th in the world in terms of the number of Internet users;
- It is in the global Top 5 in terms of the level of *connectivity* of its national segment of the Internet;
- Russian is the third most popular language on the Internet in terms of the amount of available resources (5.7 per cent of all web pages in the world were in Russian as of September 2013);
- In the period between 2000 and 2013, the number of Russian-speaking Internet users grew by a factor of 27.22, reaching 87.48million people in December 2013 (the 7th largest language group on the Internet);
- The .RU zone hosts 1.8 per cent of all domain names on the Internet (4.89 million), making it the 5th most popular top-level country domain and one of the Top 10 top level domains;
- Russia is one of only four countries in the world whose market is dominated by home-grown social networks. VKontakte is the 8th largest social network in the world in terms of unique monthly users (80 million);
- Russia is one of only three countries in the world, along with the United States and China, whose market is dominated by a home-grown search engine (Yandex controlled 53 per cent of the Russian search engine market in 2014);
- The Russian-language segment of the Internet plays a crucially important role in the support and promotion of the Russian language abroad. In countries such as Belarus, Ukraine, Tajikistan, Kazakhstan, and Kyrgyzstan, 73-86 per cent of all websites are in Russian;

- Russia is the home of Mail.Ru, one of Europe's largest Internet companies. The company's capitalization stood at $6.2 billion in September 2014;
- Russia is one of the global leaders in the end-user cybersecurity market. Kaspersky Lab controlled 5.5 per cent of the global market for anti-virus software, with $667 million of revenue in 2013 and over 300 individual users.

Map 2: Dominant social networks in the world in the end of 2014



Source: VincosBlog., <http://vincos.it/world-map-of-social-networks/>, last accessed on April 30, 2015.

It is estimated that the Internet-dependent sectors of the Russian economy contribute 5.2 trillion roubles (8.5 per cent) to Russian GDP. This is more than the contribution of such industries as agriculture, forestry, and hunting (3.7 per cent in 2013), and comparable to the construction industry (6.5 per cent in 2013).

According to the Russian Association of Electronic Communications (RAEC), the size of the Internet sector of the Russian economy topped 1 trillion rubles in 2013. There are 68.7 million Internet users in Russia (48 %of the population); 56.3 million of them use the Internet on a daily basis.

Growth figures in the Internet-dependent sectors of the Russian economy are way ahead of the overall economic growth rates. According to a study by RAEC and the Higher School of Economics headlined "The Economics of Runet in 2013", the Russian Internet sector and Internet-dependent industries will grow at an annual rate of 15-20 per cent between now and 2018. The size of the Runet economy is expected to reach 1.872 trillion roubles by 2018, and Internet-dependent sectors of the Russian economy will contribute 14.29 trillion roubles to national GDP.

These growth rates are way ahead of the overall growth of the Russian economy. According to the Long-Term Social and Economic Growth Projection to 2030, a document prepared by the Economic Development Ministry, the Russian economy will grow at an average annual rate of only 3.2 per cent in 2013-2030.

To summarize, ICT and the Internet-dependent sectors of the Russian economy have become one of the main non-commodity engines of Russian economic growth and innovation. They can serve in that capacity for the next decade at the very least, barring any major economic upheavals or suboptimal state regulation strategies.

Providing comprehensive government support for the ICT industry, creating a favorable climate for its development, and adopting stimulus measures to create new engines of growth in that industry should therefore be regarded as a key priority in any short, medium, and long-term economic strategy for Russia.

In general, following recommendations might be addressed to decision makers and expert community in Russia:

1. The Internet sector as a whole should be recognized as one of the key sectors of the Russian economy; that status should be reflected in key policy documents and legislation.

Some individual facilities and information systems of the Russian segment of the Internet may be designated as critical infrastructure facilities, regardless of their form of ownership. The government would thereby undertake an obligation to provide a proper level of security for such facilities, and to do all it can to ensure their reliable and uninterrupted work. One example of the infrastructure that could be designated as critical is the infrastructure that underpins the work of the Yandex services in Russian territory.[2]

2. The key role played by the Internet in the development of the Russian economy must be properly and adequately reflected in the system of government agencies responsible for stimulating and supporting that industry. Most of the functions related to the development of the Internet industry now lie with the Ministry of Communications, but some aspects of that industry remain outside the ministry's remit.

What is required is a constant and close ongoing dialogue on the entire range of issues related to the Internet sector, from content security issues to ensuring reliable and uninterrupted work of critical Runet infrastructure. The government could set up a mechanism for such dialogue in the form of an inter-agency coordination body that would include representatives of the Foreign Ministry, the Communications Ministry, the FSB, the Interior Ministry, Roskomnadzor (the media and telecommunications supervision agency), the Ministry of Economic Development, etc.

In a long-overdue move, in February 2014 the government set up the office of special presidential representative for international cooperation in the area of information security. At the moment of writing this office is held by Andrey Krutskikh, an experienced diplomat. It would make sense for the government to set up a similar office of presidential representative for the development of the Internet industry. Such an office could effectively lead and coordinate inter-agency efforts in this area, including efforts to tackle security issues.

[2] For more details, see Section III. Security of Critical Information Infrastructure: Key Threats and Response Strategies.

3. The government must create a favorable climate for the development of Russian Internet businesses in the foreign markets and their involvement in global competition. As far as government regulation is concerned, any initiatives aimed at reducing physical connectivity between the Russian segment and the global Internet, achieving a greater degree of infrastructural or other autonomy, or restricting the Runet in any other way, could have unpredictable consequences.

Leaving aside human rights issues, it is worth emphasizing that growth and expansion of Russian Internet business depends to a critical extent on the *scale effect*, which becomes genuinely global in the case of the Internet. Negating that effect through fragmentation of the Internet and isolation of its Russian segment would gradually deplete that segment's growth potential as the domestic market becomes saturated.

4. Gradual revision might be a timely step with regard to the role and potential of Runet as an instrument of promoting and maintaining Russian cultural and language identity and a vehicle for popularization and globalization of Russian cultural heritage, as well as modern Russian culture. Online instruments and Internet projects must be regarded as key priorities by such agencies as Rossotrudnichestvo (the Russian international cooperation agency). The colossal potential of the Russian Internet industry in this sphere also creates excellent synergies with the Russian foreign-policy goals pursued by the Foreign Ministry. Developing digital diplomacy instruments is a necessary strategy, but that strategy must be formulated and implemented with active involvement of the Russian Internet industry.

5. The government must take proactive steps to explore radically new technological niches that are opening up in the area of ICT. For example, it must stimulate imports and local development of 3D printing equipment and technologies. It must support efforts by the private sector, and improve state regulation (by making it more liberal, rather than more restrictive) in order to facilitate accelerated development of the most promising segments of this market. Proactive regulatory steps to spur the development of such new technologies will help to minimize the associated risks and security challenges. They will also create a favorable climate for the development of these technologies in the local market, turning them into Russia's asymmetric competitive advantage rather than yet another area where the country is lagging behind the world leaders.

Additional information:

1. The Runet Today. Analysis, figures, and facts, RIF+KIB Opening 2014. April 23-25, 2014,
<http://files.runet-id.com/2014/rif/presentations/23apr.rif14-s0--plugotarenko.pdf>,
last accessed on April 30, 2015.
2. Internet in Russia. Economics of Runet in 2012-2013, Organizers: RAEC, Higher School of Economics, Moscow, 2013, <http://экономикарунета.рф/>, last accessed on April 30, 2015.
3. Demidov Oleg, From Access Rights to Network Intelligence, The Russian Council for Foreign Affairs, March 29, 2013,
<http://russiancouncil.ru/inner/?id_4=1618#top>, last accessed on April 30, 2015.
.

II. International Security in the Field of ICTs: Towards Shared Visions

As governments continue to elaborate their policies in the area of the use of ICT and Internet governance, and in view of increasingly energetic international discussions and attempts to produce international agreements, norms, and regulations in this area, it becomes increasingly important to define common terminology and a shared understanding of the approaches implied by that terminology.

At the same time, there are growing differences and politicization of the debate about the terminology part of the proposed policy documents, national legislation, and international documents, especially in the area of security in the use of ICT.

The concept and terminology of *cybersecurity* has been emerging first in the United States, and later in most of the developing countries since the mid-1990s. That concept is based on the idea of the *cyberspace* as a kind of non-physical ICT environment. Even though these terms and their derivatives are not always used in national legislations, and their official definitions are not always explicit, the terminology and the very idea of cybersecurity have become firmly established in the professional community, the private sector, the strategies and doctrines of many countries, supra-national bodies (the EU), and international organizations such as NATO, the Council of Europe, the ASEAN Regional Forum, OECD, OSCE, and many others.

Meanwhile, alternative concepts and approaches based on different terminology have emerged in several other countries, especially Russia. One of the most comprehensive and detailed concepts in that area is the International Information Security Concept, which was initially formulated by Russia, and later supported and adopted by members of the Shanghai Cooperation Organization (SCO) and other countries and organizations (such as the CIS and the Collective Security Treaty Organization).

Ever since Russia began to promote this approach at international venues (especially the UN) in 1998, it has been facing opposition from several developed countries, international organizations, the technological community, and foreign private business. Russia's opponents, including experts and diplomats from the United States and Western Europe, are pointing at the discrepancy between the Russian approach and the existing practices that have emerged in the international community of technical experts, as well as private business practices in most of the countries all over the world.

Another key problem in this debate is differences as to whether the impact of information content on social, political, and other public processes should be included on the list of issues that must be discussed, coordinated, and, at some point in the future, internationally regulated as part of the ICT security approach.

The contents of the information generated and transmitted by means of ICT, and the impact of that information on public processes is one of the cornerstones of the International Information Security concept. Meanwhile, in accordance with the existing practices in the United States, Western Europe, and many other countries, this particular aspect is not regarded as an integral part of cybersecurity or the entire ICT sphere. Instead, these issues are viewed in the context of human rights and freedoms (freedom of speech, freedom of expression) or in the narrow security context of

countering terrorism and extremism. In other words, they are viewed outside the ICT-specific context. The emphasis of the entire cybersecurity agenda is on ensuring secure, reliable, and uninterrupted work of the ICT infrastructure. In that approach, the "human", or "content" aspect of the problem plays an important but indirect role.

Table 2. Definitions of cyberspace/information space in selected documents

Source document & author	Term	Definition	Year
Cyber Security Strategy for Germany, 2011	Cyber space	The virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.	2011
U.S. Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02	Cyber space	A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processes and controllers	2015 (As Amended Through 15 March 2015)
Agreement among the Governments of the Shanghai Cooperation Organization Member States on Cooperation in the Field of Ensuring International Information Security	Information space	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.	2009
Concept of Cyber security strategy of the Russian Federation	Cyber space	A field of activity in the information space which is composed by the totality of communication channels of the Internet and other telecommunication networks and technical infrastructure that enables their operation, and all forms of human activities (on individual, corporate or state level) conducted through the use of such networks and infrastructure.	2013
Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations	Cyber space	An electronic domain through which information is created, transmitted, received, stored, processed and deleted	2011

Yet another major difference between these two concepts is the interpretation of national sovereignty as applied to the area of ICT. The International Information Security concept focuses on the inviolability and supremacy of national sovereignty in the ICT sphere, and proposes mechanisms of achieving agreements that are primarily based on cooperation between sovereign states. The cybersecurity concept, on the other hand, has nothing specific to say about issues of sovereignty because these issues simply lie outside its remit. But the fundamental vision of ICT processes reflected by such an approach presupposes the recognition of the transnational nature of cyberspace, and therefore, recognition of incomplete applicability of the ideas and practices of national sovereignty to cyberspace. This lies at the core of the radical differences as to the mechanisms and instruments that can be applied to ensure security in area of ICT at the level of nation states and at the international level.

The conflict between the concepts of international information security and cybersecurity can be found even at the national level of regulation in Russia, and the definitions of basic terms such as cyberspace are not uniform in various countries, either (see Table 2).

In 2012-2013 an attempt was made to engage the expert community and the private sector in drawing up a doctrinal document in the upper chamber of Russian parliament. That attempt showed that there is clear demand among all the interested parties for reflecting cybersecurity issues in such a document. The result came in the form of the Concept of Russian Cybersecurity Strategy, which is regarded by many experts as a progressive document that reflects international trends in the area of ICT. At the same time, that Concept clearly runs counter to the terminology and concepts of other Russian legislation and doctrines, including the 2000 Doctrine of Russian Information Security and the 2013 Basics of Russian State Policy in the Area of International Information Security to 2020. In other words, the terminological and conceptual conflict on ICT security issues has already become a reality even within Russia itself, which makes it all the more important to resolve that conflict as quickly as possible.

Different opinions about state sovereignty in the area of ICT also result in different visions of the state's remit with regard to the key component of the ICT infrastructure, the Internet. The self-regulation practices and the prevailing role of the technical community in the development of the Internet that have become firmly established in the United States have also been adopted in many other countries. These practices and approaches are reflected in the concept of multistakeholder Internet governance. The essence of that concept is that Internet governance can be done properly only if it involves representatives of all the groups and parties (stakeholders) that have a direct interest in the development of the Internet, and if all these representatives have equal rights and equal status. The initial list of stakeholders included the state, the private sector, and civil society. It was later expanded to include the community of Internet users and the technical community, which makes that list fairly open.

This principle was recognized and made official in the decisions of the Tunis stage of the World Summit on the Information Society (WSIS) held in 2005. Almost all the countries in the world, including Russia, support WSIS decisions and the multistakeholder approach. That does not mean, however, that all the differences in its interpretations and definitions have been eliminated. Russia and several of its partners on the international arena do not believe that the multistakeholder Internet governance

principle somehow diminishes or negates state sovereignty on issues of Internet governance. Therefore, they insist that all international decisions in that area should be made by representatives of sovereign states. Other stakeholders must be involved in the exchange of opinions, consultations and discussions when decisions are being drafted – but they cannot actually make those decisions on their own, thereby supplanting the state as the only source of sovereignty under international law.[3]

Different approaches, and the resulting different terminology and definitions in the area of ICT security and Internet governance have the right to co-exist. Over the past several years, however, the competition between the various concepts and terminologies in this area has been increasingly politicized. That often makes it difficult to find practical solutions and identify mechanisms of cooperation between all the parties involved.

For example, differences in terminology in the area of ICT security between the United States and Russia have delayed by at least 12 months the signing of some breakthrough bilateral agreements that included a set of measures to counter various ICT security threats. In 2011 experts and diplomats began to work on a package of three agreements to be signed by the Russian and U.S. presidents on the sidelines of the G20 summit in Los Cabos, Mexico, on June 18-19, 2012. But due to the aforementioned differences, that package was signed a whole year later, on June 17, 2013. As a result, the prospects for that format of cooperation were overshadowed by the deterioration of Russian-U.S. bilateral relations, which came at a time when not all the agreed mechanisms had yet been established and put into practice. Had the agreements been signed one or two years earlier, those mechanisms would have already become more firmly established and resilient to the ongoing crisis in bilateral relations.

In the broader sense, differences in definitions and terminology are reducing the chances for constructive work at various international venues (such as the series of international conferences on cyberspace that began in London in 2011). These differences are preventing the parties from focusing on genuinely important long-term goals. Such goals include the formation of the institutional framework of a global system of countering ICT threats and preventing cross-border conflicts involving the use of ICT.

Differences in terminology are also hampering the reform and modernization of international laws that would facilitate more effective international efforts to counter the threats brought on by the emergence of the latest information technologies.[4]

Lack of progress in addressing these problems, which is often the result of inability to agree on a shared set of terms and definitions, could lead to a series of long and destructive crises and conflicts involving the use of ICT in another five to eight years.

In this light, the following recommendations might be provided on these issues for short-term and middle-term perspective:

[3] For more details on multistakeholder Internet governance, see Section V. Global Internet Governance: Legal and Policy Aspects (p. 48).
[4] For more details, see: Section IV. Military and Political use of ICTs: Challenges to Global Security and International Law (p. 36).

A common objective is to depoliticize the issue of definitions and terminology in the area of ICT security and take that issue outside the framework of developing cooperation mechanisms, where at all possible. At the same time, all the parties involved must step up their efforts to produce a shared set of definitions and terminology for use at the international level.

1. To define and agree in a non-binding form on a list of terms that do not require any further definition or interpretation since they have already become universal, or because all the parties have already arrived at a common understanding of those terms. Possible venues for that include the UN Group of Governmental Experts and the OSCE.

One example of such a term that requires no further definition is the Internet. Initially the word was used to denote the global information and telecommunication network. By now, however, the word is commonly used to denote a global communication technology, and even (as already mentioned above) a *global public good.* The precedent of defining the word "Internet" was set in 2004-2005, when experts of a working group under the UN General Secretariat arrived at the conclusion that this term requires no official explications or definitions precisely because it is so obvious and universally understood.

2. Eliminate the terminological conflict between cybersecurity and International Information Security by comprehensively promoting and popularizing at various negotiation and discussion venues the ideas and mechanisms proposed by the UN Group of Governmental Experts on Developments in the Field Information and Telecommunications in the Context International Security, and the relevant resolutions that are being adopted by the UN General Assembly every year since 1998 (these resolutions have incorporated recommendations by the UN GGE since 2005).

One of the terms under discussion is "*security of and in the use of information and communication technologies (ICTs*)", as a neutral and non-politicized term that has a broad scope.

3. To support and implement measures in the area of consensus terminology included in the initial list of confidence-building measures in the OSCE framework in order to reduce the risk of conflicts resulting from the use of ICT. That list was agreed and adopted on December 3, 2013 with active Russian participation.

More specifically, Article 9 of that list proposed the following:

- Each State shall provide, on a voluntary basis, a list of terms in use in that State in the areas of security of and in the use of ICT, with explanations and definitions attached to each term;
- The participating States shall compile, in the medium term, a common and agreed glossary of critical ICT terms in the area of international security.

It would make sense to undertake a similar effort with regard to terminology at some other venues, including the ASEAN Regional Forum (ARF) and the already mentioned UN GGE.

4. In those cases where mechanisms to reach a consensus with regard to terminology are not working or are simply absent from diplomatic practice, it would make sense to use the technology-oriented definitions provided by international organizations, especially in the UN framework.

One example of such an international organization is the International Telecommunications Union (ITU), which produced a definition of cybersecurity back in 2008 as part of its standard *X.1205 (04/2008) Overview of Cybersecurity*. According to that document, "Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment". It is also worth studying the experience of the International Organization for Standardization (ISO). Even though ISO is a non-governmental organization, it is active in 164 countries and plays an important role in producing and promulgating various international standards. One of the standards it has produced is ISO/IEC 27032:2012 "Information Technology – Security Techniques – Guidelines for Cybersecurity", which was adopted in 2012.

5. Finally, overcoming conflicts of terminology in the area of ICT and their use is impossible without an exchange of opinions between representatives of the expert communities of different countries and regions. In addition to the work of government experts in the UN GGE framework, it is also necessary to strengthen *Track 1.5* and Track 2.0 by stepping up the work on critical ICT terminology.

One successful project of that kind was implemented in 2011 by the West-East Institute and the Moscow State University's Institute of Information Security Problems. Following discussions within a group of Russian and U.S. experts, the project published a bilingual list of 20 critical cybersecurity terms and their definitions. It would be useful to resume work in that format, and to strengthen it by involving a broad circle of governmental and nongovernmental experts from Russia, the United States, and other countries. PIR Center will be ready to join such efforts in the near future.

6. Even though the Concept of the Russian Cybersecurity Strategy runs counter to various doctrines and regulatory documents currently in force, there is clear demand in the expert community for the approaches to security problems in the area of ICT that are reflected in that Concept.

It would therefore be useful to form a new working group that includes representatives of government agencies (the Security Council, Foreign Ministry, FSB, Defense Ministry, Interior Ministry, Communications Ministry, and others) and representatives of the private sector, the academia, and the technical community. The purpose of the group would be to formulate possible options for harmonizing the terminology used in the Concept of Russian Cybersecurity Strategy with the existing Russian legislation and regulation.

7. Finally, the another recommendation for 2017-2018 would imply development and adoption of a non-binding UN document containing a uniform list of critical terminology in the area of ICT and guidelines on the use of that terminology in the area of international security, taking into account the work already done at the OSCE, ASEAN, UN GGE, and other international bodies and foras.

Additional information:

1. Mikhail Yakushev. Internet 2012 and international politics. Security Index, No 1 (104). 2013. P 29-42.
2. Materials of the PIR Center's Roundtable "International information security and global Internet governance: views of Russian and international experts at a Geneva meeting", Security Index, No 1 (104), 2013. P. 185-206.
3. Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations. The East-West Institute, April 26, 2011, <http://www.ewi.info/idea/russia-us-bilateral-cybersecurity-critical-terminology-foundations#sthash.C6w9sHsj.dpuf>, last accessed on April 30, 2015.

Documents:

1. Decision No 1106. Initial Set of OSCE Confidence-Building Measures to Reduce the Risks Of Conflict Stemming From the Use of Information And Communication Technologies, Organization for Security and Cooperation in Europe, Permanent Council, December 3, 2013, <http://www.osce.org/ru/pc/109648?download=true>, last accessed on April 30, 2015.
2. Concept of Cybersecurity Strategy of the Russian Federation, Council of the Federation of the Federal Assembly of the Russian Federation, <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf>, last accessed on April 30, 2015.
3. Convention on International Information Security (Concept), Ministry of Foreign Affairs of the Russian Federation, < http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument>, last accessed on April 30, 2015.
4. Agreement among the Governments of the Shanghai Cooperation Organization Member States on Cooperation in the Field of Ensuring International Information Security, NATO Cooperative Cyber Defense Centre of Excellence website (in Russian), <https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf>, last accessed on April 30, 2015.
.

III. Security of Critical Information Infrastructure: Key Threats and Response Strategies

"Information technologies play an increasingly important role in modern military conflicts. The so-called information attacks are already being used to achieve military-political objectives. According to specialists, the destructive force of such attacks can be even greater than the destruction caused by conventional weapons. We must be ready to effectively counter threats in the information space and step up the level of security of relevant infrastructure, especially the information systems of strategically important and critical facilities."

Statement by the President of the Russian Federation Vladimir Putin
at the Russian Security Council meeting on July 5, 2013

Regardless of the motives of illicit actions in the area of ICT, threats to a certain class of facilities – namely, critical infrastructure facilities, including critical information infrastructure facilities – are in a class of their own.

Definitions, classification, and regulation of critical infrastructure facilities

The first problem that is not only academic and theoretical but practical as well is the absence of uniform definitions at the international level and even in the regulatory norms and practices of many individual countries.

Critical facility: a facility where disruption could result in loss of control over the economy of the Russian Federation or a Russian administrative unit, its irreversible negative change (destruction) or substantial deterioration in the security of life support systems.

Critical Information infrastructure (CII): A complex of automated industrial control systems of critical facilities and the IT networks that underpin their work, as well as information systems and communication networks that are vital for work of the government, national defense capability, security, and law and order.

Project of the Federal Law "On security of critical information infrastructure of the Russian Federation" (submitted to the Russian Parliament by Federal Security Service (FSB), as of August 8, 2013)

Russia is one of the countries that has started to shape a systemic regulatory approach to the provision of security of critical information infrastructure (CII) facilities. In another important step forward, in 2013 the FSB prepared a draft federal law "On security of critical information infrastructure of the Russian Federation". The definitions of CII and of Critically Important Facilities (CIF) proposed in that draft are used in this report, as is the definition of Critical Infrastructure (CI).

Comparisons of the terminology used in various documents produced in Australia, Britain, Canada, Germany, Japan, the Netherlands, Russia, the United States, and other countries indicate substantial discrepancies in the underlying logic of the definitions of such facilities. Different countries also define different classes/sectors of CII (or sometimes lump CII together with other critical infrastructure).

For example, the United States has defined 16 different sectors of critical infrastructure. Canada, the EU, Switzerland, and Japan each have 10 sectors (though the precise list is different in each individual case). The existing regulatory system in Russia identifies critical infrastructure by seven types of threats, two classes of threats, and 50 types of facilities (the seven types of threats are roughly equivalent to the sectors used in foreign countries).

The vast majority of the countries include the following facilities in the definition of critical information infrastructure (CII):

- Nuclear industry facilities;
- Electricity grids, electricity generation and distribution facilities;
- Transport systems: aviation, railways, motorways, etc.;
- Agricultural production and storage facilities, food distribution facilities;
- Government buildings and government communication facilities;
- Fuel and energy facilities, including oil and gas industry facilities;
- Key telecommunication systems, networks, hardware and software systems, and communication systems;
- Defense industry facilities;
- The financial and banking sector;
- Water supply facilities;
- Healthcare facilities.

On the one hand, this list demonstrates that some categories of facilities are regarded as Critical Infrastructure in almost every national jurisdiction. But on the other hand, even in this case there are inevitable differences in interpretations, definitions, and specific composition of these categories. For example, many countries have separate CI categories that have no equivalent in other countries, and vice versa.

There are no mechanisms at the international level that could facilitate cooperation in securing critical information infrastructure. For example, there are no special measures to provide CII security in the Budapest Convention or the intergovernmental agreement of the Shanghai Cooperation Organization. Even though cases of cyber espionage directed against CI facilities are sometimes investigated by the national CERT or CERT associations, IMPACT-ITU, or other international private sector organizations, very few of these formats specifically target cyber threats to critical facilities.

One of the few exceptions is the International Atomic Energy Agency (IAEA), which pursues efforts to strengthen cybersecurity of peaceful nuclear energy facilities as part of its remit. The agency issues technical guidelines on the provision of computer security at nuclear facilities (Series NSS 17) and develops specific recommendations in that area in its nuclear security documents (INFCIRC/255/ Revision 5). The IAEA nuclear security department leads a Computer and Information Security Program. As part of that program, it develops technical recommendations, releases various

documents, holds consultative meetings, and offers regional training courses. One of the types of threats the program aims to counter is targeted computer attacks.

Another platform that is used to study international experience and best practice in the area of CII security is the OECD. In 2007-2009 the organization released a series of reports and other documents that summarize analysis of the policies of seven states that pursue different approaches to CII security. Some of the key conclusions made in OECD documents point at the need to develop research and education policies on protecting critical infrastructure from ICT threats; stepping up international cooperation between CERTs and CSIRTs; and closer information exchange on threats, best practices, and the development of public-private partnership. It would make sense for Russia to take into account the OECD experience and conclusions (especially since the country is preparing to join the organization) as part of its own national approach to protecting CII.

Other regional organizations that are actively involved in efforts to secure critical information infrastructure include the OSCE and ASEAN/ARF. In 2013 the OSCE released Guidelines on Best Practices in the Protection of Critical Non-Nuclear Energy Infrastructure from Terrorist Attacks in Connection with Threats Emanating from Cyberspace. The document contains a list of recommendations on the development of closer international cooperation in this area.

As far as national efforts are concerned, the United States (or more precisely, the National Institute of Standards and Technologies) is one of the leaders in the regulation of CII security issues. In February 2014 NIST issued a Framework Document on Strengthening Cybersecurity (Version 1.0). The objectives of that document were formulated in 2013 in President Obama's Executive Order 13636 "Improving Critical Infrastructure Cybersecurity". They include the creation of a system of standards, guidelines, and practices to facilitate private-sector and government efforts in managing ICT risks. The NIST document is one of the key policy papers in the area of securing CII that is positioned as a model for international cooperation and a template for use by foreign countries. It is hoped that the document will help to "find common ground for international cooperation in the provision of CII security". In 2011 NIST released another document on CII security: Guide to Industrial Control Systems (ICS) Security (NIST SP800-82). The U.S. institute's wealth of experience in cybersecurity of critical infrastructure should be studied and used in the development of international practices and documents on CII security.

Cyber exercises focusing on critical infrastructure are becoming an increasingly important part of practical and applied formats of international cooperation.

The European Network and Information Security Agency (ENISA) has held the *Cyber Europe* pan-European cyber exercise once every two years since 2010. The third such exercise began on April 29, 2014. It involved 29 teams representing EU member states, and more than 400 specialists. The main objective of the event was to identify weaknesses and room for improvement in the EU's critical information infrastructure at the technical, operational, and strategic level. Countering CII threats posed by computer attacks and malicious use of ICT is also one of the main objectives of NATO's Cyber Coalition exercise. The 2013 event involved more than 300 specialists from 30 countries, including four partners that are not NATO members. CII threats and

measures to counter them are regarded as part of the cyber defense remit during these exercises.

Another rare example of an international mechanism of developing regulations and approaches to the provision of CII security is the Model Law on the Security of Information and Telecommunication Infrastructure that was developed in the CIS framework in 2013. At the same time, while the law offers the CIS states a template for national legislation in that area, it includes no actual mechanisms of international cooperation in the provision of CII security.

Some other regional organizations that focus on security have also begun to discuss the possibility of joint efforts against CII threats in recent years. They may well succeed at developing some collective mechanisms in that area.

One of the main reasons for the relative scarcity of international cooperation mechanisms for exchanging information on ICT attacks against CII is the special security regime used at such facilities. Almost every country imposes some restrictions on access to information about its ICC due to national security considerations. This is why proper international cooperation will require a whole new level of trust between the parties involved; for that very reason, the potential for such cooperation will remain severely limited for the foreseeable future. A realistic objective would be to achieve a common international understanding of ICT threats to CII and to facilitate access to best international practices and external resources that can be used to counter these threats. The forms of such cooperation and the objectives set before the participants must reflect the current state of CII threats.

ICT-driven threats to CII facilities: key development trends

On the whole, the range of threats to industrial control systems (including Automated Process Control and SCADA systems) used at critical infrastructure facilities is outlined in the OSCE Best Practice Guidelines (see Table 3).

The general trends in ICT threats to critical information infrastructure are as follows:

1. Growing number and magnitude of threats;
2. Smart Grid and new sectors;
3. Strategic motives and involvement of state actors;
4. A strategy of combining instruments of espionage and sabotage.

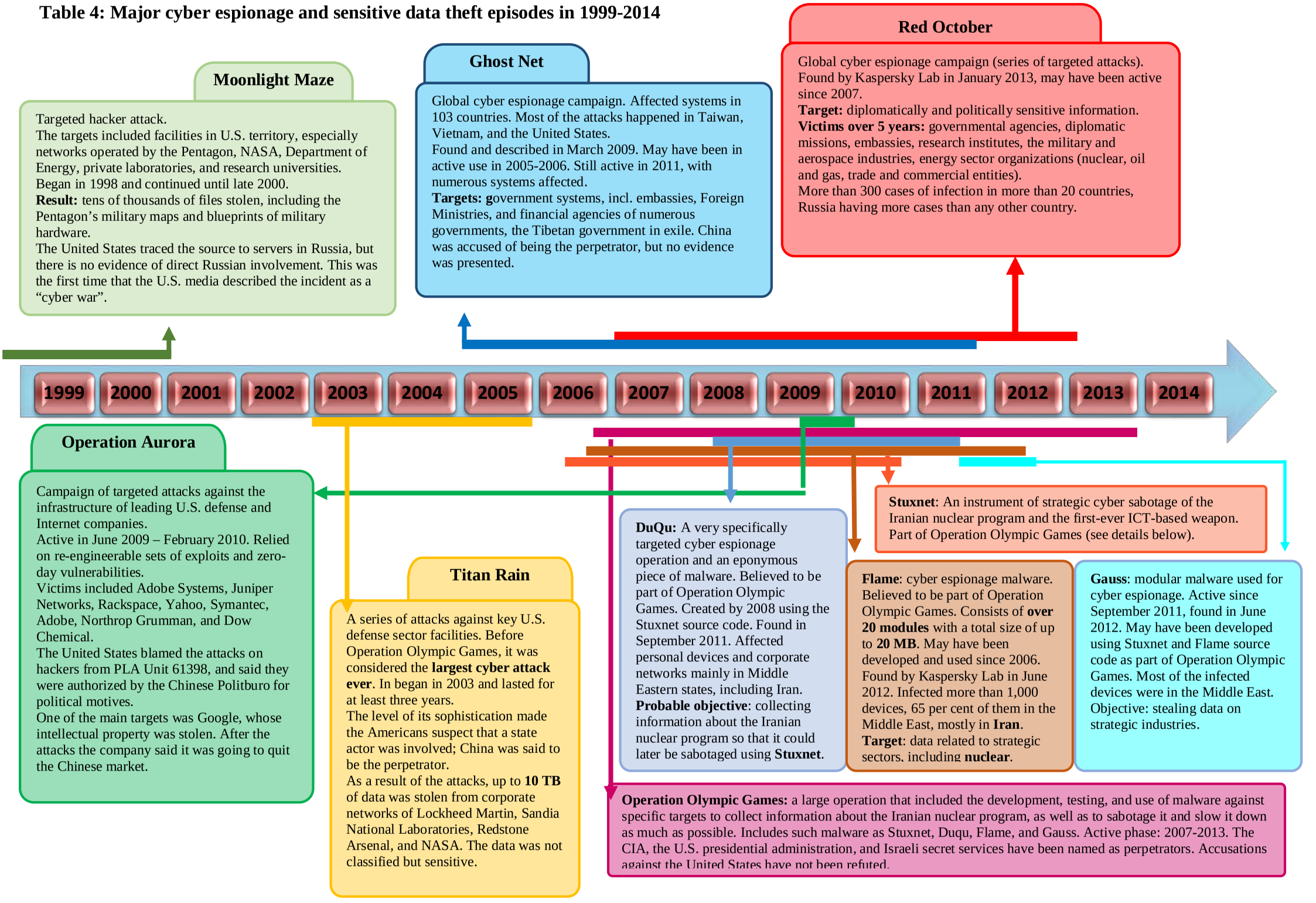
According to the U.S. Department of Homeland Security, the energy sector was the most frequent target of attacks against CII (82 attacks), followed by water supply and distribution facilities (29 attacks); the chemical industry (7), and the nuclear industry (6).

Table 3: Major threats to Industrial Control Systems (ICS) of CI facilities resulting from malicious actions

	Threat	Explanation
1.	Unauthorized use of remote maintenance access points	Maintenance access points are deliberately created external entrances to the ICS network and are often insufficiently secure.
2.	Online attacks via office or enterprise networks	Office IT is usually linked to the network in several ways. In most cases, network connections from offices to the ICS network also exist, so attackers can gain access via this route.
3.	Attacks on standard components used in the ICS network	Standard IT components (commercial off-the-shelf (COTS)) such as systems software, application servers or databases often contain flaws or vulnerabilities, which can be exploited by attackers. If these standard components are also used in the ICS network, the risk of a successful attack on the ICS network increases.
4.	(D)DoS attacks	(Distributed) Denial-of-Service attacks can impair network connections and essential resources and cause systems to fail – in order to disrupt the operation of an ICS, for instance.
5.	Human error and sabotage	Intentional deeds – whether by internal or external perpetrators – are a massive threat to all protection targets. Negligence and human error are also a great threat, especially in relation to the protection targets confidentiality and availability.
6.	Introducing malware via removable media and external hardware	The use of removable media and mobile IT components of external staff always entails great risk of malware infection. See the Stuxnet case, for example.
7.	Reading and writing news in the ICS network	Most control components currently use clear text protocols, so communication is unprotected. This makes it relatively easy to read and introduce control commands.
8.	Unauthorized access to resources	Internal perpetrators and subsequent attacks following initial external penetration have it especially easy if services and components in the process network do not utilize authentication and authorization methods or if the methods are insecure.
9.	Attacks on network components	Attackers can manipulate network components in order to carry out man-in-the-middle attacks or to make sniffing easier, for example.
10.	Technical malfunctions or force majeure	Outages resulting from extreme weather or technical malfunctions can occur at any time – risk and potential damage can only be minimized in such cases.

Source: Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, OSCE. 2013, <http://www.osce.org/ru/secretariat/110472?download=true>, last accessed on April 30, 2015.

Table 4: Major cyber espionage and sensitive data theft episodes in 1999-2014



The table above contains just a few examples of cyber espionage campaigns and attacks against CII involving the use of ICT.

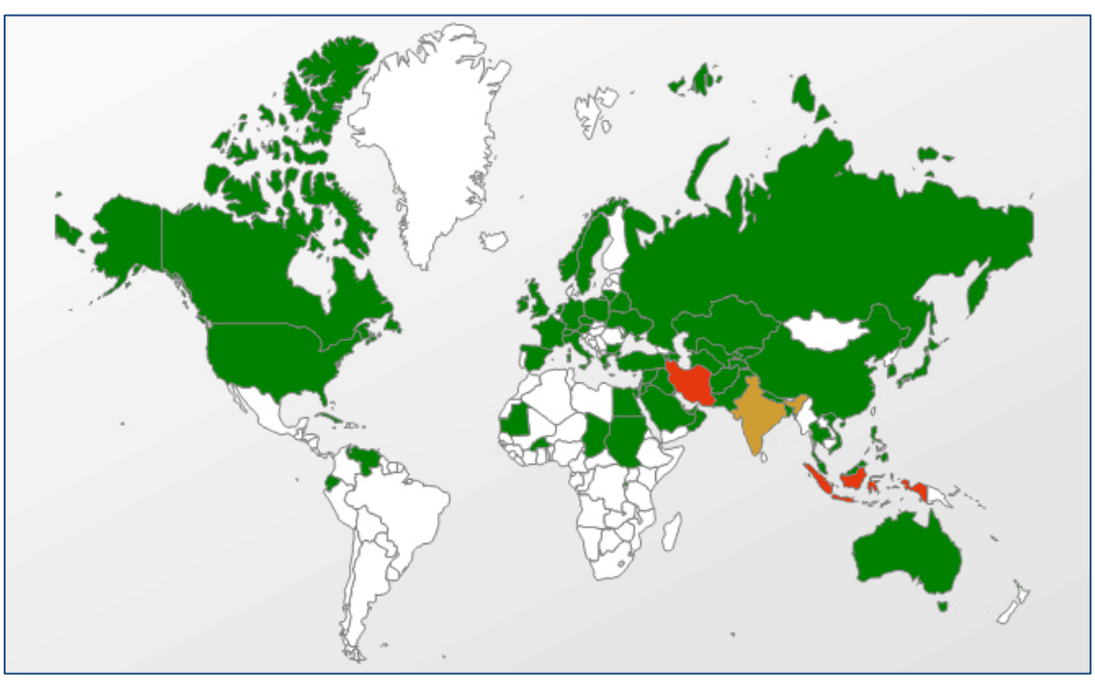
Disruption and sabotage of critical information infrastructure

Despite the menacing scale of cyber espionage against CII facilities, an even greater and more immediate threat is posed by the use of ICT with the purpose of interference with information systems of critical infrastructure facilities, including acts of sabotage targeting such facilities.

The best-known and the most serious incident involving a deliberate attack against CII is the use of the Stuxnet malware as an instrument of sabotage against Iran's uranium enrichment program at the Natanz facility in 2009-2010.

Stuxnet is the first precedent of malicious software being used to sabotage a strategic facility. Successful Stuxnet attack against the Natanz facility was unprecedented in terms of its complexity and sophistication. To make matters worse, the worm spread very rapidly all over the world after being released into the Internet in 2010. Tens of thousands of devices were infected. This did not cause any major incidents because the virus targeted only a specific model of a programmable logic controller (PLC). Nevertheless, the spread of Stuxnet over the Internet demonstrated that even the most sophisticated instruments of operations involving the use of ICT can get out of control and threaten a potentially unlimited number of targets.

Map 3: Geographic spread of the Stuxnet on the Internet in 2010



Source: Is Stuxnet a cyber weapon aimed at an Iranian nuclear site? UMBC Embuquity. 23.09.2010, <http://ebiquity.umbc.edu/blogger/2010/09/23/is-stuxnet-a-cyber-weapon-aimed-at-an-iranian-nuclear-site>, last accessed on April 30, 2015.

Looking at the Stuxnet incident, it is important to remember that the attack against the Natanz facility is not the only example of ICT being used to disrupt CII facilities, and that the range of potential ICT threats to such facilities is not limited to actions by state actors pursuing the objective of strategic sabotage. There have been numerous open-source reports in recent years about incidents involving interference with the work of CII facilities in various industries, including the nuclear industry.

- In 2003, the Slammer worm infected the Davis-Besse nuclear power plant in the United States. It spread from the externally connected network to the NPP's industrial control system and caused a disruption in the digital safety monitoring system. There was a duplicate analogue safety monitoring system, which enabled the plant's personnel to receive the necessary data for almost five hours after the failure, and thereby avoid serious consequences.

- A Trojan virus known as Shamoon is quite similar to the malware listed in Table 4. It was used to attack the infrastructure of oil companies in Saudi Arabia and, in all likelihood, Qatar. In August 2012 the virus may have infected up to 30,000 devices operated by the oil giant Saudi Aramco. In September 2012, a similar attack was mounted against the Qatari LNG company RasGas. Shamoon comes from the same malware family as the Flame virus, and uses a similar modular design. Nevertheless, according to a report by Kaspersky Lab, Shamoon was designed to destroy files on the infected systems rather than collect information. Saudi Aramco was forced to suspend its corporate network for 10 days to clean up the virus. Shamoon does not exactly qualify as an instrument of CII sabotage (because it did not actually infect any automated process control systems). Nevertheless, such an incident can disrupt the work of critical facilities.

The conclusions that can be drawn from the current picture of ICT threats to the security of critical information infrastructure are fairly grim:

1. Sabotage of strategic facilities, including facilities that can cause major man-made disasters, using ICT instruments is a real and present threat, from the technological point of view. What is more, several major actors, including governments, regard the prospect of mounting such attacks as politically acceptable under certain circumstances.
2. Even when there is a large number of pieces of indirect technical evidence pointing at the party that commissioned an attack against a CII facility, and even when such information is corroborated by independent sources (Edward Snowden, David Sanger), we still don't have any internationally agreed principles for the attribution of malicious acts involving the use of ICT. Neither do we have any agencies that monitor and investigate such incidents on behalf of the international community. As a result, the governments and the intermediary parties involved in mounting such attacks can essentially act with impunity, as far as international law is concerned.
3. Despite national security considerations, the states which operate critical infrastructure facilities that can potentially cause a man-made disaster will require easier access to best international practice and expertise in CII security, especially as the role of ICT in operating such facilities continues to grow. There are particular concerns about the developing countries that are building potentially hazardous facilities, such as nuclear power plants (India, Vietnam,

Iran, Turkey, Bangladesh, Pakistan), as well as the countries that have such plans for the near future (Algeria, Egypt, Indonesia, and others). If such countries come under an attack of Stuxnet-level complexity and sophistication, their own specialists may find themselves lacking the expertise to deal with the aftermath; Iran has been a case in point.

4. The Stuxnet attack posed no threat to Iran's Bushehr NPP. That does not mean, however, that such facilities cannot be sabotaged in the future. This new type and level of risk must be recognized and reflected in the policies and documents of the states that operate nuclear power plants and other potentially hazardous facilities (other nuclear fuel cycle facilities, dams of hydroelectric power plants, etc).

Many developing countries lack effective strategies for dealing with sophisticated ICT threats to CII facilities, and are facing a shortage of properly qualified specialists, expertise, and other resources. This, taken together with all the other factors outlined above, makes it necessary to pursue closer international cooperation in providing security of CII facilities.

Problems of international cooperation and recommendations for Russia and the international community

1. Given the limited prospects for international cooperation in protecting critical information infrastructure from ICT attacks, a more realistic objective would be to develop basic framework mechanisms for exchanging information about threats and security incidents at CII facilities.

More specifically, progress in these areas can be achieved through the following steps:

- The first step could come in the form of firmly putting the issue of protecting CII from ICT threats on the international agenda. In fact, that process has already begun at several venues, as far as cybersecurity of peaceful nuclear energy industry is concerned. For example, the need to counter the growing threat of cyber attacks against automated process control systems of CII facilities, including nuclear installations, is highlighted in the communiqué of the Nuclear Security Summit held in March 2014 in The Hague. The IAEA is also becoming more active. The first International Conference on Computer Security in a Nuclear World was held on June 1-5, 2015 in Vienna. The IAEA-organized event aims to set up a platform for a broad exchange of views on protecting nuclear industry facilities from ICT threats. One of the key issues in focus of the Conference – possibilities for a clearer and more effective role of the IAEA in pursuing closer international cooperation in this area.

  It would be useful for Russia and other countries to support these efforts and participate in these tracks. Similar calls have already been voiced by reputable expert organizations, including the East-West Institute (EWI) and others.

  Strong emphasis on the issues of cyber threats to CII infrastructure (including not limited to the nuclear industry) took place at the Global Conference on the Cyberspace (GCCS-2015), which was held in The Hague on April 16-17, 2015. Another useful venue is the international scientific forum "Partnership Among

State, Business Community and Civil Society in Ensuring Information Security, which is held every year in Garmisch-Partenkirchen, Germany. Finally, problems of CII security in the nuclear industry should be discussed at the IAEA general conferences.

- Since the IAEA already has a wealth of expertise in developing recommendations and practical measures in the area of cybersecurity at nuclear fuel cycle facilities, it would make sense, in the medium term, to formalize the agency's central role in the development and coordination of international cooperation in countering ICT threats to CII in the nuclear industry. In particular, the following measures could be discussed:
    - The formation, in the IAEA framework, of an international database of computer incidents at nuclear industry facilities. Information confidentially supplied to such a repository by member states, companies, Internet security experts, and nuclear industry facilities, could be used to develop recommendations and add to the agency's existing expertise in this area. Efforts to set up such a database could draw on the experience of similar mechanisms that already exist in the private sector, such as the Repository of Industrial Security Incidents (RISI).
    - If such a repository can be set up, the IAEA could function as a link between Internet security companies, teams of government experts, and states that are facing computer attacks against their nuclear industry CII and require help in countering and investigating such attacks. Taking the Stuxnet incident as an example, if such a mechanism had existed, Iran could have quickly turned to the IAEA (openly or confidentially) for information about similar incidents from the repository. Iran could also have requested assistance in stopping the attack and investigating it in an expeditious manner. Such assistance could be provided by the IAEA's own experts as well as Russian specialists from Kaspersky Lab. A voluntary and, where required, confidential nature of the parties' participation in such a mechanism could help to address the problem of the lack of confidence. Also, the global remit of the IAEA could give all of its member states access to such a mechanism, unlike the RISI or other existing databases.
    - Finally, in the medium term, the IAEA could launch and coordinate efforts to develop a framework agreement on the provision of CII security in the nuclear industry. Apart from creating incentives for states to develop proper regulation of these issues, such an agreement could facilitate a better use of the best practices and expertise accumulated by the IAEA as part of the project to create a repository of information about incidents at CII facilities in the nuclear industry. At this stage, however, it would be premature to discuss the specific contents of such an agreement or the possible time frame of its adoption.

- Beyond the IAEA, there are other venues that have the potential to strengthen international cooperation in protecting CII facilities from ICT threats. Nevertheless, it is the nuclear industry facilities (and possibly some other facilities that have the potential to cause a major man-made disaster) that are the most likely to become the launch pad for international efforts to improve

CII security. This view is supported by the fact that the international community has already realized the potential danger posed by such facilities, the fact that they are relatively few and easily identifiable, and the well-established practice of international regulation of their work (to which the IAEA has also contributed).

- There is also an area of work that cannot be easily arranged in the IAEA framework: namely, efforts to achieve greater mutual understanding at the international level with regard to the classification of CII and the inclusion of various types of facilities on the CII list. This measure is a necessary precondition for closer international dialogue on threat prevention in this field. A clear understanding of what types of facilities are regarded as CII by various foreign partners could become an important step towards mutual confidence-building measures and the prevention of crises related to cross-border incidents involving the use of ICT.

- Parties could make use of various formats of bilateral and multilateral consultation to exchange experience in the area of classification of CII facilities. As a next step in such cooperation, they could develop a joint system of CII facilities classification. These efforts could be based on the principle of eliminating those types/sectors where there is no consensus between the parties. For example, out of the 16 CI sectors defined by the United States, 28 by Switzerland, and 50 classes (contained within seven types of threats) defined by Russia, the final list could include 10-12 categories that are shared by all three national classifications.

- The overall goal of these efforts should be the adoption of a uniform open list of CII types, along with instruments for their classification. Such a list could be limited to nuclear industry CII facilities, or it could include the CII of other potentially hazardous facilities and other CII types/sectors. The availability of a shared system of CII classification would facilitate the development of bilateral and multilateral confidence-building measures on security issues in the use of ICT. In particular, it would help to establish a system of early warning about attacks against critical facilities in other countries, in accordance with agreements on confidence-building measures.

  Besides, the availability of a uniform list of CII types and of a system for their classification could serve as a starting point for negotiating international agreements that would ban attacks on some specific types of facilities on that list. In particular, the parties could try to negotiate the already mentioned framework agreement on CII security in the nuclear industry, using the IAEA as a platform.

  It would be useful to involve the UN Group of Governmental Experts on information and telecommunications in drawing up such agreements. The third composition of the GGE, which was convened in 2013, has already begun to discuss CII security issues. The fourth composition will continue these discussions in 2015 (for more details, see Section 5).

We believe that practical progress in resolving these problems could be achieved in 2020, provided that Russia is actively involve

Particular recommendations on that regard might include:

1. To compile, at an international level, an open-ended uniform list of CII facilities and a system of their classification for use in the development of confidence-building measures in the area of the use of ICT.
2. To develop a framework agreement on CII security in the nuclear industry (probably via IAEA mechanisms).

Documents:

1. Project of the Federal Law "On security of critical information infrastructure of the Russian Federation" (submitted by the FSB on August 8, 2013), Government portal for information on the elaboration of legislation and regulations by federal executive bodies of the Russian Federation, August 8, 2013, <http://regulation.gov.ru/project/5890.html?point=view_project&stage=2&stage_id=2938>, last accessed on April 30, 2015.

2. Fundamentals of government policy on security of automated industrial and process control systems at critical infrastructure facilities in the Russian Federation, Approved by President Dmitry Medvedev on February 3, 2012, No 803, Security Council of the Russian Federation, <http://www.scrf.gov.ru/documents/6/113.html>, last accessed on April 30, 2015.

IV. Military and Political use of ICTs: Challenges to Global Security and International Law

Attempts at liberal interpretations of the existing international legal norms in order to justify what are essentially acts of aggression involving the use of ICT are unacceptable. Speaking of the agreements that regulate conduct during military conflicts, we are talking about a whole branch of international law that includes conventions developed back in the late 19th and early 20th century, in the late 1940s, and in the 1970s. Are all the norms stipulated back then capable of reflecting the specifics of cyberspace?

Alexander Zmeevsky, Special Representative of the President
of the Russian Federation for International Cooperation
in the Fight against Terrorism and Cross-Border Organized Crime

Cyber weapons, cyberwars, and threats that exist in cyberspace must be properly countered, condemned, banned, and punished. In particular, there must be a ban on using cyber weapons in the Internet, preferably a UN-level ban. Unless this is achieved, all our networks and devices will become fertile ground for further development and spread of such weapons.

Andrey Yarnikh, Head of Strategic Projects at Kaspersky Lab

Growing potential for use of ICT for military and political purposes

It is now safe to say that the rise of ICT as an integral component of national defense capability, military doctrines, and infrastructure, has essentially become irreversible in the leading global powers. This trend has several aspects (see Table 5).

Technologically advanced countries have developed a comprehensive financial and infrastructural capability and expertise to use ICT for military-political purposes. In view of the evolution of malicious software; growing threats to critical infrastructure; increasing dependence of all the key sectors or the global and national economy, governance, and security on ICT; and other trends analyzed in Sections 1-5, it is safe to say that in the developed countries, the potential to achieve the goals of the conflict using ICT is approaching the potential of kinetic weapons and even WMD.

Also, the military ICT potential is increasingly being formalized in state policies and doctrines. In most cases, these policies and doctrines stipulate (or at least fail to rule out) the need for preemptive operations in information networks. In the absence of any restraining factors of international law, we are witnessing an erosion of an unspoken principle that came into being after World War II and the adoption of the UN Charter – namely, the principle that by default, state activity in the military-political sphere pursues only *defensive* goals, and is limited to self-defense.

Table 5: Rise of the military and political agenda in the use of ICTs

	State/int. organization	Use of ICT for defense and other military goals in doctrines and legislation	Formation of structural, organizational, financial, and HR base of ICT defense potential	Development by states of a technological base to strengthen ICT defense potential
1.	**Britain**	1. In September 2013 the UK MoD announced plans to set up the Joint Cyber Reserve. The new outfit is to support the Joint Cyber Unit by helping the British military to develop a full range of operational capability in the IT operations sphere, including preemptive strike operations.	1. In 2013 the UK announced plans to recruit several hundred IT specialists to the Joint Cyber Reserve starting from October 2013. The budget of the new outfit was estimated at $808milion.	
2.	**Germany**		1. In 2011 Germany set up the National Cyber Defense Center, which pools the information security and defense resources of several federal agencies, including the Armed Forces and the Federal Office for Information Security. The job of the new center is to defend Germany's state information networks from ICT attacks.	
3.	**China**		1. According to the U.S. government and the Mandiant company, the structure of the PLA has included Unit 61398, also known as Advanced Persistent Threat 1, since at least 2006. The outfit conducts pro-active operations in the information networks of other countries, especially the United States. It has up to 2,000 people on its payroll, and operates more than 1,000 servers.	
4.	**Russia**	In 2013-2014 it was announced that Russia would set up an equivalent of the U.S. Cyber Command at the General Staff of its Armed Forces by the end of 2014.		1. On October 17, 2012 the Russian MoD announced contracts for R&D projects in several areas, including "Methods and instruments of

		Presumably this will be a separate new armed service, which will be given the status of a Main Department within the Russian MoD at the early phase.		circumvention of anti-virus systems, network security, and OS security systems". The project includes the development of software to defeat the adversary's IT security systems.
5.	**USA**	1. The U.S. International Strategy for Cyberspace (May 2011) asserts the principle of regarding cyberspace as a space for operations by the U.S. Armed Forces, i.e. another battlefield, along with sea, air, land, and outer space. 2. In November 2011 the Pentagon reiterated the right, claimed in the above Strategy, to use "all necessary means", including military ones, for "defense from cyber threats", equating cyber attacks to an armed attack. This set an international precedent of a nation claiming the right to respond asymmetrically to ICT threats, using the entire range of available weapons.	1. The U.S. CYBERCOM was set up on June 23, 2009. It merged the cyber defense resources and units of the Air Force, the Navy, and the Army (the U.S. Navy Cyber Command (10th Fleet), the 24th Air Army, the Cyber Command of the U.S. Army, and others). The U.S. CYBERCOM protects the ICT infrastructure of the U.S. Armed Forces. It conducts operations, including offensive ones, in cyberspace, and is subordinated to the Strategic Command of the U.S. Armed Forces as a coordinating center for Armed Forces operations involving the use of ICT. 2. According to the information disclosed by Edward Snowden, the financing of operations in foreign information networks by the NSA and other agencies, including the U.S. CYBERCOM, stood at 4.3 billion in 2013. According to the same source, in 2011 these agencies conducted 231 pro-active operations, whose goals included "preventing the proliferation of nuclear weapons". Some $447 million was to be spent on CYBERCOM in 2014, a 130-per-cent increase compared to the previous year's figure of $191 million. One of the key spending items is hiring additional personnel to bring the total number to 1,800 in 2015 and 6,000 in 2018.	1. In August 2014 it was reported that the NSA was developing and using the Monstermind software as an instrument of proactive defense on the Internet. The software can automatically recognize and defend against cyber attacks, and take proactive action without human involvement, such as obtaining access to data on the control servers used to wage an attack, by overcoming their defenses. 2. The development of the Stuxnet virus that infected Iran's uranium enrichment facilities is seen as an element of a large program called Olympic Games. That program was active from 2007 until 2012, if not longer. It involved specialists of the U.S. CYBERCOM. In particular, they took part in developing software for sabotaging strategic facilities. The Olympic Games program is also though to have included the development of many other pieces of sophisticated malware found in the Middle East in 2011-2014 (Flame, Mini-Flame, Gauss, and DuQu.)

			3. The Pentagon's total spending on cybersecurity and cyber defense has increased to $5 billion in the 2015 budget, whereas spending on many other defense items was slashed.	
6.	**France**	The White Paper released by the French MoD in April 2013 states that if an information attack threatens France's strategic national interests, the countermeasures may include all available resources, including those of the MoD. To that end, the national cyber defense strategy includes offensive operations in cyberspace and intelligence gathering.	1. In January 2014 France's defense minister, Jean-Yves Le Drian, announced plans for the launch of a 2bn-dollar program to strengthen the national cyber defenses. The program includes a two-fold increase in the number of cyber defense personnel at the MoD to 450 people. Some of that increase will be achieved by launching a Cyber Crisis Management Master's course at the MoD in 2015.	
7.	**NATO**	1. Effective cyber defense was mentioned as one of the main requirements for NATO security in the organization's new Strategic Concept released in 2010. 2. At the September 4-5, 2014 NATO summit in Wales, the organization adopted a new Enhanced Cyberdefense Doctrine, which regards cyber attacks as one of the key security threats faced by the alliance. 3. The NATO summit in Wales also adopted a statement that an attack in cyberspace against NATO members can in some cases be regarded as grounds to invoke Article 5 of the NATO Treaty (the right to use the collective defense mechanism beyond cyberspace).	1. In 2008, a year after a protracted wave of attacks against Estonia's ICT infrastructure (in which Russia was suspected as the main culprit), NATO set up the Cooperative Cyber Defense Center of Excellence (CCD COE) in Tallinn. The center focuses on researching the use of ICT for military-defense purposes from the legal and strategic point of view, capability-building, and sharing expertise.	

This is resulting in a gradual transformation of the international security landscape, and a reassessment of the risks and threats in that sphere by all members of the international community. Using the asymmetric nature of the military potential of ICT, the less developed countries are also gradually being drawn into the digital *arms race* in the hope of obtaining their own advantages in that sphere and negating the threats posed by the more digitally advanced countries. According to Andrey Krutskikh, Special representative of the President of Russia for international cooperation in the field of information security, over 130 nation states were experimenting with programs of developing "information weapons" in 2013.

It is also worth highlighting the unresolved problem with identification of actors behind cyberattacks and with reliable attribution of such attacks. The technological complexity of attribution in cyberspace, coupled with the new doctrines of proactive defense in the ICT-enabled environment, could well trigger or exacerbate international conflicts.

- Attacks on Estonian infrastructure in 2007, Georgian government and private sector networks in 2008, and U.S. financial institutions and private sector companies in the spring of 2014 (the Energetic Bear campaign and the Dragonfly malware) have persistently been attributed to Russia by several countries, including NATO members, even though there is lack of reliable technical evidence that could prove such an attribution. Although national CERT in Estonia was established in 2006, by the moment of cyber attacks in 2007 it still lacked technical capabilities and qualifications to trace back the attacks to the C&C servers and identify the origination paths. As a result, no technical report of cyber incidents of 2007 was ever provided by Estonian CERT.
- In the event of a lighting-fast cyber-attack that imitates the "signature" of Russian perpetrators (for example, Cyrillic code fragments and other linguistic patterns) and targets the infrastructure of NATO countries using servers in Russian territory, there is a risk of a NATO military retaliation against Russia. In accordance with the NATO doctrine, retaliatory measures may include the use of kinetic weapons and the involvement of all NATO members in a retaliatory strike. In theory, such a development could generate a risk of an international conflict between nuclear-weapon states breaking out. One of the key factors in that risk is that attacks in the ICT environment cannot be accurately attributed in the short space of time that will be available to decision-makers when their countries' critical infrastructure is threatened.

Therefore, one potential **t**hreat for the middle-term perspective is breakout of international conflicts as an outcome of hostile activities in information networks, as well as the use of kinetic weapons in response to such operations by 2020.

Adaptation of the international law to new ICT-driven military-political challenges

The key problem in the current situation is the lack of international mechanisms for preventing and containing the aforementioned conflicts. The current system of international law is not adapted to the challenges and threats posed by the use of ICT for military-political purposes.

The key unresolved issues in this area are:

- The use of ICT for military and defense purposes is not covered by any of the existing international treaties, agreements, or conventions. Approximate equivalents in other areas include the international agreements that regulate the development and use of WMD (the 1967 Nuclear Weapons Non-Proliferation Treaty, the 1993 Chemical Weapons Convention Treaty, the 1972 Biological and Toxin Weapons Convention, and others); agreements on the limitation of some types of weapons (the 1987 Intermediate-Range and Shorter-Range Nuclear Forces Treaty and the three successive START treaties); and agreements on conventional weapons (the 1990 Conventional Forces in Europe treaty and the 1983 Inhumane Weapons Convention).
- As a result, there are no international organizations charged with the supervision and monitoring of national activities regarding the use of ICT for military-political purposes, or with verification of compliance with any restrictions and limitations in that area. Even though the idea of an "IAEA for cyberspace" has repeatedly been voiced by representatives of various countries and organizations (including E.V. Kaspersky, head of Kaspersky Lab), there has been no tangible progress on this front.
- One of the worst problems is the fact that even the existing body of international laws that regulate conflicts and wars, regardless of the types of weapons being used, cannot be used by default in the ICT sphere because of that sphere's technological peculiarities. We are talking about the norms of international humanitarian law (*jus in bello*) and the rules of armed conflict (*jus ad bellum*) incorporated in such acts as the 1899 and 1907 Hague Conventions, the 1928 Geneva Convention, the I-IV Geneva Conventions of 1949, and the I-III Additional Protocols of 1977, 1997, and 2005 to the I-IV Geneva Conventions. Applying these documents to the use of ICT for military-political purposes would require their uniform and legally binding international interpretation. In view of the aforementioned negative international security trends (i.e. the growing military-political potential of ICT), developing such uniform interpretations should be regarded as an important priority for the international community in the near term.

The ongoing international discussion on these issues pursues two different approaches:

1. Recognition of the sufficiency of the existing body of international law (especially *jus in bello* and *jus ad bellum*) for regulating the use of ICT for military-political purposes, provided that these laws are properly interpreted and adapted to the specifics of the ICT environment. Such an approach rejects the need for developing and adopting any new legally binding international agreements in this area.

This approach was adopted by the project led by a group of experts from NATO countries in 2011-2013 at the CCD COE center in Tallinn. The project produced the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, which was released in the spring of 2013. Even though this was originally an unofficial document, the decisions adopted at the NATO summit in Wales essentially reflect all of its key conclusions, thereby institutionalizing the proposals made by CCD COE experts.

Some of the key conclusions made in the Tallinn Manual are as follows:

- Recognition of the responsibility of states for actions perpetrated in cyberspace by their proxies;
- Applicability of the international legal ban on the use of force to cyber operations. In the absence of any official definitions, the criterion by which the use of force is judged is the infliction of damage to health or property as a result of cyber operations;
- If a state conducts cyber operations in foreign networks, it becomes a legitimate target for retaliatory operations in its own networks;
- A state that has become a victim of an armed attack involving the use of ICT has the right to retaliate by using force, including ICT instruments and kinetic weapons. An armed attack is defined as actions that have resulted in the loss of life or major destruction;
- A conflict that unfolds strictly in the ICT environment can, under certain circumstances, be recognized as an armed conflict using the terminology of international humanitarian law. As a result, some categories of the participants in that conflict become combatants;
- If civilians are involved in conducting cyber operations during a conflict that involves the use of ICT, these civilians become legitimate targets for retaliatory measures.

The key distinctive feature of this approach is that it does not aim to ban the use of ICT for military-political purposes. It merely helps to produce a set of rules for such activities in accordance with the body of international humanitarian law and the laws of armed conflict.

2. The alternative approach is based on the notion that the emergence of the new technological reality and sphere of relations in the ICT environment requires major innovations in the international law. That includes development of legally binding international norms that specifically regulate the ICT sphere, in addition to the existing international laws, including *jus in bello* and *jus ad bellum*. One of the solutions being proposed is the adoption of a global treaty or a UN convention that would impose an international ban on the use of ICT for military-political purposes.

Russia, which is the main proponent of this approach, has undertaken practical steps towards drawing up such a document. It presented its own draft Concept of a UN Convention on International Information Security at a meeting of senior international security officials held in Yekaterinburg on September 21-22, 2011. The draft concept incorporates all the main principles of the Russian approach, including those related to countering military-political threats in the sphere of ICT use.

Article 6 of the Concept lists several key measures to prevent armed conflicts in the information space:

- All parties must desist from the use of force or threats of force against the information space of other countries;
- Each state must make all possible efforts to prevent the use of its territory or infrastructure for illicit action involving the use of ICT;
- All parties must refrain from developing and adopting doctrines that could potentially trigger the rise of threats in the information space and the breakout of “information wars” ;

- All parties must adopt measures to limit the spread of "information weapons" and technologies of making such weapons.

The document met with a fairly critical response from Russia's Western partners, who argued that it represents an attempt to "curtail rights and freedoms on the Internet". Nevertheless, the measures it proposes represent a clear set of goals for Russia and other proponents of the approach that calls for a reform of international law in order to neutralize the threats related to the use of ICT for military-political goals.

After comparing these two different approaches, the following conclusions can be drawn:

1. In theory, it is possible to develop adequate interpretations of the existing norms of international humanitarian law and the laws of armed conflict, as proposed by the NATO approach. Nevertheless, such an approach contains no proposals for developing a system of international mechanisms that would prevent conflicts in the area of ICT. As already mentioned, the ICT sphere lacks the equivalent of the mechanisms that act as a safety net and augment international humanitarian law in the area of preventing and containing conflicts involving the use of kinetic weapons (such as confidence-building measures; treaties that limit or ban some types of weapons; control, monitoring, and verification mechanisms; arms reduction agreements, etc.). The efficiency and adequacy of the norms of international humanitarian law in terms of keeping peace and preventing conflicts cannot be assessed without taking into account these "special" mechanisms, because the international security regime is a holistic system. As a result, in the absence of initiatives and norms that specifically target the ICT sphere, efforts to promote and adopt at the national level any policies that aim to adapt the norms of international humanitarian law would be premature and potentially pose international security risks.

2. At the same time, norms of international humanitarian law are a necessary element of any future regime of global security in the area of ICT use. It is important, however, that possibilities for a proper adaptation of these norms should be explored in global rather than regional formats. The danger of duplicate efforts in this area at various regional platforms is that they can lead to the emergence of numerous different interpretations of the same global norms of international humanitarian law. Practical consequences of such differences would include conflicting interpretations by different parties of the legitimacy of each other's actions. That could potentially trigger an uncontrolled escalation of conflict, possibly beyond the use of ICT.

3. Progress towards the adoption of a legally binding international agreement to ban and prevent the use of ICT for military-political purposes would be difficult as long as the problem of attribution remains unresolved. Discussing any norms that cannot be enforced though mechanisms of verification, control, and identification of those responsible for their violation, could devalue the very idea of adopting such a document. Nevertheless, as we make progress towards resolving the problem of attribution, the goal of developing and adopting that document will become increasingly relevant.

4. Resolving the problem of attribution requires active cooperation between state representatives and the technical community. Given that the bulk of the threats in the area of ICT require the use of the Internet, it would be useful to set up a new platform for technical work and dialogue on the issue of attribution. That new platform should bring together representatives of states and experts of the Internet's technical organizations, including the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the IESG, and others. This effort would be a new step towards resolving the attribution problem. It would also help to involve a broader range of specialists, including engineers of the global network, in identifying a solution to this problem.

5. To avoid an unnecessary politicization of efforts to develop an acceptable approach to the regulation of the military-political aspect of the use of ICT, this discussion should be moved to a neutral international venue. Such a venue already exists: it is the UN Group of Governmental Experts (UN GGE) on developments in the area of IT and telecommunications. That group, which includes representatives from Russia and NATO countries, has been working on this problem since 2013 (see Insert No 6).

The GGE conclusions regarding the application of the norms of international law to the use of ICT were released in a 2013 report, which included the following key points:

- International law, including in particular the UN Charter, is applicable to and necessary for maintaining peace and security in the field of use of the ICTs;
- State sovereignty and related international laws and principles are applicable to state-led activities that involve the use of ICTs;
- States must not use proxy actors to conduct activities that violate international law, including actions involving the use of ICT; states must strive to prevent their territory from being used by proxies to commit illegal actions involving the use of ICT.

The value of the GGE format comes (among other things) from its use of the UN platform. The UN is the only international organization whose decisions have a global scope and an undisputed global legitimacy authority. Further promotion of GGE conclusions and recommendations could potentially provide a basis for negotiating a legally binding international document that regulates the conduct of states in the area of ICT use.

In the context of the conclusions drawn by the UN GGE, it is especially important to recognize the applicability of the UN Charter to actions involving the use of ICT – but there are also some unresolved problems in this area. One of the most serious of these problems is the absence of any criteria by which actions involving the use if ICT would qualify as an act of aggression or an armed attack under article 51 of the UN Charter.

Even though the UN Charter does not have a definition of "aggression", there is a detailed interpretation of that term in UN General Assembly Resolution A/RES/29/3314 of December 14, 1974. That document lists seven types of actions that can qualify as an act of aggression "regardless of whether a declaration of war has been made". Unfortunately, when it was adopted back in 1974, it could not take into account future actions involving the use of ICT.

UN Group of Governmental Experts for Developments in the Field of Information and Telecommunications

- The group was established on the basis of a Russian initiative proposed in September 1998, when Russian Foreign Minister Sergei Ivanov sent a letter to the UN Secretary-General containing a draft UN GA resolution headlined "Developments in the area of information and telecommunications". In December 1998 the resolution was submitted to the First Committee of the UN General Assembly and approved without a vote (A/RES/53/70). One of its paragraphs called on all UN members to express their views on ICT-related security issues. The UN General Assembly has been passing such resolutions every year since 1998.
- In December 2001 Russia proposed an initiative to set up the UN GGE in order to discuss existing and possible threats in the area of ICT and possible cooperation measures, as well as to study key challenges in that area. The first GGE, which included representatives from Russia, the United States, and 13 other countries, held a series of meetings in 2004 and prepared a formal report (there were major differences on some key issues). Nevertheless, the participants expressed an interest in taking the GGE project further. As a result, the second and the third GGEs held series of meetings in 2009 and 2013, respectively. Both groups produced substantive reports.
- The fourth GGE was arranged and started to conduct its meetings in the second half of 2014 on the basis of UN GA Resolution A/RES/68/243 of December 27, 2013. The work of the 4th GGE is focused on detailed study of the possibilities of the application of international law in the field of the use of ICT and conduct of states in cyberspace. The Group has been extended to 20 governmental experts; it is expected that the Group will elaborate a consensus-based Report of the Secretary General that will be presented in 2015. The report should shed light upon concrete issues and disagreements existing with regard to the issue of application of international law to cyberspace. Those include feasibility of reliable attribution of cyberattack initiators, differentiation between combatants and non-combatants in cyberspace; recognition of cyber attacks as use of force if falling under certain criteria, legitimacy of kinetic response to cyberattacks posing threats to national sovereignty and defense capacity, etc.

As a result, when the terms "aggression" and "armed attack" are used in the policy documents and doctrines of states and regional organizations in the context of ICT use, the definitions and interpretations of these terms cannot be referenced with any universally recognized source of international law, and are left for each individual actor to interpret on their own.

It is therefore necessary, first, to update the text of the UN General Assembly resolution, and amend it with a paragraph that describes the actions involving the use of ICT that qualify as an act of aggression. As an alternative, states could produce a consensus interpretation, with regard to the use of ICT, of Paragraph (g) of the aforementioned UN GA Resolution 3314 of December 14, 1974.

Resolution 3314 is also relevant to another potential area of strengthening the international legal regime of state responsibility for the use of ICT. We are talking about enlarging the scope of the International Criminal Court's jurisdiction to include

actions involving the use of ICT that represent a threat to international security, including those covered by the definition of the crime of aggression.

The ICC's right to exercise jurisdiction with regard to the crime of aggression was approved when states adopted the Rome Statute of the ICC in 1998, but the issue of actually exercising that jurisdiction has yet to be finally resolved. Article 5 of the Rome Statute lists the crime of aggression among the crimes that fall under the ICC's jurisdiction, and the definition of aggression incorporated in the Statute was borrowed from UN GA Resolution 3314. As a result, it would be possible to amend the definition in the Statute by including aggression involving the use of ICT, if the same amendment is made to the text of the UN GA Resolution.

Nevertheless, the ICC has not yet begun to exercise jurisdiction with regard to the crime of aggression because the process of incorporating that crime into the Rome Statute is not yet complete. Progress towards resolving this issue has been made over the past several years. The ICC's right to investigate crimes of aggression and prosecute those charged with that crime was reiterated during the First Review Conference of ICC member states in 2010. It was also noted, however, that the ICC would be able to start exercising its jurisdiction over this crime only after a positive decision has been made on this issue by the Assembly of ICC State Parties, and that decision can be made on January 1, 2017 at the very earliest.

To reiterate, the ICC will not be able to begin exercising jurisdiction over the crime of aggression before 2017 or possibly an even later date.

Nevertheless, it would make sense to explore the possibility of updating the definition of aggression (to include the use of ICT) in the framework of the ICC and Resolution 3314. Even though the practical usefulness of ICC mechanisms is not great at the moment, the ICC format also has its advantages:

- Unlike the UN GA resolution, ICC rulings are legally binding for the 122 states that have ratified the Rome Statute.
- An ICC ruling or even the initiation of an ICC investigation on suspicion of an act of aggression involving the use of ICT would set an important precedent that would essentially formalize the nature of actions involving the use of ICT and qualified as an act of aggression.

Additional information:

1. A War in Cyberspace: Lessons and Conclusions for Russia, Round table at the editorial office of "Nezavisimoye Voennoye Obozreniye", NVO, No 46, 13.12.2013, <http://nvo.ng.ru/concepts/2013-04-26/1_war.html>, last accessed on April 30, 2015.
2. Chernenko Elena. A Virtual Front. Kommersant Vlast, No 20 (1025), 27.05.2013, <http://www.kommersant.ru/vlast/74525>, last accessed on April 30, 2015.
3. Interview with Oleg Martyanov, member of the Russian government's Military Industrial Commission, and Igor Denisov, deputy head of the FPI, by Ekho Moskvy radio, 02.09.2014, <http://fpi.gov.ru/press/media/intervyyu_chlena_boenno_promishlennoy_komissii_pri_pravitelystve_rf_olega_martyyanova_i_zamestitelya_direktora_fpi_igorya_denisova_radiostantsii_jeho_moskvi>, last accessed on April 30, 2015.

Documents:

1. Conceptual views of the activity of the Russian Armed Forces in the information space. Russian MoD, 2012,
<http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle>,
last accessed on April 30, 2015.
2. Resolution adopted by the General Assembly 3314 (XXIX), Definition of Aggression, A/RES/29/3314, General Assembly of the United Nations, A/RES/29/3314, <http://www.un-documents.net/a29r3314.htm>, last accessed on April 30, 2015.
3. Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations Office for Disarmament Affairs, < http://www.un.org/disarmament/topics/informationsecurity/>, last accessed on April 30, 2015.
.

V. Global Internet Governance: Legal and Policy Aspects

Institutional Architecture of global Internet governance

The Internet governance system, whose key functional, structural, and institutional aspects emerged in the 1990s and 2000s, continues to evolve at a rapid pace. From the technical point of view, the evolution of the Internet architecture and the system of Internet governance is still based on a set of fundamental principles outlined in a document called RFC 1958 (the so-called Architectural Principles of the Internet).

Functionally, the Internet is governed by various participants; the exact list of those participants varies depending on the scope of their activities (global, regional, national, or local). At this time, the central role in Internet governance is played by a historically evolved model called multistakeholder Internet governance.

Multistakeholder Internet governance

- Lack of official definition of Internet governance.

Usage in international practice:

- Geneva stage (2003) and Tunis stage (2005) of the World Summit on Information Society (WSIS) (held in accordance with UN GA Resolution 56/183).
- Conclusions of the Working Group on Internet Governance at the UN General Secretariat (set up in 2004 in the run-up to the Tunis stage of the WSIS, consisted of experts from over 40 countries).

Key stakeholders:

1. governments;
2. private sector;
3. civil society institutions (including nongovernmental and non-commercial organizations, Internet user groups);
4. included at a later stage: academia representatives
5. community of Internet users (ICANN ALAC, etc.)

Decision-making mechanism:

The position of governments is not prioritized when making decisions; all stakeholders have equal status and their positions are taken into account on equal footing.

The development of international Internet governance practices in the general vein of this model highlights the preeminent role of various technical community organizations that came into being at the very early days of the Internet in the 1980s and 1990s. Table 6 lists the main participants of the global process of Internet governance.

Table 6: Major technical organizations of the global Internet community

	Organization	Description and function	Status
1.	Internet Society (ISOC)	Alongside with ICANN, the Internet Society is one of most widely represented and influential technical community structures. It facilitates open development of standards, administration protocols, and technical infrastructure of the Internet. ISOC is not producing technical standards itself, but serves as a supporting framework and a vehicle to IETF activities and debates, promoting its standardization agenda. ISOC also facilitates elaboration of national and global policies to support growth and improvement of the Internet all over the world. The following working formats benefit from coordination of their activities with ISOC: the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF), the Internet Engineering Steering Group (IESG), the Internet Research Steering Group (IRSG), and the Request for Comments (RFC) Editor.	ISOC is a not-for-profit corporation registered in District Columbia, United States. Its organizational structure is based on the membership principle. Its activities are financed mainly from contributions by members (individuals and legal entities). ISOC holds the rights to all RFC documents.
2.	Internet Architecture Board (IAB)	The IAB conducts its activities under the ISOC auspices. On the authority of ISOC, it oversees issues related to the Internet architecture, including protocols and other technical standards. The IAB consults ISOC Board of Trustees on issues related to the Internet architecture. It also acts as a technical body for liaison on behalf of ISOC. The IAB coordinates the work of the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRFT). It serves as the IRTF Committee for technical issues.	The IAB is not a legal entity but a technical coordination body (committee).
3.	Internet Engineering Task Force (IETF)	The Internet *Engineering Task Force* (IETF) is neither an organization nor legal entity at all. It can be described as a largely volunteer working process bringing together the technical community. However, for many years the IETF has been the central work stream for standardization of the Internet's protocols and technical parameters of the DNS, IP resource allocation and other issues related to the Internet's UIS. Within the IETF structure, over 120 Working Groups (WGs) exist. The IETF WGs provide contribution to SSR-related discussions and standardization efforts to the majority of the technical community structures, including ICANN and IANA, NRO, ASO and RIRs, IAB, and others.	The IETF is not a legal entity, so it has no nor formalized corporate structure and is not under any national jurisdiction. Although an established structure of the Working Groups exists, IETF does not have approved corporate budget. The IETF meetings take place three times a year in different locations.

		The IETF functions include: • Developing specifications, standards, and agreements on the general architectural principles of Internet protocols • Developing recommendations on the standardization of protocols and their submission for IESG consideration • Facilitating the spread of technologies and standards developed by the Internet Research Task Force (IRTF). • Major mechanism for the IETF work on standardization are Request for Comments (RFCs) which are published online and usually provide general technical description of the discussed systems or standards. RFCs do not have legal power, but they constitute the key consensus format with regard to standardization of protocols and parameters on the Internet for technical community, private sector and other stakeholders.	
4.	Internet Corporation for Assigned Names and Numbers (ICANN)	ICANN is one of the central structures of global technical community; it was established in 1998 in order to globally coordinate the Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems. According to ICANN Bylaws its coordination function comprises three different areas; in particular, ICAN: 1. Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are a. Domain names (forming a system referred to as "DNS"); b. Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and c. Protocol port and parameter numbers. 2. Coordinates the operation and evolution of the DNS root name server system. 3. Coordinates policy development reasonably and appropriately related to these technical functions. ICANN establishes and contributes to development of collaboration frameworks with nearly existing bodies and working processes across the global technical community. This includes cooperation with IETF and IAB (see ICANN-IETF MoU and Supplementary Agreements), RIRs (through ASO and NRO frameworks), W3C, ISOC, etc. ICANN performs the role of a major discussion framework for all policies	ICANN was established as a non-commercial corporation registered in California, USA. The scope of ICANN responsibilities is largely defined by its formalized relationships with the U.S. Government.

		and issues related to standardization and development of the Internet's global infrastructure and its management model. ICANN provides the platform for and is the formal founder of the DNS Root Server System Advisory Committee (RSSAC) – an informal interface for communication between ICANN and the DNS Root Name Server operators' community.	
5.	Internet Assigned Numbers Authority (IANA)	The Internet Assigned Numbers Authority (IANA) is a technical department of ICANN, which is responsible for support of operation of specific functions related to DNS and the Internet's UIS. These functions include: • coordination of assigning technical protocol parameters, on which the Internet works; • administration of the DNS root zone file and several other functions related to the DNS root server system; • proper delegation and distribution of Internet resource addresses - high level domain names and IP address blocks; • management of the top level domain ".int" (reserved for intergovernmental organizations) and the top level domain".arpa" (reserved for special technical usage related to maintaining the DNS system's functionality). Starting from March 12, 2014 the IANA Oversight Transition process was launched by the USG	IANA is not a separate legal entity. Instead, it is a technical department within ICANN corporate structure. IANA was included into ICANN structure when ICANN was established in 1998. Since ever, the Internet Corporation was a Party to the Contract with USG (represented by DOC) for performance of IANA function. Latest Contract was signed in September 2012 and expires on September 30, 2015. This date serves as a final deadline for the proposed IANA Oversight Transition process as for April 30, 2015.
6.	World Wide Web Consortium (W3C)	Development, optimization, and facilitation of the implementation of Internet protocol standards. W3C serves as the organization for the standardization of Internet protocols. While W3C develops specific standards such as Open Web Platform for application development (CSS, SVG, WOFF, the Semantic Web stack, XML etc.).	W3C is a not-for-profit association. It was jointly founded by the CSAIL laboratory of the MIT and the European Research Consortium for Informatics and Mathematics (ERCIM).
7.	Regional Internet Registries (RIRs), ASO and NRO	Regional Internet Registries (RIRs) manage the allocation and registration of Internet number resources, which are delegated to them by IANA. Today, there are five regional RIRs that together are components of the Internet Number Registry System described in IETF RFC 7020[5]. Those include APNIC, LACNIC, RIPE NCC, ARIN and AfriNIC, which are	RIRs need a collaboration framework. With regard to IP addresses issues, such framework was initially presented by the Address Supporting Organization (ASO), which was established

[5] The Internet Numbers Registry System, Request for CommentsL 7020, Internet Engineering Task Force, August 2013, <https://tools.ietf.org/html/rfc7020>, last accessed on April 30, 2015.

		loosely based on a geographic principle and altogether cover the world's regions and continents except Antarctica. From a legal viewpoint, RIRs are not-for-profit non-incorporated associations conducting their activities within particular regions, though their membership criteria might not necessarily imply geographic restrictions (as in the cases of APNIC and RIPE NCC). RIRs play the key role in distribution of the Internet's Number Resources, including IP addresses and ASNs. Large stacks of IP addresses (from 2011 and on they are IPv6 addresses), as well as blocks of 1024 ASNs are delegated to RIRs by IANA as a part of its functions. IP and ASNs delegation process and decisions are based on the technical requirements to RIRs, reports from RIRs to ICANN, and, in case of newly established RIRs, on their technical compliance and eligibility criteria. After receiving the Number Resources from IANA, RIRs are largely free to distribute them among ISPs and other organizations according to the policies and procedures that they establish and follow. This is a principal moment, as neither ICANN, nor NTIA, nor the formal jurisdiction of the respective RIR have no legal power to control the RIR's Number Resource allocation policies. The RIRs policies have been summarized in regularly updated RIR Comparative Policy Overview documents, which state the goal of the RIR system: "All allocations and assignments of Internet resources must be consistent with the goals of the Internet Registry system: *aggregation*, *conservation* and *registration*"[6]. The Policy Overview documents also provide a comprehensive comparative set of the RIRs' technical policies with regard to the Number Resources allocation, technical requirements and eligibility criteria for their recipients, etc.	in 1999 and affiliated with ICANN. However, a few years later another institutional mechanism was launched and largely took over the ASO's role of the RIRs' interface for policy making and collaboration. It was the Number Resource Organization (NRO), an unincorporated organization uniting the 5 RIRs. It was established on October 24, 2003, when the 4 existing RIRs (AfriNIC was established and joined NRO in 2005) entered into a Memorandum of Understanding (MoU) in order to undertake joint activities, including joint technical projects, liaison activities and policy coordination. According to the ICANN Address Supporting Organization (ASO) MoU of 2004 (which was an agreement between ICANN and the Number Resource Organization (NRO)), the NRO took the role, responsibilities and functions of the ASO[7]. Today, RIRs cooperate among themselves, with ICANN and other technical community bodies largely through the NRO interface.

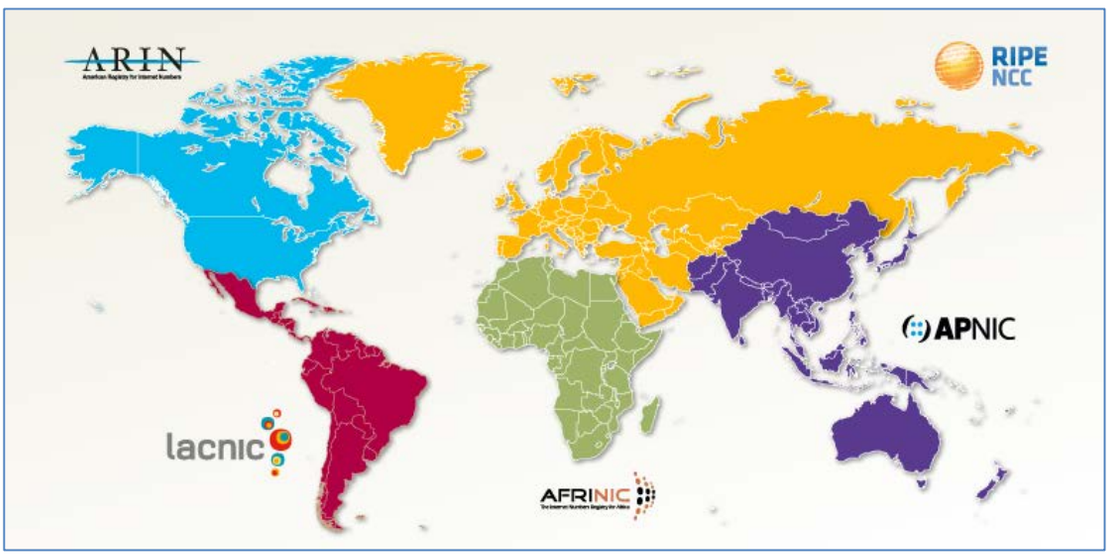
[6] RIR Comparative Policy Overview, 12 April 2015, <2015-01https://www.nro.net/rir-comparative-policy-overview/rir-comparative-policy-overview-2015-01#1-1>, last accessed on April 30, 2015.

[7] ICANN Address Supporting Organization (ASO) MoU, ICANN, 21 Octobeer 2004, <https://aso.icann.org/about-the-aso/aso-memorandum-of-understanding/>, last accessed on April 30, 2015.

Apart from these technical structures and outfits, the business processes related to management of the Internet's infrastructure also involve TLD registries, and registrars, ISPs and other network operators. At the national level, these and other participants could be part of private sector, technical and academic community, or to be controlled by governments.

All the key developments and decisions related to the Internet architecture are coordinated, approved, and implemented by the technical community, which is not linked to any international legal regime governing such activities. What is more, some of the key formats of developing and coordinating such decisions do not have any legal form governed by any national jurisdiction.

Map 4: Geographic distribution of Regional Internet Registries as of April 2015



Source: Regional Internet Registries Global Internet Resources Administration. Number Resource Organization website, <https://www.nro.net/about-the-nro/regional-internet-registries>, last accessed on April 30, 2015.

At the same time, states and international organizations are also involved in the process of Internet governance. Most of that work is done at organizations and venues that are part of the UN framework.

1. The most important of these venues is the already mentioned WSIS, which did not cease to exist when the Tunis stage ended in 2005. At present, work is under way on the WSIS+10 process. Its key stage will be the 2015 WSIS summit to be held in New York in December 2015. Issues related to the development and governance of the Internet will be at the top of the WSIS+10 agenda. The New York summit is expected to take stock of the international community's efforts on the development and governance of the Internet over the past 10 years.

2. Another mechanism that was created in accordance with the decisions of the Tunis state of WSIS is the Internet Governance Forum (IGF). It was set up under the UN auspices as a global platform for multilateral political dialogue involving all

stakeholders. The IGF was given a five-year mandate, with a possibility of prolongation. That prolongation was approved in 2010. The next WSIS summit in 2015 will consider another prolongation, as well as proposals to update and review the IGF format and remit. At this time, the IGF is not a platform for developing international documents. It does not perform any supervisory role; neither is it involved in the day-to-day running and maintenance of the Internet. The main format of its operation is annual meetings; the last such meeting was held in Istanbul on September 2-5, 2014.

3. Some of the functions related to Internet governance are performed by the ITU. In the late 1980s and early 1990s, the ITU's efforts to liberalize price formation and the provision of services in the area of telecommunications made a substantial contribution to the development of the Internet. As a UN agency, the ITU also actively participated in the Geneva and Tunis stages of the WSIS. Several countries, and especially Russia, currently regard the ITU as the best platform for creating a global intergovernmental organization on technical Internet governance issues.

4. Another organization involved in Internet governance is the World Intellectual Property Organization (WIPO). It participates in the development of approaches and standards in the area of protecting intellectual property on the Internet. It also works with ICANN and RIRs on the resolution of conflicts over domain names.

5. Internet governance issues are also part of the agenda of many regional organizations and dialogue platforms. They include the OECD, the Council of Europe, the G20, the G8 (which has temporarily suspended Russian membership), and others.

Transformation of approaches to Internet governance: globalization vs. internationalization

On the whole, over the past 10-15 years this *hybrid* system of Internet governance has proved flexible, effective, and viable. Now, however, the global architecture of Internet governance is undergoing major transformations. This is largely because many of its participants want a revision of the existing model and of their role within it.

Over the years since the Tunis stage of the WSIS, the growth of the Internet, the expansion of its infrastructure, its increasing complexity, and a giant leap in the capitalization of the Internet sector have stimulated an expansion of the technical community, the strengthening of its positions, and the growth of its remit. The unique practice of many years of work with a relative freedom to make decisions and, until recently, very limited governmental intervention, has helped technical community organizations to formulate their own comprehensive vision of the Internet governance agenda. Even though that vision focuses primarily on technical issues, there is a growing demand for the involvement of the technical community in formulating global policies of the development of the Internet, including issues that go far beyond the technical aspects.

As the Internet continues to grow and evolve, some of the aspects that used to be strictly practical begin to acquire new aspects and dimensions, including political and legal ones.

A case in point is the development of the global domain space, including the launch of new top-level domains (nGTLDs) by ICANN, which began to accept applications for these domains in June 2011. As part of that project, ICANN had to address conflicts related to the so-called *geographic* domains. For example, an application for the .amazon domain was filed by the Amazon corporation. That application was rejected under pressure from several South American states, which argued that they have the *natural right* to that domain name. Before the arrival of nGTLDs, international disputes also broke out over the .XXX domain for pornographic content (objections were raised by the ICANN Governmental Advisory Committee, GAC) and in several other cases. One way or another, in many such cases the Internet Corporation was forced to address issues that had social, political, cultural, and economic repercussions.

Another factor that adds international political aspects to the ICANN agenda is the long process of the transformation of the corporation's relations with the U.S. government. ICANN was set up in 1998 on the condition that the U.S. Department of Commerce would then cease exercising any control over the corporation, and that eventually the DoC's contractual relations with ICANN would end as well. That process, however, is still ongoing, even though it received a fresh impetus in the summer of 2013. America's image as the main champion of openness and freedom of the Internet suffered a major blow following Edward Snowden's revelations. The resulting vacuum of moral leadership in that area has served as a catalyst for ICANN's reassessments of its own objectives and priorities. The corporation has realized that the potential for leadership within the Internet community it had accumulated over the years must be fulfilled as soon as possible.

As a result, it has now assumed the role of the main platform for the articulation of the Internet community's interests on Internet governance issues. An important factor that enables ICANN to play such a role is its formidable financial resources, including those generated by the launch of the new nGTLD domains. The corporation's revenues reached more than 200m dollars in the 2014 financial year. That is a more than threefold growth compared to the 2009 figure. Using its growing financial muscle and leadership of the technological community, in 2012 ICANN launched the Global Stakeholder Engagement program, as well as a program of globalization of IANA functions.

As part of its efforts to globalize its presence and some of its functions, ICANN has undertaken the following steps:

- In October 2013 it announced its intention to take all the critical functions of the Internet outside the framework of U.S. government control. There were further developments on that front in March 2014 (see Section 8).
- It has begun to expand its presence at the regional level by opening a network of regional offices and hubs. In April 2013 it opened a regional office in Istanbul, and considered the possibility of turning it into its new head office. It also announced plans to open regional offices and stakeholder engagement centers in Singapore and Beijing.
- It has launched a strategy of stepping up cooperation with regional organizations. In February 2014 it announced the opening of a new office in Geneva, the home of many international organizations, including the WIPO, the ITU and several other UN agencies, as well as the WEF. The ICANN vice president for global stakeholder engagement, Veni Markovski, essentially serves as the "ICANN ambassador to international organizations" at the

corporation's New York office, which opened in 2013. The remit of the office includes liaison with the UN, its various agencies, and the national representative offices at the UN headquarters.

- ICANN has designated the strengthening of its international legitimacy, including the institutional aspect of it, as a strategic priority. On February 17, 2014 the ICANN Board passed a resolution that initiated the establishment of the President's Globalization Advisory Groups. The task set before the advisory group for legal structure is to set up an auxiliary parallel international structure to strengthen ICANN's global legitimacy.

As a result of these efforts, and with the help and support of other members of the Internet community, ICANN is beginning to set the agenda on global Internet governance, with little regard for the traditional intergovernmental mechanisms.

A case in point is the NETmundial track, which emerged following the disclosure by Edward Snowden than the NSA was spying on Brazilian President Dilma Rousseff. After a meeting on October 9, 2013 between ICANN President Fadi Chehade and Dilma Rousseff, the two parties agreed to hold a global meeting on issues of future Internet governance, to be attended by all interested parties. The purpose of that initiative was to agree a set of principles of Internet governance that would reflect the will of all stakeholders (including principles that would limit government programs on the Internet, such as the one pursued by the NSA).

The NETmundial summit was held on April 23-24, 2014 in São Paulo, Brazil. It was attended by more than 1,500 delegates, who approved a Final Statement that contained principles of Internet governance and a roadmap for future development of the Internet governance ecosystem.

The documents adopted at the summit reiterate the principle of multistakeholder governance. They also propose principles that have to do with security, cultural and linguistic diversity, human rights, innovation, etc. The road map contains a list of proposals on such issues as strengthening the IGF mechanism and platform, the transfer of control over the execution of IANA functions to the Internet community, strengthening multilateral cooperation in the area of cybersecurity and law in the Internet, etc.

The summit in Sao Paolo created an important precedent: a platform that has no intergovernmental status, with a technical community organization (ICANN) playing the leading role, has produced a document that covers all the key issues of global Internet governance in the institutional, social, cultural, economic, and other spheres. What is more, it is now being proposed that the decisions adopted at NETmundial should be used as a basis for the development of a global discussion on Internet governance involving all stakeholders. In June 2014, the World Economic Forum (WEF) also became involved in the NETmundial initiative. In other words, the Internet community has become to formulate and implement the global agenda on the entire range of Internet governance issues, bypassing intergovernmental platforms and mechanisms (although state representatives are also involved in the process). This is a new phenomenon in international practice, and its full potential and implications have yet to be properly understood.

Meanwhile, there is an opposite process going on; it boils down to the growing presence and role of governments in the Internet. One of the components of that process is that governments are increasingly trying to strengthen their control of the Internet infrastructure in their national territory. Russia is a staunch proponent of such an approach. It has repeatedly voiced various initiatives to that effect at the international level. Russia's SCO (Shanghai Cooperation Organization) partners have adopted a similar stance. In 2009-2011 the IBSA states (India, Brazil, and South Africa, who are Russia's partners at BRICS) advocated the establishment of a new international agency in the UN framework to coordinate Internet governance issues.

The key components of this approach are as follows:

1. All the key issues of Internet governance and the development of Internet infrastructure must be discussed and decided at a legitimate intergovernmental platform that would represent the entire international community, and preferably work in the UN framework. Russia believes that such a platform can be provided by the ITU. It advocates the proposal to transfer the remit of overseeing the critical functions of the Internet to the ITU, and to make Internet governance issues an integral part of the ITU agenda. The Russian delegation voiced these initiatives at the 2012 World Conference on International Telecommunications (WCIT), the recent IGF conferences, NETmundial, and other international events. The Russian position at the 2014 ITU Plenipotentiary Conference also placed an emphasis on these proposals. The same will probably apply to the final WSIS+10 summit. At the national level, the proposal to give the ITU a central role in Internet governance is reflected in the Basics of Russian State Policy on International Information Security to 2020, a policy document signed in 2013.

2. The principle of multistakeholder Internet governance is reflected in the WSIS final documents, as well as in the agenda and work format of the ITU, the IGF, and several other agencies. That principle is no longer in any doubt. Nevertheless, its interpretation proposed by ICANN and other technical community organizations (and reiterated at such platforms as NETmundial) is not entirely correct. The need to take into account the opinions of all stakeholders (and not just governments) is no justification for taking decisions that fail to take into account the interests and positions of states, and have not been agreed with state representatives. Even though all stakeholders have equal status and their positions must all be taken into account, the right to make final decisions on Internet governance should lie with states as the only wielders of sovereignty and the only subjects of international law.

3. The principle of state sovereignty fully applies to the Internet. It is therefore entirely right and proper to take into account the existence of the national segments of the Internet when working on Internet governance issues. The policies of regulating these national segments depend on the sovereign will of the state in question, so there may be differences between them, even though they follow the same general principles.

4. One of the key elements of the present status quo that must be revised as part of the formation of an *international* model of Internet governance is the system

of managing IP addresses, domains, and the DNS system. Essentially, the role and status of the Internet Corporation must be revised. Those who propose giving the central Internet governance remit to the ITU believe that ICANN cannot be regarded as the optimal mechanism of executing critical Internet functions or exploring Internet governance issues. The reasons for that are as follows:

- The Internet Corporation is not an international organization. As a result, it does not have the international legitimacy to make global decisions on issues that affect the entire international community. Internet governance is just such an issue.
- Even though formally ICANN is a not-for-profit organization, it earns substantial revenues thanks to the domain space extension programs. This creates a conflict of interest and raises questions as to whether ICANN is an impartial entity that takes into account the entire range of public interests in these areas.
- ICANN is not a neutral or independent entity since it was set up and continues to exist within the U.S. jurisdiction. It is linked to the U.S. government by various contractual commitments. As a result, it is liable to favoring narrow interest groups rather than the coordinated position of all stakeholders.
- Entrusting critical Internet functions to ICANN impinges on the interests of the international community and threatens its security because to all intents and purposes, the U.S. government controls critical Internet functions thanks to its contracts with the Internet Corporation. The concept of control over the Internet, which is an *international public good*, being exercised by a single state is seen as unacceptable and no longer justified by any technical requirements.

Challenges to Internet governance: politicization and fragmentation

The problem is that the simultaneous development of the two aforementioned approaches increasingly leads to competition and clashes, including those seen at various international venues.

One perfect example of such a clash is the debates and decisions made at the World Conference on International Telecommunications (WCIT) held in Dubai on December 3-14, 2012. The key goal of that conference was to coordinate and approve changes to the International Telecommunication Regulations (ITR). The ITR is essentially a global agreement between ITU members that regulates the establishment of common principles in the area of international telecommunications; interconnection between telecommunication networks; coordinated development and effective operation of technical systems, etc. The last time the ITR was updated was back in 1988, i.e. before the rise of the Internet as we know it today. That is why an update was well overdue in 2012.

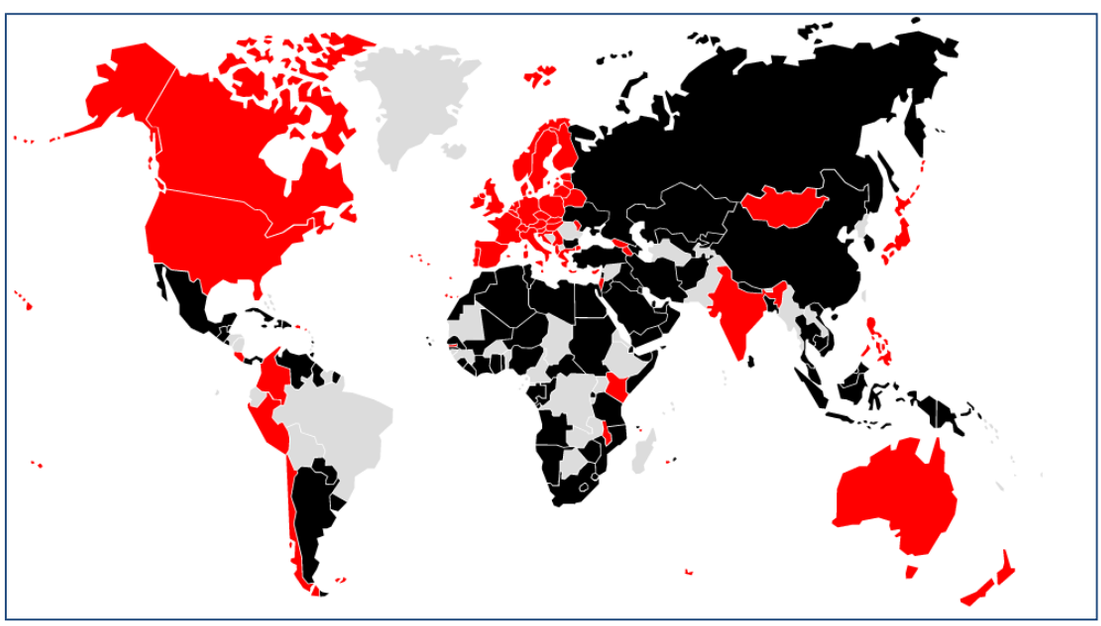
Before and during the WCIT, Russia proposed amendments to the ITR under which Internet governance issues would become part of the ITR, to be decided on an intergovernmental level. These proposals were supported by Iran, China, and several African and Arab states. The initial version of the Russian proposals (of November 17, 2012) included the following changes:

- Introduction of the terms of definitions of *the Internet*, Internet *traffic*, Internet *root infrastructure*, and the *national Internet segment*.
- Introduction of Article 3.A "Internet", which established equal rights of all ITU member states in the area of Internet governance, including such issues as the use and management of IP address resources; the distribution and delegation of domain names and development of the DNS system; and the sovereign right of states to develop Internet governance policies and regulate the national Internet segments and the work of ISPs within their national borders.

These proposals were later withdrawn and replaced by less ambitious ones. Nevertheless, the participants failed to reach a consensus even on these watered-down amendments to the ITR. As a result, they were forced to abandon the previous practice of adopting all decisions unanimously, and held a vote. The vote left the community of ITU member states split into two large groups (see Map 5).

In the end, the new ITR did not contain any provisions on national sovereignty in the Internet (or even the term "Internet"). Nevertheless, developments at the WCIT and the outcome of the conference were seen by many Western countries and technical community organizations as an attack by certain states on the technical community, ICANN, and the principle of multistakeholder governance. The idea that the WCIT signaled the onset of a "Cold War for control of the Internet" became popular in the media and the public debate, even though it was not an accurate reflection of the outcome of the conference.

Map 5: Results of the vote on the updated ITR at the 2012 WCIT event in Dubai



Note: The 89 countries that signed the new ITR are highlighted in **black**. The 55 countries that refused to sign the new ITR and continue to follow the 1988 edition of the document are highlighted in **red**.

Source: I Country positions on ITR proposed at WCIT 2012, IPV Website, <http://www.ipv.sx/wcit/>, last accessed on April 30, 2015.

Another example of conflicts between the different approaches is the already mentioned NETmundial summit in Sao Paulo. Even though the summit adopted a Final Statement, representatives of several states, including Russia, refused to support that document or recognize it as reflecting the opinions of all the participants. The reasons for that included insufficiently transparent process of drafting the text of the Final Statement and failure to take into account the opinions of all participating states and other parties (through the mechanism of written commentaries or other instruments).

For now, conflicts between the proponents of different approaches have not led to any infrastructural problems with the Internet. There is no real threat to that infrastructure's stable and resilient operation. Nevertheless, further deterioration of such conflicts could prove destructive for the Internet ecosystem because of various negative consequences:

1. Politicization of originally technical issues and challenges and problems in the field of Internet governance.

The 2012 WCIT in Dubai was an example of conflicts breaking out over essentially technical issues because they have become politicized. The storm of criticism of the new ITR by representatives of the technical community and the Western Internet community is not entirely understandable, if the Final Acts are viewed outside the context of the Conference itself and of the debate in Dubai. Because of the politicization of WCIT, Article 7 of the ITRs (Unsolicited Electronic Communications) was often interpreted as an attempt by proponents of "digital sovereignty" to disguise the inclusion of Internet content regulation in the ITU agenda. In actual fact, that provision was a neutral (albeit poorly phrased) measure against spam messages distributed via electronic communications, including the Internet (which is never mentioned by name in the new ITR). Another example, which is even more dangerous in terms of its potential consequences, is the politicization of the issue of the physical location and management of DNS root server infrastructure (see Section 7).

At the same time, major Internet governance issues remain unexplored or ignored because the attention and efforts of all the parties are monopolized by the discussion of politicized issues.

- A year after the electronic espionage programs by the NSA and other secret services came to light, there is still no international mechanism to prevent such programs. Worse, no serious proposals have been made as to the strategy the Internet community must pursue in that area. The hopes that some answers to these questions would be provided by the NETmundial summit in April remain unfulfilled.
- There is a growing need to develop global approaches to questions of identification on the Internet, especially in view of the increasingly popular trans-border services and the rise of cybercrime, as well as other threats on the Internet.
- Little is being done on the issue of Net Neutrality, which requires the involvement of ISPs, first and foremost.
- There are important unresolved problems of jurisdiction in the Internet, especially with regard to trans-border services; the same is true of the development of cloud services, big data processing services, etc.

2. Emerging of parallel agendas, documents, and formats for Internet governance issues

The rise of the NETmundial track, which has not been backed by Russia and some other countries, has set a precedent for the emergence of duplicate agendas that evolve in different directions, even though their scope includes the global stakeholder community.

There have also been attempts to formulate the agenda for Internet governance at intergovernmental venues without properly engaging the technical community or taking its opinions into account. A case in point is the 2012 WCIT event. Of its 1,576 participants, only nine represented ISOC and 15 regional registries. All 24 were excluded from the final vote.

The split and divergence of the global agenda for Internet governance at different venues is dangerous because it creates the preconditions for political fragmentation. The worst-case scenario (which still remains very unlikely, but demonstrates the potential scope of the problem) is the formation of regional blocs and coalitions of states, corporations, and technical community entities that promote their own approaches to Internet governance and ignore the initiatives and proposals of their opponents.

4. As a result of these negative trends, some of the participants in this process, having failed to reach an understanding with other parties, could well decide to go it alone and develop their own technical policies and standards of Internet regulation. Political polarization and divergent Internet governance tracks could potentially set the stage for the development of autonomous governance policies at the infrastructural level.

States – including those that advocate using international bodies for Internet governance - have the greatest resources available to them to pursue such a course. In the opinion of states themselves, the strategy of trying to achieve infrastructural sovereignty has entirely rational motives:

- The problem of global electronic espionage and data gathering on the Internet remains unresolved. Attempts by governments to ensure the security of their systems and their citizens on their own lead to solutions based on the localization of data, creating independent trunk infrastructure, toughening policies on imported software and information protection systems, etc.
- As already demonstrated, control over critical Internet resources and functions is a sensitive subject for a number of governments. Led by national security considerations, they will try to reduce the dependence of their national Internet segments on the global DNS system, unless other solutions can be found.
- Although the economic effects of infrastructural fragmentation of the Internet are extremely questionable and contentious, infrastructure development and import substitution in the national segments is an attractive proposition for some of the players in the Internet sector.

Even though the Internet retains its infrastructural and architectural integrity for the time being, the growing politicization of Internet governance issues could eventually lead to tangible steps being made towards autonomization of individual nation-wide or region-wide Internet segments. In fact, there has already been certain movement in this direction.

- In 2003 the Chinese government proposed the introduction of the WAFI standard, a Chinese-developed alternative to WiFi (IEEE 802.11), a family of data link layer protocols.
- In 2013 Edward Snowden's revelations prodded the governments of Brazil and Germany to explore the possibility of moving the data servers that process personal data of their citizens to their own national territory. In addition, Germany began to explore the possibility of creating a national closed network for its government agencies.
- In recent years Chinese specialists submitted to the IETF several editions of a memo outlining a quasi IP addressing technology that duplicates the functions of the national DNS segment.
- The concept of a DNS segment with an autonomous quasi IP addressing system has already been partially implemented at the national level by Iran.
- It was reported in April 2014 that a working group under the Russian presidential administration had developed proposals on restructuring of the Internet architecture in the Russian segment. The proposals included moving to Russian national territory the top-level DNS servers that process requests for the .RU and .РФ domain zones. They also included restrictions on cross-border data transmission by the networks of several federal-level ISPs.
- In July 2014, the Ministry of Communications and Mass Media of Russia conducted a large cyber training in July that year. The training was conducted with participation from Federal Security Service, Federal Protective Service, MOD, Ministry of Internal, Russia's largest ISP Rostelekom, Coordination Center for ccTLDs .RU/.РФ, and Russia's largest IXP – MSK-IX. The training, according to the data disclosed by the Ministry and mass media, inter alia was focused on a scenario implying disruption of operation of the Russian segment of the Internet as a result of "external hostile actions". In follow-up of the cyber training Aide to the President of Russia Mr. Igor Shchegolev in his interview to the media states that the training revealed the Runet's "insufficient resiliency"; he also noted that the USA still owns the administrative levers to the Net's global infrastructure, including the DNS Root Zone and the Internet's Number Resource system.
- During Fall 2014, statements were made by Russian officials including Russian Minister of Communications and Mass Media Mr. Nikolai Nikiforov, on launching consultations and collaboration with the BRICS states on the ensuring robustness and resiliency of the critical infrastructure of the Internet's national segments in the light of possible "external destructive actions". This agenda advanced to the forefront of Russian expert discussions and became the topic of the Russian Security Council's closed session in October 2014, a few months after the July cyber training.
- Finally, at an international *Track 2* forum on information security in April 2015, a high level Russian official explicitly stated if the USA does not make steps towards internationalization of the global Internet's infrastructure management system, Russia could engage into infrastructural collaboration with China that might ultimately result in fragmentation of the global Internet to the benefit of security and stability of the new autonomous segment that would emerge, even though it would imply massive damage to transborder Internet-enabled business processes.

Unlike most other layers of the Internet infrastructure, the global DNS system operates as a globally hierarchy with a centralized control on its top level – the Root Servers system. Centralized and hierarchical nature is also inherent to other components of the Internet's Unique Identifiers system – IP address allocation system and the Autonomous System Number allocation system (which together constitute the Number Resource Allocation system manages by IANA and RIRs).

This architecture in the case of DNS cannot be reformed quickly without major implications for the Internet users. It is, however, the most important part of the whole system as far as the autonomization of nation-wide and region-wide Internet segments is concerned. If the next round of international discussions, including the 2015 WSIS global summit, fails to produce a broad compromise between the interests of states and other stakeholders, there will be a strong likelihood of some countries pursuing further experiments to achieve a greater degree of autonomy of their national Internet segments in order to ensure their national security and *digital sovereignty*.

However, far-reaching steps in this direction would pose a threat to the entire Internet ecosystem because integrity and cohesion are key features of that ecosystem. The greatest danger posed by radical scenarios is a fragmentation of the Internet into national and/or regional segments. Inability by stakeholders and states to find the right balance of their rights and responsibilities and an effective model of managing critical Internet resources could slow down the development of the Internet, which has undoubtedly been a major driver of the economy, science, trade, finances, culture, and innovation over the past two decades.

Depoliticizing Internet governance and next steps to prepare for WSIS+10

One of the possible answers to these challenges is for all the participants of the Internet governance process and the proponents of all the different approaches to return to some common ground and partially re-launch the discussion on the key issues of Internet governance between the proponents of different approaches. All the parties could move closer to overcoming their differences – or at least to working together productively despite the remaining differences – by undertaking a joint effort to produce a global document that would serve (in terms of its objectives, format, and process) the interests of both the technical community and the proponents of international regulation of the Internet.

But for work on such a document to become possible, the parties need to choose a platform in the spirit of compromise. That platform should meet the following requirements:

a) It should be global and relevant for all members of the international community;
b) It should enable the participation of all stakeholders;
c) It should have a neutral status and not be linked to any state, Internet community organization, some intergovernmental or other interest group, etc.

Of all the existing platforms, the one that best meets these requirements is the Internet Governance Forum. The procedural and executive weakness of the IGF could actually prove a strength by giving it an impartial and neutral status and making it politically acceptable to all stakeholders, including governments.

It would therefore be useful and timely to propose an initiative on reformatting the IGF and turning it into a standing body tasked with preparing a global agreement on Internet governance in the 2-4 years timeframe (by 2018). The purpose of such an agreement would be to agree, in an international framework, a set of key principles of Internet governance. The agreement could be signed in the form of a UN convention or treaty incorporating all the Internet governance principles that are shared by all the parties, such as the multistakeholder approach, openness, Net neutrality, integrity and cohesiveness of the Internet, etc. Also, the new agreement should finally provide some answers to the problem of the Internet being used by states for illegitimate purposes and protecting the right to privacy on the Net. In addition, the agreement should contribute to establishing a system of responsible multilateral controls over the critical Internet functions, including the DNS system.

The proposed agreement could use some of the solutions and principles incorporated in the December 19, 1966 Outer Space Treaty, which does not contain any specific commitments by the state parties, but outlines the general principles of cooperation.

Progress in this area will require:

- Extension and enlargement of the IGF mandate, as well as better and more stable financing;
- Reformatting of the IGF to turn it into a standing body tasked with preparing an international agreement. In particular, the forum's Secretariat should become a standing body that works all year round (Executive Secretariat);
- The WSIS+10 summit in December 2015 will have to agree and include in its final documents a plan of action on restructuring the IGF and modifying its remit. An agreement on this can be reached through a consolidated effort of all interested parties (including states). For example, Russia and its BRICS partners could form a united front on this issue at the WSIS summit.
- Working and expert groups will have to be formed under the Executive Secretariat to work on a standing basis on the key issues and principles that must be reflected in the final document (including Net neutrality, protecting the right to privacy and preventing systemic violations of that right by the NSA and the secret services of other countries, localization of data and preventing Internet fragmentation on the infrastructural level, etc).

With a constructive approach by states and other stakeholders, work on such a global agreement could begin in 2016, to have it ready for signature by late 2017 or 2018.

2. In order to take the interests of states with regard to multistakeholder Internet governance more fully and effectively, the mechanisms of state involvement in making decisions at the relevant bodies will have to be strengthened.

To that end, relevant parties could revisit proposals on strengthening the role of the ICANN Governmental Advisory Committee in the overall decision-making process at the Internet Corporation.

Relevant parties should also explore the possibility of changing the current status of the GAC and giving it greater independence within the ICANN framework. That will help

to ensure a comprehensive and responsible nature of GAC decisions with regard to the supervision and audit of IANA functions in the interests of the global stakeholder community, as well as the Russian Internet community. For the duration of the transfer of the IANA functions (that process could prove quite lengthy), representatives of states could be given special voting rights to make sure that the interests of states, which have a very special role to play among all the stakeholders, are properly taken into account.

To that end, it would make sense to support the proposed amendments to the ICANN Charter that were released for commentary on August 15, 2014. One of these proposals is to raise the voting threshold the ICANN Board needs in order to overrule GAC decisions. More specifically, it is proposed that overruling GAC decisions should require a two-third majority rather than simple majority of the Board votes.

3. The WSIS+10 process, and its key stage in December 2015, could be used by all stakeholders to promote the principle of depoliticization of global Internet governance issues. In particular, proposals could be formulated to consider the following issues separately from political aspects:
а) Developing policies in the area of Internet governance (drafting an international treaty on the principles of Internet governance, development of the global domain space, and elaborating approaches to protecting the right to privacy online);
б) Technical issues (assigning and distributing the parameters of Internet protocols, developing the WHOIS service of identification of domain name owners; introducing IPv6 and DNSSEC; and strengthening the encryption of user traffic to improve personal data protection);
в) Administration of the Internet governance system (DNS root servers management structure, decision-making process at the IETF (the RFC mechanism) and other entities of the technical community).

Clearly, many of these issues, such as the transfer of control over IANA functions, must be dealt with in a comprehensive fashion, and cannot be regarded outside the political context. Nevertheless, even a partial depoliticization of the agenda can help to make that agenda more effective and reduce the risk of a confrontation between the various stakeholders.

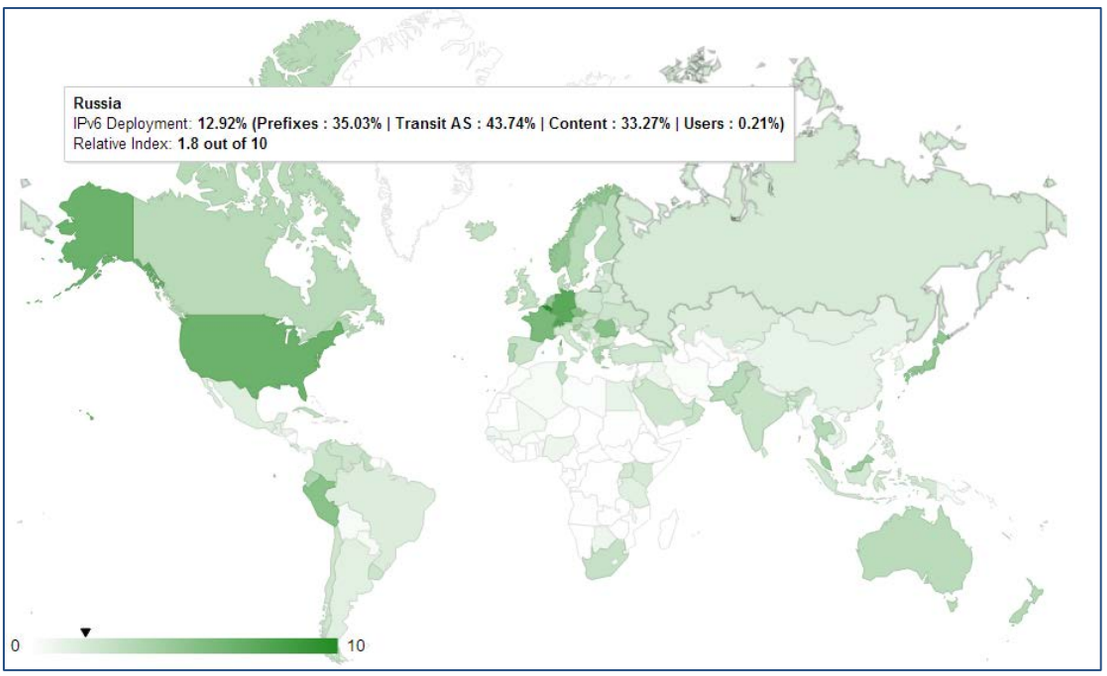
To that end, it would be very useful to put these proposals on the agenda of the final event of the WSIS+10 process in December 2015, and to reflect them in the Final Document.

Apart from resolving the political differences over the architecture of global Internet governance, it is necessary to step up efforts to implement, on a national and global level, a number of technical solutions that ensure security and reliability of the Internet.

Development of the Internet's Unique Identifiers: Deployment of IPv6 and DNSSEC

One of the important and pressing objectives for the international community, including Russia, is a full-scale rollout of the updated version of the IP protocol called IPv6, and ensuring that new protocol's compatibility with the previous version, IPv4. The problem of transitioning to IPv6 has long been on the agenda because the last available stack of IPv4 addresses was allocated back in February 2011.

Map 6: Global penetration of IPv6 in June 2014

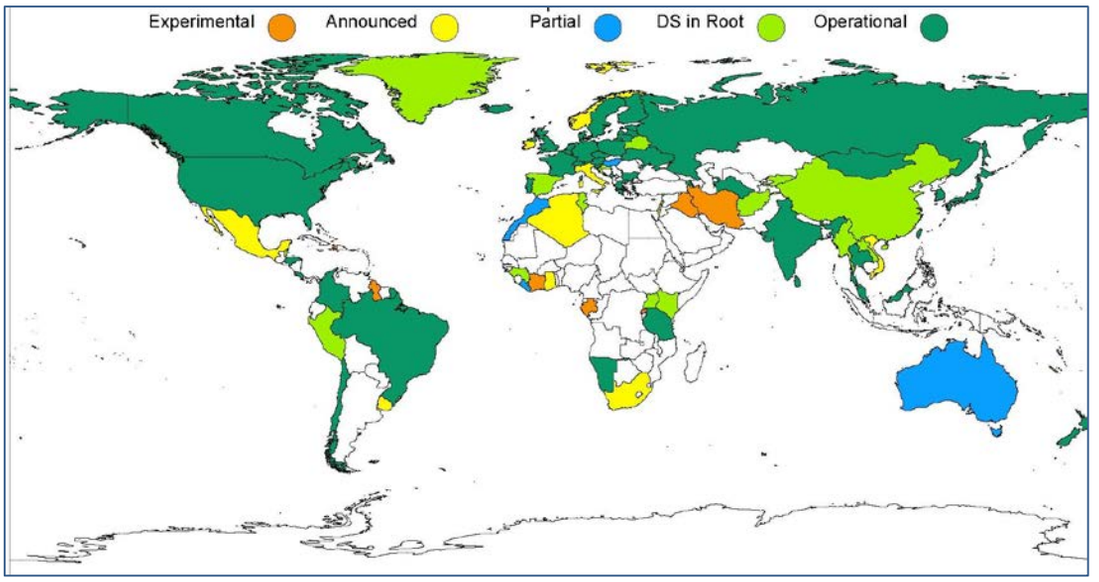


Source: Display Global Data. Cisco Systems,
< http://6lab.cisco.com/stats/>, last accessed on Apil 30, 2015.

The pace of the rollout of IPv6, which continues to coexist with IPv4, is clearly too slow. According to Cisco Systems, as of June 2014, two years after the start of IPv6 rollout, only 4 per cent of the world's Internet users were using the updated protocol. The figure for the United States was 8 per cent. The rise of the Internet of Things, with a growing number of industrial devices and household appliances getting online, requires a substantial acceleration of the IPv6 rollout. According to various forecasts, there will be up to 50bn Internet-connected devices by 2020, which is almost 10 times the number of all available IPv4 addresses. In another 10 years, the number of such devices could reach trillions. The potential economic effects of the Internet of Things are estimated at 10-15 trillion dollars over the next 20 years, according to GE. That makes it an important priority for states and the technical community to facilitate that trend. It might be therefore reasonable and even necessary for governments to do all they can to speed up the deployment of IPv6 at the national level.

The Chinese government has set an example of energetic efforts in that area, in cooperation with the technical community and all other stakeholders. In April 2012, it adopted a 10-year plan of IPv6 deployment. The development, adoption, and implementation of a similar national plan to complete the transition to IPv6 (for example, in the 2015-2020 framework) should be a notable priority for Russia. The plan should be developed and approved by the relevant government agencies, in close cooperation with all stakeholders, including RIPE NCC, local internet registries, CC TLD .RU/.РФ and other representatives of the Internet sector and the technical community.

Map 7: ccTLD DNSSEC Adoption as of October 14, 2014



Source: DNSSEC Deployment Maps, Internet Society 01.07.2014, <http://www.internetsociety.org/deploy360/dnssec/maps/>, last accessed on April 30, 2015.

4. Similar measures and efforts are required for the deployment and validation of DNSSEC (Domain Name System Security Extensions). The DNSSEC plays a crucial role in prevention and mitigation of attacks and other DNS security challenges, such as Data Corruption attacks. In particular, DNSSEC could be used to protect data in transit and in storage, reducing the risk of cache poisoning and man-in-the-middle (MITM) attacks.

The concept of the Domain Name System Security Extensions (DNSSEC) was first introduced by RFC 2065 in January 1997. The document identified the key concept of the new security extensions to the DNS protocol, in particular, those should:

- provide the DNS services to security aware resolvers or applications through the use of cryptographic digital signatures, the latter being included in secured zones as RRs.
- provide for the storage of authenticated public keys in the DNS, which could support general public key distribution service as well as DNS security.
- provide for the optional authentication of DNS protocol transactions.

The document also provided an extensive set of technical considerations with regard to the validation keys, their parameters, generation periods of validity, etc. The design and technical concept of the DNSSEC was later extended and detailed in different aspects by a set of RFCs including RFC 2931, 3008, 3110, 3130, 3225, 3226 and some others not necessarily solely dedicated to the DNSSEC issues.

However, DNSSEC was fully standardized much later, with RFC 4033 “DNS Security Introduction and Requirements” published by IETF in 2005. According to the document, DNSSEC provides origin authentication and integrity assurance services for Name Servers data, including mechanisms for authenticated denial of existence of DNS data. As a development to RFC 4033, more RFCs on DNSSEC were, published as a

single document family; those include RFC 4034 “Resource Records for DNS Security Extensions” and RFC 4035 “Protocol Modifications for the DNS Security Extensions. Despite the progress made since the release of the first DNSSEC specification (RFC 2065 in 1997) – such as the signing of the DNS root zone by July 2010, the .com domain in March 2011, and the .RU and .РФ domains in November-December 2012, the overall level of DNSSEC penetration in Russia and globally still remains in the 10-15 per cent range.

To date, one of the major issues related to DNSSEC remains its full-length deployment across all levels of the global DNS infrastructure. The Extensions were designed in such a way, that their correct operation demands existence of a full validation chain. E.g., a security-aware resolver cannot verify DNS responses originating from an unsigned zone, since it is necessary that all zones along the path from the trusted starting point to the zone containing the response zones are signed, and all name servers and resolvers involved in the resolution process are security-aware.

The DNS deployment is a continuous process which to date demonstrates steady progress but is still far from completion at the level of country-code domain zones. However, the procedure of signing the Root Zone level of the DNS was accomplished. It started on December 1, 2009 when the Root zone was signed for internal use by VeriSign and ICANN and was finished on July 15, 2010 when ICANN after holding two KSK ceremonies published the root zone trust anchor and root operators began to serve the signed root zone with actual keys. On October 21, 2010, the DNSSEC Practice Statement for the Root Zone Key Signing Key (KSK) Operator by the Root DNSSEC Design Team was published, which provides an extensive and comprehensive technical guidance for IANA as a Root Zone Operator and VeriSign concerning its specific functions of technical management with regard to the Root Zone file management.

The .ORG top-level domain was signed with DNSSEC in June 2010, followed by .com, .net, and .EDU later in 2010 and 2011. Country code top-level domains were able to deposit keys starting in May 2010. Detailed statistics of DNSSEC Deployment is also provided by one of the RIRs – APNIC:

Table 7. DNSSEC Validation Rate by country (per cent)

Code	Region	DNSSEC Validates	Uses Google PDNS	Samples	Weight	Weighted Samples
XA	World	12.99%	14.07%	71112827	1	71112827
XB	Africa	18.02%	27.10%	3777008	1.83	6903960
XC	Americas	17.19%	12.25%	18817342	0.8	14975508
XE	Europe	17.09%	8.35%	16269506	0.75	12264544
XF	Oceania	15.24%	6.24%	333077	1.83	610362
XD	Asia	8.80%	14.55%	31915874	1.14	36358423
XG	Unclassified			20	0.09	1

Source: DNSSEC Validation Rate by country (%), APNIC, <http://stats.labs.apnic.net/dnssec>, last accessed on April 30, 2015.

We believe that the relevant government agencies (the Communications Ministry in Russia), with the assistance of technical organizations (IETF) as well as regional and national domain registries should launch programs of facilitating DNSSEC rollout at the national level.

Additional information:

1. Yakushev Mikhail, Internet 2012 and International Politics, Security Index, No. 1 (104), 2013, <http://www.pircenter.org/media/content/files/10/13559076950.pdf>, P. 29-42, last accessed on April 30, 2015.
2. Kassenova Madina, Global Internet governance in the context of international law. Security Index, No 1 (104), 2013, <http://www.pircenter.org/media/content/files/10/13559079720.pdf>, P. 43-64, last accessed on April 30, 2015.

Documents:

1. Final Acts of the World Conference on International Telecommunications. International Telecommunications Union, 2012, <http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12-ru.pdf>, last accessed on April 30, 2015.
2. Key elements of official Russian position on the outcomes of the Global Meeting on Internet Governance Issues. Russian Embassy in Argentina, June 19, 2014, <http://argentina.mid.ru/-/19-06-2014-osnovnye-elementy-oficial-noj-pozicii-rossijskoj-federacii-po-itogam-global-noj-vstreci-po-voprosam-upravlenia-internetom>, last accessed on April 30, 2015.
3. Affirmation of commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers, September 20, 2009, <https://www.icann.org/resources/pages/affirmation-of-commitments-2009-09-30-ru>, last accessed on April 30, 2015.
4. ICANN's Major Agreements and Related Reports, ICANN website, <https://www.icann.org/resources/pages/agreements-2012-02-25-en>, last accessed on April 30, 2015.

VI. Oversight of the Internet's Global Infrastructure: Searching for an Optimal Model

Coordination of the operation of the Internet's global infrastructure has been taking place under a unique organizational and architectural model that has no direct equivalents in the world practice. Indispensable role in this model has been performed by the Internet Corporation for Assigned Names and Numbers (ICANN), which was mentioned in Section 5. ICANN operates two key layers of the Internet infrastructure, IP addresses and domain names, which are the unique identifiers used on the Net.

Even before ICANN was established in 1998, as the Internet continued to grow and commercialize, the U.S. government decided to start transferring the running of the Internet's global infrastructure to the community of technical experts. In June 1997, the National Telecommunication and Information Authority (NTIA), a part of the U.S. Department of Commerce, released a Request for Comments (RFC) about the current and future system of Internet domain names registration. In January 1998, the NTIA released a Green Paper outlining (and inviting comments on) its early vision of the path towards privatizing management of the DNS system and a gradual transfer of that remit away from the U.S. government.

After taking on board the comments received, on June 5, 1998 the NTIA released the so-called White Paper that invited the Internet community to set up a private non-commercial corporation to run the DNS system and function as the Internet Assigned Numbers Authority (the IANA functions). Further to the proposals outlined in the White Paper, on November 25, 1998 the Department of Commerce signed a memorandum of understanding with ICANN, in which the Internet Corporation was officially recognized as the private non-commercial organization that figured in the White Paper. In February 2000 the same parties signed, on a non-competitive basis, another contract under which ICANN undertook to fulfill the IANA functions. That contract was later extended on several occasions.

Relations between ICANN and the U.S. government as far as the IANA functions are concerned are currently regulated by another non-commercial Contract (worth $0) of January 10, 2012. The contract expires on September 30, 2015, but DoC has the option to extend it on a unilateral basis until September 2017 and then once again until September 2019.

Several countries, including Russia, have long criticized the institutional construct of the Internet Assigned Numbers Authority (IANA). The main criticism is that two critical layers of the global Internet infrastructure, which are both managed in a centralized and hierarchical way, are controlled by a corporation located within the U.S. jurisdiction that operates under Californian jurisdiction and is accountable to the U.S. government. Several states have therefore argued that the United States has too much control over the Internet's global infrastructure and its operation business processes. Since 2000-s, a number of governments including China, Brazil, India and Russia have been periodically calling to a revision of the existing model, and for ultimate internationalization of the IANA functions – or in particular, to their transition from IANA to an intergovernmental organization which would be probably linked to the UN. The International Telecommunication Union has been repeatedly mentioned as an optimal venue to overtake the stewardship of the IANA functions from the USG. Quite

recently, the issue appeared on several international gatherings, including the 2012 WCIT event in Dubai (where it was mentioned in draft proposals of the updated text of the International Telecommunication Regulations). No consensus on that issue was found; on the contrary, the final voting procedure split the ITU members into two groups: signatories to the new ITRs, and those who refused to sign the amended documents.

A new round of changes in ICANN policy and its relations with the U.S. government was largely triggered by the events of summer 2013, which undermined the White House's reputation as far as respect for human rights and freedoms online is concerned. The scandal also had major implications for Internet governance. In October 2013, at the height of the scandal caused by Edward Snowden's revelations, ICANN President Fadi Chehade announced during an IGF meeting his intention to take ICANN outside the scope of U.S. government control. Six months later the Department of Commerce responded to that announcement. On March 14, 2014 the NTIA posted a publication on its website in which it outlined its intention to transfer key functions of the DNS system to the global community of stakeholders. That decision largely forms the context of the problem of transfer of control over critical Internet functions (the IANA functions).

The NTIA announcement on the transfer of IANA functions puts the following questions and challenges before the international community and stakeholders:

1. Uncertainty over the process of transferring oversight of critical functions related to the Internet' global infrastructure as far as the institutional design of the new mechanism is concerned.

   The U.S. government says it would prefer to have the transfer process completed by the time the existing contract between ICANN and the DoC expires. Nevertheless, it has yet to be decided what entity will take over control over IANA functions. Some details about the U.S. government's intentions were revealed in a statement by NTIA chief Lawrence Strickling at the 49th ICANN Conference in March 2014 in Singapore: the White House will not transfer IANA functions to a state or any government, group of government of an intergovernmental organization. Any successor of the NTIA will have to be led by the principle of equality of all stakeholders. Also, in the opinion of the NTIA and ICANN itself, the successor does not necessarily have to be an entirely new entity.

2. Politicization of the process of transfering oversight of IANA functions and excessive politicization of issues related to the operation of the Internet's global infrastructure.

   One case in point is the politicization of the debate (in which Russia is also involved) on the operation of DNS root servers. Critics focus on the disproportionate concentration of DNS root servers in the United States (10 out of 13) and Western Europe (2 out of 13), as well as on the control exercised by ICANN, a U.S. entity, over all root servers. But the technilogical development of the root infrastructure of the Internet over the past 15 years has changed the situation very substantially. The functions of each of the original 13 root servers are now duplicated by numerous mirrors that are spread quite evenly across the

world. For example, Russia hosts three mirrors of the L root server, and one mirror apiece for the F, J, and K servers. The total number of physical sites that host root servers and their mirrors has reached 493 by April 2015 (see Map 8).

Also, the entity that coordinates the running of DNS root servers – the DNS Root Server System Advisory Committee – was originally set up by the ICANN Board, but it works and makes its decisions independently; it is not subordinated to ICANN. The companies and organizations that run each specific root server are also independent entities, and they are not bound by any commitments to ICANN in terms of their day-to-day work. In other words, the issue of the physical location of DNS root servers and of the running of these servers is no longer a priority in terms of the interests of the global Internet community or Russian interests.

3. The U.S. government will retain a degree of control over some critical technical business processes and functions related to the opertaion of the Internet global infrastructure even after the transfer of critical IANA functions; that problem still remains unresolved.

   One example is the functions of the U.S. corporationVeriSign. Under the terms of its own contract with the NTIA, VeriSign performs technical maintainance the DNSRoot Zone, which includes generation of the Root Zone file (a register of IP addresses and top level domain names) on a hidde master server, and distribution of this file to DNS Root Server operators. So far, transition of oversight of IANA functions from the U.S. government has not emompassed these VeriSign functions, even though it has been stated in the NTIA statement from March 14, 2014 that these issues must be addressed as well.

Map 8: Location of DNS root servers as of April, 2015

Source: Root Servers Website, <http://www.root-servers.org>, last accessed on April 30, 2015.

In view of the situation, the following recommendations could be offered to stakeholders in Russia and abroad:

1. A debate should begin on the prospects for setting up a new institutional mechanism to supervise and audit the execution of IANA functions instead of the U.S. government. That debate should be based on the notion that for now, the process of transfer of the IANA functions does not follow a clearly defined plan or time frame, and that tangible progress may well have to wait until the expiry of the second option for the extension of the contract between ICANN and the U.S. Department of Commerce in September 2019. At the same time, stakeholders should call for a speedy and final transfer of control over the IANA functions in accordance with the interests of the global Internet community.

2. An initiative should be proposed on the separation of IANA functions in order to depoliticize the issue of control over the execution of critical Internet functions. Proposals in this area include removing from the list of IANA functions the coordination of the assignment of technical parameters of the protocols that underpin the work of the Internet. These functions could be transferred to the IETF, which develops all these protocols and works with IANA on the basis of RFC 2860. Also, Regional Internet Registries (RIRs) could take responsibility with regard to oversight of IANA functions related to the Number Resource Allocation system (allocation of IP addresses and ASNs).

3. Transparent, accountable and independent control over the operation of the Internet's global infrastructure should be provided as an integral component of the post transition IANA (PTI) institutional architecture. This implies truly multistakeholder nature of the new institutional mechanism of PTI, external audit of critical technical business processes (like the DNS Root Zone management business process), publicly available information on IANA functions operation, and public reporting.

4. VeriSign functions as the DNS Root Zone Technical Maintainer should also be included into the scope of IANA Transition. For the moment, under the Contract with NTIA VeriSign does not provide open information on how it operates its functions, neither it discloses technical standards and procedures that if follows in order to ensure and maintain stability, security and resiliency of the DNS Root Server system. This should change, and one of the options is transition of the DNS Root Zone Technical Maintainer functions from VeriSign to a PTI multistakeholder entity outside of the US jurisdiction.

5. In order to strengthen stability, security and resiliency of the Internet's Unique Identifiers systems and functions related to its operation, harmonization of standards might be a positive effort. Currently, technical standards related to operation of the Internet's global infrastructure are standardized within the IETF work stream. However well-established and efficient, this framework lacks legal power and legitimacy in terms of national and international law. At the same time, ITU which is legitimate UN agency conducting work on standardization in the telecommunication sector, has not been involved in development of the Internet standards. One option for future consideration, including the WSIS +10 Summit discussion in December 2015, might imply intensification of collaboration between IETF and ITU on standardization matters. In particular, it might be a mutually beneficial effort if the ITU launches

initiative on recognition and incorporation of the IETF standards related to the Internet's global infrastructure, into its own system of standards. That could increase legitimacy of the IETF standards (and IETF itself) for nation states and generate additional incentives for compliance with such standards by the operators of the Unique Identifiers infrastructure on national and local levels. At the same time, it would not imply overtake of the IETF role in the Internet governance institutional architecture by ITU as an intergovernmental format.

The key recommendation for issues within IANA Transition agenda to be achieved by 2017 might be formulated as follows: to ensure of the transition of oversight of the technical functions related to the Internet's global infrastructure operation, including transition of the IANA functions and VeriSign DNS Root Zone Maintainer's functions from the US Government to multistakeholder community on the principles of transparency, accountability and guarantees to the international community.

Additional information:

1. Demidov Oleg, IANA Transition: A Russian View from Singapore, The PIR Center Blog, March 28, 2014, < http://www.pircenter.org/en/blog/view/id/163>, last accessed on April 30, 2015.
2. Kassenova Madina, Global Internet governance in the context of international law, *Security Index*, No 1 (104), Spring 2013.
<http://www.pircenter.org/media/content/files/10/13559079720.pdf>, last accessed on April 30, 2015.

Documents:

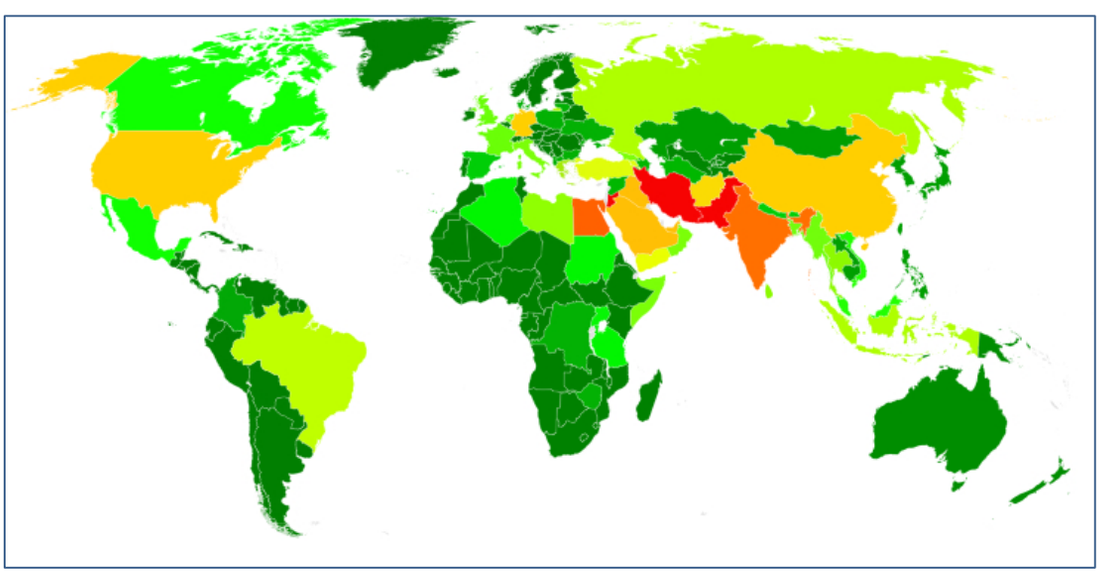
1. IANA Functions Contract, 2012 Contract, NTIA website, U.S. Department of Commerce, <http://www.ntia.doc.gov/page/iana-functions-purchase-order>, last accessed on April 30, 2015.
2. Verisign Cooperative Agreement, National Telecommunication&Information Administration, United States Department of Commerce, <http://www.ntia.doc.gov/page/verisign-cooperative-agreement>, last accessed on April 30, 2015.
3. NTIA Announces Intent to Transition Key Internet Domain Name Functions, National Telecommunication&Information Administration, United States Department of Commerce, Marh 14, 2014, < http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>, last accessed on April 30, 2015.
4. NTIA IANA Functions' Stewardship Transition, Internet Corporation for Assigned Names and Numbers, < https://www.icann.org/resources/pages/transition-2014-03-23-en>, last accessed on April 30, 2015.

VII. Leviathan on the Net: Protecting the Right to Privacy in the Digital Age

Over a short period of time starting from June 2013, Edward Snowden, a former agent of America's National Security Agency (NSA), has exerted enormous influence on international politics, as well as the public and expert debate on ICT, Internet governance, and especially the issue of privacy on the Internet. The community of technical experts on information security had already had a pretty clear idea of the practices revealed by Snowden to the general public, including mass and systemic Internet surveillance by some governments, who spy on their own and foreign citizens. Nevertheless, the effects of those revelations have been profound and irreversible. The facts disclosed by Snowden have demonstrated to political leaders and the international community the depth of the crisis of confidence in relations between governments and their international partners, as well as their own and foreign citizens. The effects of Snowden's disclosures on international politics go well beyond the blow suffered by America's reputation on the issue of protecting human rights and freedoms online.

These effects are much more profound. The scandal has essentially demonstrated that ICT and the Internet are not just a global engine of progress but also an instrument of systemic unilateral control by some governments over society and foreign partners. The information disclosed about the NSA surveillance programs is not fundamentally new for technical specialists. Nevertheless, it has highlighted the fact that cyber espionage, cyber sabotage, and illegal gathering of personal data online, when ramped up to a certain scale, can confer a strategic advantage to the countries that practice such methods. They also represent a strategic threat to the security and interests of the targets of such programs.

Map 9: Global scope of NSA electronic surveillance



Source: The Guardian. Boundless Informant: the NSA's secret tool to track global surveillance data, 11 June 2013, <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining, last accessed on April 30, 2015.

Color legend: **dark-green** signifies low espionage activity by the NSA; **red** signifies massive activity.

ICT and the Internet have created new opportunities for espionage and intrusion into private life:

- Global nature: the campaign by the NSA and British secret services simultaneously targeted dozens of countries, including their own allies (members of NATO and U.S.-led coalitions).
- Mass scale: this was probably the first completely non-selective campaign of personal data gathering and surveillance in history. Every citizen has become a target of electronic surveillance by default as a result of the development of Big Data technologies and infrastructure.
- Clandestine nature: the NSA's technological arsenal has enabled it to gather personal data of tens of millions of users (including political leaders from other countries) for years, keeping the whole thing secret until the summer-autumn of 2013.
- Safe and secure nature: despite the political and reputational losses, the United States has not lost a single agent or a single piece of equipment as a result of Snowden's disclosures, thanks to the trans-border nature of the Internet that has eliminated the need for the presence of agents on the ground.

Edward Snowden's revelations have had some clear positive effects. In particular, they have stimulated a new round of debate about the need to develop international norms of responsible behavior by governments online.

Also, the technical community is busily discussing the reasons for the pervasive online surveillance campaign organized by the NSA and British secret services. In terms of its architecture, technological instruments, and forms of government regulation, the Internet had long been regarded as the best medium for secure anonymous communications. Obviously, these views were increasingly being questioned even before Snowden's revelations because of the widespread cyber espionage campaigns, hacking attacks, and growing online activity of governments. But the events of 2013 made it perfectly clear to the general public that the Internet has become a glass house as far as the privacy of the users' personal data is concerned, and that secret services can get their hands on almost any bit of online information they want.

As a result, the technical community found itself facing the following questions:

- Is the phenomenon of large-scale government espionage in the Internet an accidental malfunction of the system, or a systemic defect inherent in the existing Internet governance architecture?
- If the reason is a systemic defect of the Internet and its governance system, then what technical and institutional steps are required to address the problem?

Table 8: Key revelations by Edward Snowden

№	Program codename	Brief description
1.	The Bullrun program	Starting from 2000, the developers of encryption tools in the United States were engaged in half-voluntary, half-forced cooperation with the U.S. National Security Agency (NSA) and other American secret services. Yielding to pressure or commercial incentives, the developers have been leaving various hardware and software backdoors in their products used by IT services, banks, and other clients - including foreign ones. Essentially, according to Edward Snowden, major U.S. information security software vendors were purposefully providing backdoors and embedding other fundamental vulnerabilities into their software. As part of the SIGINT program, which is related to Bullrun, the NSA was spending up to $250 mln annually to bribe companies into leaving backdoors in their commercially marketed software products. The methods used by the NSA as part of Bullrun program undermine the foundations of Internet security and violate its underlying principles, including trust to security solutions generated and competing at the global open market. That is why they pose a fundamental threat. A consensus opinion of cybersecurity experts on the NSA activities in this area was summarized by a prominent U.S. cybersecurity expert Bruce Schneier, who said, "The U.S. government has betrayed the Internet".
2.	Purposeful exploitation by NSA of critical vulnerabilities in major cryptography standards and algorithms unknown to end-users and the industry	Apart from making cybersecurity vendors to plant vulnerabilities in their data protection products and cryptography solutions, NSA also exploited the critical vulnerabilities in major cryptography standards and algorithms (AES, OpenSSL) of which even their developers presumably were not aware of. Thus, according to Edward Snowden, NSA hacked the SSL cryptography protocol by 2011 or earlier; for the moment, various modifications and versions of SSL still constitute the most popular and widely used cryptography solution for communications on the Internet. To strengthen and expand its capacities to crack encryption, the NSA also created an integrated database of encryption algorithms in order to facilitate instant real-time generation of crypto keys to these algorithms and cark them as quickly as possible. According to recent revelations in 2014, the NSA also for any years practiced exploitation of *Heartbleed* – a critical vulnerability in the OpenSSL cryptography packet. Neither industry vendors, nor end users were not aware of the vulnerability until it was revealed by cybersecurity experts; according to the estimates before first patches were urgently released, up to 66per cent of websites on the Internet were subject to Heartbleed and could be successfully attacked with its help. Though the vulnerability has been in place for 18 years, and the NSA reportedly knew about it for a number of years, the Agency not only did not share information with anyone, but also exploited Heartbleed to its own benefit till the vulnerability was ultimately disclosed.
3.	Program "Follow the money" and Trackfin database	At least since 2011 NA was conducting systemic surveillance after transactions of individuals and corporate clients via the global payment system Visa, and also was monitoring transactions between banking institutions via SWIFT. As part of the program, records have been accumulated for a total of 180 million operations, of which credit card operations by private individuals accounted for 84%. In 2012, if not earlier, the NSA gained access to the SWIFT system of bank transfers, which is used for 3 billion wire transfer operations monthly. The geographic priorities of this program included Africa, the Middle East, and Europe. VISA itself denied any involvement; if these statements are assumed correct, then the conclusion is that NSA hacked the world's largest payment system.
4.	PRISM surveillance program	The PRISM program, which was launched in 2007, enabled the U.S. government to download secure information from the servers of such U.S. internet giants as Microsoft, Yahoo!, Google, Facebook, AOL, Skype, YouTube, Apple, PalTalk, and others. That information was usually accessed with the knowledge of these Internet companies, which means that they were closely affiliated with the U.S. secret services. The PRISM program has given the NSA, the CIA, and the FBI access to private email communications, video and voice chats, video recordings, photos, other information stored on hard drives, VoIP traffic (internet phone calls), all kinds of computer files transferred over the Internet, online video conferences, logins and passwords, messages and activities in the social networks - the list goes on and on. The program also has been keeping records about phone calls – both domestic and international - made by the subscribers of the largest U.S. mobile phone companies.

5.	Xkeyscore program	Global cyberespionage program sophisticated enough to intercept and steal data in numerous formats from end-user devices, servers and corporate networks. By typing in an email address, the operator could gain access to the contents of the mailbox, the contacts list, and the IP address used to access the email box. By typing in an IP address, the operator could see the list of all the websites visited from that address, all the logins and queries entered from it, and all the documents viewed. He is also able to break into accounts on social networks and intercept chatroom messages. The program keeps records about all connection sessions, intercepts and stores all text communications logs, identifies the nationality of the subject based on the contents of intercepted email communications, and highlights any anomalies in communications, such as the use of PGP-type encryption programs to browse the Internet. The program could even identify the original author and source of the documents copied or transferred via the Internet. The Xkeyscore infrastructure reportedly included on 700 servers, most of them physically based in the U.S. embassies and consulate offices in other countries; there is a server in Moscow as well. For the moment when Edward Snowden made his revelations in Fall 2013, further NSA for this program included new capability to intercept VoIP and geo-positioning (GPS) data.
6.	Proactive cyber operations of the U.S. special services in Russian, Chinese, Iranian and other foreign networks	According to the classified budget of the U.S. secret services revealed by Edward Snowden, 4.3 billion dollars was allocated to finance operations in foreign networks in 2013. In 2011, some 231 such operations were conducted that were described as proactive, i.e. offensive. In particular, apart from preventing intrusions into U.S. networks, a number of these operations pursue the purpose of "preventing nuclear weapons proliferation". These activities could hardly be regarded out of the context of sophisticated cyber espionage and cyber sabotage campaigns conducted primarily in the Middle East since the end of 2000s and allegedly targeted Iran and its nuclear program (Stuxnet, Flame, MiniFlame, Gauss, Duqu, etc.). Moreover, in 2013 Edward Snowden also confirmed that creation of Stuxnet and its deployment at the Iranian uranium enrichment facility in Natanz was part of the Olympic Games operation deigned an implemented by CIA in cooperation with the U.S. and Israeli militaries and special services.
7.	Covert interception by GCHQ and NSA of communications (mobile phones, emails) of political leaders of different countries, including U.S. and British allies and partners	A number of eavesdropping operations were conducted from the Menwith Hill spying station in the UK; the results are unknown. In 2009, the U.S. and British secret services broke the encryption used by Blackberry smartphones to intercept phone calls and messages between the G20 delegates. In 2009-2013, the list of targets of these eavesdropping activities included, but was not limited to the Russian President Dmitry Medvedev (in 2012), the Mexican President Felipe Calderón, the President of Brazil Dilma Rousseff and the German Federal Chancellor Angela Merkel.
8.	Surveillance programs by the British Government Communications Headquarters (GCHQ): Tempora, Mastering the Internet and Global Telecoms Exploitation	The program Tempora was deployed in order to collect vast amounts of information about phone calls and Internet traffic. The data collected by the program could be stored for up to 3 days; the metadata was stored for up to 30 days. The program recorded phone calls, email exchanges, instant messages and personal data on Facebook and other social networking services. In 2011, some 200 broadband lines, each with a 10 Gbps capacity, were used to obtain, process, and store information as part of the Tempora program. As of 2013, the British government was planning a tenfold increase in the surveillance broadband capacity. The list of the targets of this intelligence-gathering operation has not been disclosed; experts described it as "endless".
9.	NSA's espionage on private business including foreign strategic companies	The NSA was systemically intercepting phone calls and email exchanges by senior executives of the Brazilian oil giant Petróleo Brasileiro S.A. (PetroBras). Infuriated by this discovery, the Brazilian President Dilma Rousseff noted that "PetroBras is not a threat to the national security of any state". However, the company is a very large and strategically important actor of the Brazilian economy, with a market capitalization of over 100bn dollars, gross annual revenues of 144bn, and an 80-per-cent share of Brazil's national oil output (as of January 2015).
10.	NSA programs RAMPART-A, Optic Nerve	The programs RAMPART-A and Optic Nerve enabled massive-scaled interception and collection user data by NSA from all over the Net due to direct access to backbone fiber-optic infrastructure. The access was achieved through tapping fiber optic cables. The infrastructure installed by NSA as a part of the program allowed for processing of a 3 Tb/sec stream of covertly intercepted user data. According to Edward Snowden, NSA was running the program enjoying collaboration with numerous partners – the list includes over 30 nation states, including Denmark and Germany.

Recognition of a systemic problem with the mechanism of Internet governance could have far-reaching consequences on the architectural and technical level, including the level of basic technical infrastructure of the Internet. These could include changes in the parameters and instruments of protection from the interception of data packets for the most ubiquitous application and transport-layer protocols (HTTP, TCP/IP, and others), as well as online encryption standards. Such proposals were voiced at the IETF meeting held in November 2013 in Vancouver.

Even though it has been more than a year since Snowden blew the whistle, there are still no clear answers to these questions. We believe that formulating these answers will require professional work by experts, including members of the technical community listed in Section 7 (IAB, IETF, IANA, ISOC, W3C, and others). The venue for such work could be provided by the IGF as part of the initiative to strengthen and reform that body and of the efforts to negotiate an international treaty on the principles of Internet governance. The standing Executive Secretariat of the IGF could set up an expert commission to study the fundamental weaknesses of the Internet architecture and governance system.

It is important to ensure that not only technical experts but also government representatives are engaged in that effort. That includes government representatives from the countries that were targeted by the NSA and GCHQ surveillance programs (which does not rule out the involvement of U.S. and U.K. representatives).

If such a format of cooperation between technical experts proves productive, it could produce some practical recommendations aimed at reducing the Internet's vulnerability and the technical scope for large-scale personal data gathering online.

Regardless of the conclusions to be drawn by technical experts, there are several obvious areas on which efforts to reduce the scope for mass online surveillance should focus:

- The main application and presentation layer Internet protocols must be strengthened; this has already been highlighted by IETF representatives. Inasmuch as possible, all Internet traffic must use the protected and encrypted HTTPS protocol by default.
- The fundamental vulnerabilities in the most ubiquitous encryption algorithms and standards (SSL, RSA) that have been exploited by secret services must be eliminated. At the regional level these efforts could include the promotion of "non-traditional" information protection standards, such as the Russian GOST system of encryption standards, which is already becoming quite popular in some foreign countries (especially in the Arab world).
- Efforts should be made to encourage the development of network communications that rely on new technical solutions, including networks that can work both within and outside the Internet framework (such as Mesh, P2P, and other networks). Other possible options could include anonymizing solutions such as TOR, but only if ways can be found to prevent their use for illegal purposes (that issue lies outside the remit of technical experts).

One of the measures that require support at the level of cooperation between governments and business is the so-called corporate transparency reports that are increasingly being practiced by such Internet giants as Google, Facebook, Yahoo!, Microsoft, Twitter, and others following

Edward Snowden's revelations. Voluntary disclosure by corporations of information about storage and use of user data, including responses to government requests for such data, does not give users protection against actions by secret services. Nevertheless, such instruments increase user awareness of the protection and processing of their data, and encourage a more active position on this issue by civil society. Recent transparency reports show a steady increase in governments' interest in user data. According to the Google report for January-June 2014, the number of government requests for user data rose by 15 per cent in the indicated period, and by 150 per cent in the past five years.

Finally, there are several tasks facing governments and other stakeholders at the international politics level:

- Reduce the scope for global online espionage at the hardware and technical level. Opportunities must be explored for limiting the circulation of and criminalizing the software used for electronic espionage. Of course, such measures cannot address the entire arsenal of instruments used by the NSA. Nevertheless, "spying" software (programs used to eavesdrop on voice communications, key loggers, PRISM, Optic Nerve, etc.) which is not always classed as malware, forms a separate market niche. Still, effective criminalization and suppression of that niche is entirely possible with adequate international cooperation mechanisms, such as the proposed global UN document on fighting trans-border cybercrime.
- Up until now, not a single attempt at outlawing mass online espionage and violation of the right to privacy on the Internet has yielded tangible results. Neither the final document of NETmundial, nor the UN General Assembly Resolution A/RES/68/167 of December 18, 2013 is legally binding. Neither document contains any specific measures to bring governments to account for mass online espionage.

If episodes such as the ones disclosed by Snowden in 2013 are repeated, possible mechanisms of international legal responsibility for such violations could include international sanctions.

With sufficient consolidation of the international community, a new UN General Assembly resolution could formulate advisory criteria and conditions of imposing commercial, procedural, and/or other sanctions on countries caught pursuing mass electronic espionage programs. Possible criteria for imposing such sanctions could include:
a) Clear violation of the right to privacy, as demonstrated by the nature of the data being collected (personal data, private correspondence, etc.), with the exception of metadata. For governments and organizations, this criterion could include gathering confidential, commercially sensitive, or classified data.
b) Indiscriminate mass surveillance on the Internet (i.e. programs targeting large groups rather than individuals, or total non-selective surveillance)
c) Threat to global security, i.e. when governments go beyond their national borders and collect online data about foreign citizens, companies, and other entities from other countries
d) Systemic nature of surveillance programs, i.e. programs that cannot be described as one-off actions taken accidentally or erroneously; cyber espionage and personal data gathering programs that are conducted on a permanent or long-term basis; evidence of special infrastructure being built specifically for clandestine gathering of online data.
e) Absence of any special circumstances that would justify mass cyber espionage. Possible examples of such circumstances could include the situation in the United States in the

immediate aftermath of the 9/11 attacks, when the country and the general public were facing a clear and present threat, and when there was an urgent need to gather information that could prevent further attacks.
f) Evidence of the political leadership being responsible for cyber espionage programs, i.e. when such programs are planned and authorized at the decision-making level that implies awareness by the top political leadership rather than rogue intelligence officers.

In practical terms, there would be little point trying to explore the possibility of such sanctions via the UN Security Council mechanism. But a possible UN General Assembly resolution could serve as a template for regional organizations, including the EU, the Council of Europe, OSCE, and ASEAN. These organizations could explore the possibility of sanctions such as restrictions on ICT cooperation and bans on exports of some types of ICT products to countries caught waging global cyber espionage programs. Another possibility is procedural sanctions, such as suspension of membership and/or voting powers at various international organizations.

A discussion of such a UN GA resolution could be held at the UN Group of Governmental Experts or the Internet Governance Forum.

Additional information:

1. Kulikova Aleksandra, Transparency reports and confidentiality policies of ICT corporations before and after Snowden revelations. The CyberPulse, The PIR Center E-newsletter, No 1 (108) 2014, <http://www.pircenter.org/media/content/files/12/14011883610.pdf>, last accessed on April 30, 2015.

Documents:

1. Report on IETF 88 Vancouver, 4-8 November 2013. Council of European nTLD Registries, <https://centr.org/system/files/share/centr-report-ietf88-20131115_0.pdf>, last accessed on April on 30, 2015.
2. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, < http://www.wassenaar.org/>, last accessed on April on 30, 2015.

VIII. BRICS: Synergy Potential for Global Internet Governance and Cybersecurity Agenda

Today the BRICS states constitute one of the most massive and rapidly growing segments of the global Internet community. In 2013 total number of Internet users in BRICS states exceeded 900 million (which accounted for 38per cent of the world's Internet audience) while still undergoing a rapid growth ranging from 10per cent to 41%. The total contribution of the Internet sector to BRICS economies in 2013 topped $500 billion, and yet the forecasts say it will double by 2015. In the nearest future BRICS will represent the most numerous and active part of the XXI century's digital society.

Table 9: Demography and the use of the Internet in BRICS countries (as of September 2014)

Country	Population as of March 2014 (thousands)	Number of Internet users as of June 2013 (thousands)	World rank by the size of Internet audience	Internet penetration rate as of June 2013, %	Share of the global Internet audience as pf June 2013, %
Brazil	201,032	99,358	5	49,4	4,13
India	1,242,580	151,599	3	12,2	6,30
China	1,363,780	568,192	1	41,7	23,62
Russia	143,666	75,926	6	52,8	3,16
South Africa	52,981	20,012	25	37,8	0,83
BRICS	**3,004,039**	**915, 087**	**---**	**38,8**	**38,01**

At the same time, this remarkable statistics only stresses the underrepresentation of the BRICS states in the field of global Internet governance and cyber governance. As the developments in 2014 show, the forum was not able to consolidate and articulate the voice of the non-Western world and the developing countries on vital issues related to the ICTs in international security and global governance field. Neither the global discussion on transition of the oversight of the critical Internet functions, kick-started by the USG statement from March 14, 2014[8], nor the attempt to set global rules to stop uncontrolled governmental surveillance in the Internet which emerged and failed at the NETMundial summit in April 2014, didn't reveal any consistent and concrete BRICS position on these issues. Even when taking the lead, the giants of the non-Western world preferred to act in their own capacity – like Brazil who hosted the NETMundial summit.

In fact, the ICT agenda remains a "missing pillar" in the BRICS identity and agenda, as its elaboration has been limited to trivial passages on the benefits of the global ICT revolution repeated in each BRICS Summit declaration. This situation seems to be a paradox taking into

[8] The IANA functions oversight transition, see details: IANA Accountability Transition: A Russian View from Singapore, Oleg Demidov, 05.04.2014, PIR Center, <http://pircenter.org/en/blog/view/id/163>, last accessed on April 30, 2015.

account the immense role of the forum's states in the global ICT sector, and their intensive cooperation in other areas, such as reform of the global financial architecture. More than that, in fact neither of the BRICS "baskets" and pillars can be truly successful without addressing the ICT issues – just because both finances, economic growth, security, science and education today are equally dependent on Internet and other digital technologies.

And finally on the issue why BRICS itself does need this "ICT basket": the transborder nature of the Internet makes the BRICS format free of its most serious weaknesses such as clash of regional interests and mismatch of geographically determined agendas. Instead, the Internet brings BRICS states and its stakeholders together, and this is a chance not to miss.

So what could BRICS states do in order to claim its leadership on crucial ICT issues today, in less than a year before the summit in Ufa?

1. First, to provide a consensus-based vision of the new global Internet governance architecture. The agenda for the WSIS+10 Summit – a milestone event, which is going take place in the end of 2015, should have been shaped by now, and BRICS has full potential to raise its voice on the behalf of the non-Western world. One of the states of the forum – Brazil – demonstrated a very smart move in April 2014 by adopting the Marco Civil Act – a national law on the Internet, codifying the core principles of the national policy with regard to the Net.

Today, one year after Edward Snowden revelations, everyone slammed massive governmental e-surveillance – but no one provided a vision of checks and balances for the international community aimed at limiting and preventing such precedents in the future. No one was able to formulate a global Marco Civil – a Set of Principles of the Internet Governance, fixing some truly important things. Those might include: 1) limits to governmental e-surveillance and responsibility of states for conducting it; 2) the right for access to the Internet; 3) globalization of the Internet governance, implying responsible international and multistakeholder control over the Internet's critical functions (the IANA functions). The document could also encompass already existing and widely accepted basic principles like the multi-stakeholder approach, network neutrality, openness, integrity, universality of the Internet, etc.

The draft Set of Principles of Global Internet Governance might be regarded as a milestone document summarizing the updated vision of all stakeholders and reflecting the major changes in this area since the adoption of the Okinawa Charter on Global Information Society of 2000. However, unlike the Okinawa Charter, it should be perceived as a next and unprecedented step in this field – a codification of the principles of Internet governance that could be adopted in the form of the UN Convention or a Treaty. Thus, the idea is to negotiate and state the core principles of the global stakeholder interaction in the form of a legally binding act – which makes a great distance from the declarative status of the Okinawa Charter. At the same time, being just a list of key principles, the document might be regarded as a loose analogue of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies adopted on 19 December 1966. The idea is the same – the document does not fix any liabilities of particular Parties, but rather postulates the universal principles of cooperation.

However, effective engagement of the global community in the work on such a document requires strengthened institutionalized global and multistakeholder framework for the global Internet governance. In particular, the mechanism and mandate of the Internet Governance Forum (IGF) might be developed and transformed in order to establish a permanent IGF Executive Secretariat that would work on a multistakeholder basis under the UN auspices on the key goals and issues of the global Internet governance agenda. The 9th IGF was conducted in Istanbul on September 2-5, and the it was marked with calls to strengthen its format and its contribution to the global Internet governance transformation.

Of course, BRICS states cannot and should not be the only initiators and conveyers of this process since it is obviously a global initiative that requires contribution from all stakeholders and all regions. However, the BRICS leaders might take the lead of this process in order to make it more oriented towards the developing world and stressing the changes in the global composition of stakeholders towards the non-Western fraction.

The BRICS states could not only provide diplomatic support for this initiative and promote it internationally (including next IGF and the next BRICS Summit), but also take a leading role in technical and administrative work on establishment of the Executive Secretariat. Moreover, they might bring up the initiative of hosting this Secretariat – e.g. in Brazil, South Africa or Russia, which might be a proper reflection of the rising powers' increasing role in the ICT and Internet governance agenda.

2. Next Big Issue is determination of the roots and reasons behind the massive governmental surveillance in the Internet. Revelations made by Edward Snowden in 2013 made the global technical Internet community and policy makers face a fundamental question: is systemic and global governmental surveillance in the Net a bug, or a feature of the existing global Internet governance model? The answer might imply very concrete and far-reaching consequences on the technical level.

Acknowledging massive e-surveillance a direct consequence of systemic malfunction of the Internet architecture in its present day form might imply far-reaching consequences on the technical layer. Let alone policy makers and the issues of trust in the international relations, this conclusion might trigger significant revision and update of the technical backbones of the Internet. This includes the work of basic Internet protocols (HTTP, TCP/IP) and traffic encryption standards. Such ideas already were announced at the meeting of the Internet Engineering Task Force (IETF) that took place in November 2013 in Vancouver, Canada.

To take the lead in this investigation effort, the BRICS states could facilitate the establishment and work of a Research Committee on Fundamental Risks of the Internet Governance Architecture in the framework of the IGF Executive Secretariat - or within some other UN-based multistakeholder framework. The work of the Committee should be aimed at production and discussion of a Report with recommendations to international policy makers and the global technical Internet community (Internet Society (ISOC), IETF, Internet Architecture Board (IAB), regional Registries, etc.).

3. However, most thorough investigation of the reasons behind the massive e-surveillance would be fruitless if its conclusions are not used for creation of mechanisms, undermining the

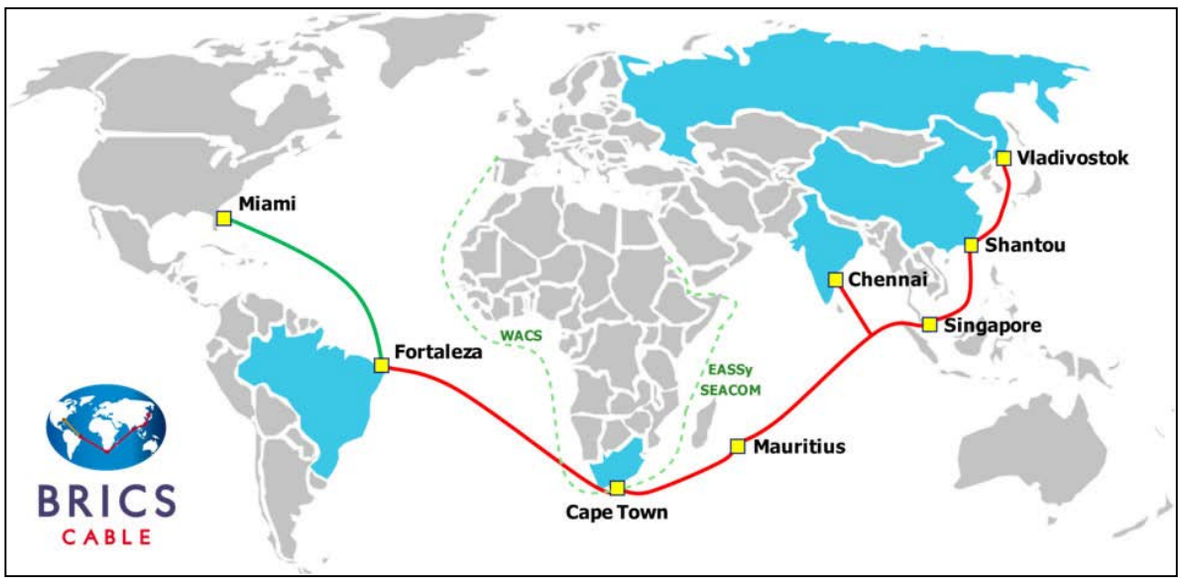
incentives for such behavior on the international level. What could BRICS do in this part, since no law or Set of Principles is able to make NSA and similar structures in many other countries to quit its activities? Building the "confidence matrix" in the field of the use of ICTS might be a strategically wise move. This is just what Russia did on the bilateral level, striking a set of three agreements on CBMs in cybersecurity area with the USA on June 17, 2013, despite its tensions with Washington on security issues and even despite the following outbreak of the Snowden scandal. Intensive cooperation of national CERTs, control of potential cyber-conflict escalation with the help of urgent high-level communication hotlinks, and exchange f data between national Nuclear Risk Reduction Centers turned out to be a good basis for mutual trust building even between the two difficult partners. Half a year later similar mechanisms were adopted for the OSCE, and the ASEAN is now on the way to similar CBMs.

BRICS could also make use of the CBM instruments even despite the obvious lack of trust between some of its members (etc. China-India). In addition to sharing information on major abnormalities of transborder traffic and cybersecurity incidents parties to the CBMs agreements could join their forces for monitoring cyber espionage and e-surveillance campaigns targeted at their territory and infrastructure by third parties. Here all BRICS countries have common stake, and the diversity of their cyber infrastructure in terms of geography and technology could enable a synergy in locating e-surveillance activities and tracking their source. As a further step, BRICS states might think of enabling greater openness of their own transborder flow for their partners in the forum in order to show that they do not conduct cyber espionage or surveillance activities themselves. The idea of CBMs in the field of use of the ICTs should be in demand for most countries of the forum. One potential proponent is Brazil where the President Dilma Rousseff and the biggest national oil company PetroBras became victims of the NSA e-surveillance programs.

Another potential advocate of this approach is Russia – first, because it successfully tested the format of CBMs in the information security area and is willing to foster its further development in multilateral and bilateral frameworks. However, Russia is widely known as a consistent architect of the global regime of cyber-governance aimed at prevention of the use of cyber-weapons and "digital disarmament". Therefore, the CBMs mechanism implemented in the BRICS framework might be a good tool for responding to a number of information security issues. One example is leveraging cooperation of CERTs (or creating BRICS-CERT or BRICS-CSIRT) as a part of CBMs, which also helps to counter transborder cybercrime and cyber terrorism.

In fact, the whole CBMs arsenal can be regarded as complementary to the mechanism of real-time 24/7 transborder information exchange on cybercrime and other cybersecurity incidents. Of course, this demands the level of trust that does not always take place now among BRICS states – but if the countries start with small, but effective cooperation (defending themselves together from third parties' activities) the positive result will likely be just a matter of time. Finally, the BRICS-based CBMs network in case of its successful operation might involve new members thus becoming a core for a wider international "trust network" and raising its synergy effects. That would be a good basis for a new global mechanism for fighting cybercrime and cyber terrorism that has been promoted by Russia and some its allies (e.g. the idea of a global universal UN Convention on countering transborder cybercrime).

Map 10: Project of transcontinental submarine fiber-optic BRICS cable (as of 2013)



Source: Rob Minto, BRICS: a new south-south cable, FT Blogs, Apr 16 2012, <http://blogs.ft.com/beyond-brics/2012/04/16/brics-a-new-south-south-cable>, last accessed on April 30, 2015.

Finally, one more essential component of the ICT agenda as a potential pillar of BRICS activities is joint IT-infrastructure and Internet-sector projects. They should be big in order to stimulate policy-level debates and to correspond to the size of the forum's economies. They also should be global or transregional in order to keep all BRICS states interested and engaged. For the moment, members of the forum already accumulated enough experience, technological background, financial resources and political leadership to move this agenda forward in a more dynamic way. First project of such kind probably was the BRICS Internet Cable aimed at diversification of the global network of backbone transcontinental fiber-optic cables. However, the project of the 32 000 km cable connecting Russian Vladivostok with Brazilian Fortaleza through Indian and Chinese hubs has not been finished yet though its implementation was initially scheduled for 2012-2013. Still, once it's finished, what are next steps?

The probable answer includes major software development initiatives that might bring together market demands and certain policy imperatives for the BRICS states. Therefore, the BRICS states could join their human, financial and technological resources for developing better security standards for the Internet protocols, protected operation systems and applications. Strangely, detailed recommendations on this issue were already provided specially to BRICS by the Just Net Coalition – a "global network of civil society actors committed to an open, free, just and equitable Internet"[9], established in February 2014 and bringing together both Western experts and representatives of the developing world including many Indian experts. In the

[9] About Us. Just Net Coalition website, <http://www.justnetcoalition.org/about-0>, last accessed on April 30, 2015.

Statement to the BRICS Summit in Fortaleza[10], the JNC experts identified four possible areas of synergies for BRICS states in the ICT field. One of them was "the development of new open Internet platforms and tools including in the areas like search, operating systems, data storage and cloud services given that they have the necessary skills, large internal markets and political motivation to break with the current mass surveillance and rent-seeking based business models". One should notice that this list mostly follows in line with the priorities of the "digital sovereignty" concept that is often mentioned in Russia and in many other states today. Looping the issue back to the e-surveillance, that joint activities might also include elaboration of not only protected Internet protocols, but also new cryptography standards and products, including market-oriented solutions for "civil cryptography". The BRICS-led effort might serve as an incentive for innovations on a nation-wide level, e.g. for the Russian ГОСТ cryptography market and its regulation.

Neither of these projects and initiatives should be regarded as a silver bullet for the challenges the BRICS countries face in the ICT area. Equally, the ICT agenda itself is not a silver bullet for the forum's questionable identity or relatively low practical output of its initiatives. And yet it totally meets the fundamental goal of the BRICS format – to facilitate transformation of the global governance architecture in a way that corresponds the interests and needs of the global community including the non-Western world. That's why is the missing ICT basket is vital for BRICS and BRICS countries – and not to least extent for Russia.

Additional information:

1. Demidov Oleg, ICT in the Brics Agenda Before The 2015 Summit: Installing the Missing Pillar? Security Index: A Russian Journal on International Security, Volume 20, Issue 2, 2014, <http://www.tandfonline.com/doi/abs/10.1080/19934270.2014.965968?journalCode=rsec20#.VW8Lu8_tmko>, last accessed on April on 30, 2015.

Documents:

1. Sixth BRICS Summit – Fortaleza Declaration, VI BRICS Summit, Ministry of External Relations of the Federal Republic of Brazil, < http://brics6.itamaraty.gov.br/media2/press-releases/214-sixth-brics-summit-fortaleza-declaration>, last accessed on April on 30, 2015.
2. Just Net Coalition Statement to the BRICS Summit in Fortaleza, Brazil, NewsClick, July 16, 2014, <http://newsclick.in/international/just-net-coalition-statement-brics-summit-fortaleza-brazil>, last accessed on April on 30, 2015.

[10] Just Net Coalition statement to the BRICS Summit in Fortaleza, Brazil. Just Net Coalition website, <http://www.justnetcoalition.org/Satement-to-the-BRICS-Summit-in-Fortaleza-Brazil>, last accessed on April 30, 2015.

Working Group on International Information Security and Global Internet Governance under the PIR Center's Advisory Board

Elena V. Chernenko	Head of the Foreign Policy Department, *Kommersant* Newspaper
Oleg V. Demidov	Consultant, PIR Center
Vitaly V. Kabernik	Head of the Advanced Elaborations Office, MGIMO University under the MFA of the Russian Federation
Madina B. Kassenova	Chair of the International Private Law, Diplomatic Academy of the MFA of the Russian Federation
Alexandra V. Kulikova	"Global Internet Governance and International Information Security" Program Coordinator, PIR Center; Secretary of the Working Group
Irina Y. Levova	Head of Strategic Elaborations Department, Russian Association of Electronic Communications
Alexey V. Lukatsky	Information Security Business Consultant, Cisco Systems
Natalya A. Piskunova	Project Coordinator, "ZAO "Expotronika"
Andrey A. Romanov	Deputy Director, Coordination Center for Top Level Domains .RU/.РФ
Ilya K. Sachkov	CEO and Director General, Group-IB
Leonid L. Todorov	General Manager, Asia Pacific Top Level Domain Association (APTLD)
Alexander V. Fedorov	Member of the Advisory Board, PIR Center
Elena K. Volchinskaya	Program Director, Non-Commercial Partnership "ZAO "InfoForum"
Mikhail V. Yakushev	Member of the Advisory Board, PIR Center
Uliana V. Zinina	Advisor on Legislation and Regulation, Microsoft Russia
Elena S. Zinovyeva	Associate Professor, MGIMO University under the MFA of the Russian Federation

Oleg Demidov

Global Internet Governance and International Security in the Field of ICT Use

Report

Reviewers: Alexander Fedorov, Mikhail Medrish, Mikhail Yakushev

Proofreading: Josh White

Editor: Alexandra Kulikova

Translation into English: Ivan Khokhotva

The author would like to thank:
Vladimir Orlov, Albert Zulkharneev, Olga Mostinskaya, Andrey Baklitskiy
and the rest of the PIR Center's team

Signed off for printing: 01.06.2015
Circulation: 300 copies

PIR Press
Address: 123242 Moscow, Druzhinnikovaskaya str. 30, building 1

For questions and comments on the report, please contact Alexandra Kulikova,
the PIR Center "Global Internet Governance and International Information Security"
Program Coordinator (email: kulikova@pircenter.org)
and the PIR Center Consultant Oleg Demidov (email: demidov@pircenter.org)

Centre russe d'études politiques
15, rue du Cendrier, Case Postale 1106, CH-1211 Geneva 1, Switzerland,
e-mail: crep@pircenter.org

Printing: Raduga LLC
115280, Moscow, Avtozavodskaya str. 25
http://www.raduga-print.ru

The PIR Center's e-journal on ICTs in foreign policy and global security

Published in Russian bimonthly since 2012

- **First Russian e-journal on legal and policy aspects of cyber security and global Internet governance**
- **Actual analysis of the problems of cybersecurity and Internet governance in Russia and globally**
- **Exclusive articles and interviews with the leading Russian and world experts**
- **Regular reviews of the legislation updates and other relevant documents**
- **Announcement of the key events and conferences in Russia and abroad**

Topics highlighted:

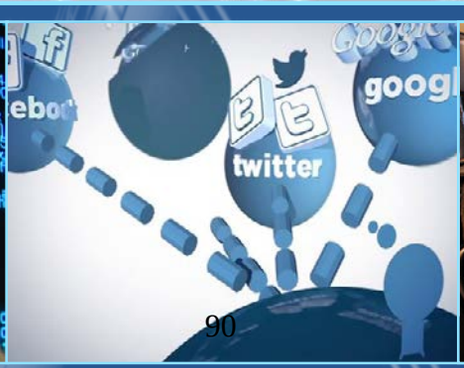
- **Cyberattacks, threats and cybercrime**
- **Cybersecurity in the USA**
- **Chinese strategy in cyberspace**
- **Global cyber governance and cooperation in cyberspace**
- **Cybersecurity and regulation of the Internet and IT sector in Russia**

Collaboration opportunities:

- ✓ **Providing site for advertising materials of your organization**
- ✓ **Thematic issues and publications on a commercial basis**
- ✓ **Publication of your analytical content in the e-journal**

Free subscription: ***subscribe.pircenter.org***

Editor: Alexandra Kulikova ***(kulikova@pircenter.org)***



Over the last few decades, digital technologies have completely altered and transformed the international security landscape and the global processes dynamics. Users, businesses, civil society structures, governments and intergovernmental organizations found themselves equally and vitally interested in mastering the tremendous opportunities brought into life by the ICTs – but at the same time, all these stakeholders turned out to be equally and critically vulnerable to the challenges that accompany the ICT revolution.

The future of global security heavily depends on finding answers to fundamental questions. How could we effectively prevent international conflicts unfolding in cyberspace without undermining rights and freedoms on the Internet? What should the future institutional mechanism of governance over the Internet's global infrastructure look like in order to meet the demands for transparency, accountability, and to ensure stability, security and resiliency of the global net? What is the path towards harmonization of national approaches to application of the international law to cyberspace, alongside with elaboration of new norms and rules of behavior in the field of ICT use?

The Report prepared by the PIR Center's Consultant Oleg Demidov with contributions from leading Russian experts representing academia, private sector, technical community and other stakeholder groups, aims to highlight these issues in details and to suggest some ideas for further search of solutions to specialists and all those interested in global security agenda.