Routledge
Taylor & Francis Group

INTERNATIONAL INFORMATION SECURITY AND GLOBAL INTERNET GOVERNANCE: A VIEW FROM GENEVA

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

The first 12 years of the twenty-first century were marked by revolutionary changes stemming from meteoric development of information and communication technologies and the internet in particular. These changes affected practically all spheres of social life and international relations from the social and political transformations in the Arab world (the so-called Arab Spring) to an unprecedented rise of hacktivism, cyberespionage, and global concern over the issues of preventing (or victoriously conducting) cyberwars, with the internet and its evolution lying at the core of all these processes. Due to the trans-border nature of the Global Net the implications of its transformation are also transnational. In particular it is true for international security, which is becoming heavily dependent on the security of cyberspace. Multiple witnesses to the latter include the establishment of military (or quasi-military) cyberunits in a number of states worldwide, the adoption of U.S. cyberstrategies in 2011 treating cyberspace as a new operational domain for armed forces, and the revelation of a number of extremely sophisticated cyberespionage and cybersabotage tools including Flame and Stuxnet malwares in the Middle East networks.

Apart from the military and strategic security dimension, the whole architecture of global internet governance has also been in the process of major transformations in recent years. The explosive growth in the number of physical devices led to a boost in communications, alongside an increase in the number and range of communication channels at the physical level, which made possible a mobile revolution on the internet, pushing the PC into second place. Other radical changes are coming at the level of IP addresses with a global migration to the new version of IP protocol (from IPv4 to IPv6) under way. A distinct revolution has been unfolding on the third level of network architecture—in the space of DNS names. A separate issue is the regulation of cross-border social networks, a true potential of which has been realized during the events of the Arab Spring and last year's riots in London. Yet, none of these issues for the moment has been settled within the framework of universal, harmonized, and comprehensive international regulation—or at least transnational cooperation efficient enough to close all blank spots and overcome challenges arising in this particular area.

However, broad international expertise is required to analyze these fundamental trends from the angle of a joint and balanced approach by the international community. Russia, as one of the world's fastest-growing internet markets and one of the major cyberpowers, is highly interested in international expert dialogue on these issues both on governmental and nongovernmental levels. The PIR Center, being one of the leading nongovernmental think tanks in Russia specialized in international security, has been paying increasing attention to the issues of information security and international dialogue in this area. With its Geneva-based European branch Centre russe d'études politiques, the PIR Center has a brilliant opportunity to initiate a discussion that would bring together top Russian and international experts in this field in order to bridge positions among expert communities and elaborate a non-governmental vision for a Russian and European joint agenda in this area. An attempt to launch such international discussion was made by the PIR Center in 2012.

ISSN 1993-4270 (print)/ISSN 2151-7495 (online) http://dx.doi.org/10.1080/19934270.2013.826948

© PIR Center, 2013 www.pircenter.org

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

On April 26, 2012 in Geneva, Switzerland, the joint extended meeting of the PIR Center's Trialogue Club International and the PIR Center's European branch Centre russe d'études politiques was held in the format of a round table dedicated to the issues of international information security and global internet governance. The event was opened by the President of the PIR Center, Vladimir Orlov; the keynote report was presented by the Chairman of the PIR Center Executive Board, Mikhail Yakushev. The list of participants in the discussion also included the Deputy Permanent Representative of the Russian Federation to the United Nations Office and other International Organizations in Geneva, Viktor Vasilyev; the Deputy Permanent Representative **of the** ***United States to the Conference on Disarmament, Walter Reid; the Vice-President of the Internet Society (ISOC), Markus Kummer, and the Director of Public Policy at ISOC, Ms. Constance Bommelaer; the Head of Section for Caucasian, Central Asian, and Eastern European Countries, Division for Certain Countries in Europe and Asia at the World Intellectual Property Organization, Alexander Matveev; the Strategy and Policy Advisor at the Corporate Strategy Division of International Telecommunication Union, Jaroslaw Ponder; and the Programme Lead of Emerging Security Threats Programme at the United Nations Institute for Disarmament Research, Ben Baseley-Walker. One of the leading European researchers and theorists of information technologies, Professor for Civil, Commercial and European Law at the University of Zurich, Rolf Weber, gave a commentary on the keynote speech by Mikhail Yakushev.***

VLADIMIR ORLOV (PIR CENTER): Currently the PIR Center is in the process of developing the project on global internet governance and international information security as it is seen in Russia. There are quite a few problematic areas in this regard such as cloud computing and cloud technology security, identification in the internet, and the use of social networks. Sometimes I feel that we are overwhelmed by a number of topics which are packed in that one title of the project. Of course there are many legal issues resulting from Russia's nonparticipation in the Budapest convention and other instruments of hard and soft law aimed at effective countering of transborder cybercrime. So our ambition at the PIR Center is to embrace all this multilayer subject field—from the legal to the technical dimension and further to a practical policy level.

The PIR Center is interested in the whole complex, but the major issue is of course the *policy*—how the policy is influenced;, how the policy may or should be changed to adjust to realities and to keep in mind the global development. So this is what we had in mind when we started the project. So let us get started with the very first large meeting within this project. Key issues I would like to discuss today are including changes in the principles of internet architecture and global internet governance, a new agenda of international cybersecurity regulation and key challenges emerging in cyberspace—and, of course, the role of Russia in all these issues.

INTERNET ARCHITECTURE AND LEVELS OF INTERNET GOVERNANCE

MIKHAIL YAKUSHEV (PIR CENTER): First of all I should point out the difference in definitions and wordings of what we are talking about. In the Russian language and Russian diplomacy they prefer to use different words from the widely accepted terms of ''internet governance'' and ''cyber security,'' introducing instead the Russian concept of ''information security,'' which is much more common internally in our country. However, we are talking about the same problems and the same issues—probably in different words. Ultimately, we should try to understand each other and try to speak the same language.

Internet governance has a lot of aspects, just like any other complex aspect of international security. When we talk about outer space exploration and its legal and political implications, we should bear in mind the principles of outer space activities, as well as the principle of liability, rights, and obligations of launching states, the legal status of the Moon and other celestial bodies, etc. When we deal with nuclear power, we have to keep attention on the issues of arms control, nonproliferation, the military and peaceful use of nuclear materials, liability of nuclear operators, etc. The same happens with the internet—it is not possible to give a short and precise answer in terms of what should be done in the sphere of internet governance, who is responsible for it, and what kind of legal treaty or a convention should be developed in order to fill the gaps and to answer all the questions. In fact when we are talking about the internet we are sometimes talking about totally different things that altogether constitute what we call the internet. The

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

technical infrastructure, telecommunication channels, and various types of equipment which provides access to the network can be mentioned here. The network infrastructure is totally different from what we had in the age of traditional telecommunications like the telegraph or telephone. Finally, talking about the application level we should keep in mind that the internet has become so important and particularly due to tremendous developments on this level. But even on the level of infrastructure we have different sub-levels regulated by different bodies and with different principles. Infrastructure means fiber optics, satellite channels, radio spectrum, etc. It also includes all the issues with the last-mile access, different types of access equipment, user equipment, and customer premises equipment, the regulation of which is totally different in the case of satellite stations, for example.

The same feature is also relevant when we are talking about network architecture itself—which is quite heterogeneous and remarkably diversified in a technical, organizational, and regulatory sense. In the network architecture we should differentiate between the level of the root servers—the famous 13 root servers that are the core basis of the internet located in different countries of the world. We should understand the issues of IP-addressing and now we have a wonderful picture of the transformation of the previous version of IP-addressers from IPv4 to IPv6, which changes very significantly the overall image of the internet. Now the internet is being converted from a network of persons to the internet of things, with our refrigerators, cars, and various types of electronic equipment receiving their own IP addresses and becoming able to communicate with each other. The third level of the network architecture is the domain name system, which is related to geopolitics. By now we have a number of so-called country-code top-level domains which somehow correspond to the principle of sovereignty of states. However, this year we also have a transformation to the system whereby the top-level domains will increase in number up to several hundreds or even thousands—e.g. .microsoft, .facebook, .google, .religion, .luckilyman—everything is possible under such brilliant change—and many people do not yet understand what changes should be introduced soon and what their influence will be on all of us.

Finally, on the application level there are a lot of websites—billions of them already—regulated in different ways and in different jurisdictions—but with the help of such websites we understand what happens on the internet, and exactly what the internet is used for. But the website per se must be regulated by specialized web services, just like the mass media. The mass media are regulated in different countries irrespective of whether they are online or offline and this is a very important source of information dissemination and mass communication. Soon it will not be a problem at all to find any information on the internet without using the domain name system—with the help of advanced search engines like Google—or Yandex in Russia. For example, if you would like to check what the Centre russe d'études politiques is (which organized our meeting today), it is not necessary to remember the name of this organization in the Swiss domain.ch. It is enough just to put the name of this organization—or any other organization—into Google or Yandex or the Microsoft website—and with 100 percent certainty you will be delivered to the exact location of the web resource without paying attention to where this resource is located.

Social networks are the internet of today, providing fantastic opportunities partially because social networks are not regulated at all. Most social networks are cross-border and transnational—for example the population of Facebook has recently exceeded 900 million people, which can be viewed as the third in the world after China and India. So the question is who should regulate the activities of Facebook users and what kind of body or authority this social network should have in terms of global security. A new dimension which is being actively developed right now is mobile system space. In many countries—and Russia is not an exclusion here—many people have access to the internet not through computer systems as they used to do traditionally but through mobile phones, tablet computers, and portable devices, and this also changes the landscape of the internet very significantly because there are already applications that cannot be used through a desktop computer—they are adapted for the portable devices while being useless for traditional desktops. Thus we should also talk about integration of mobile networks and computer networks on the internet, so the internet of today would be quite different from that of 2020, as well as the internet of today being quite different from what we had 15 or even 10 years ago. So this was also a kind of introduction to show you the variety of issues and dimensions we should analyze when checking what happens in the field of internet governance.

ROLF WEBER (UNIVERSITY OF ZURICH): No doubt infrastructures are important; we also realize that we have different infrastructures—it is not sufficient just to look at telecommunications networks: we have satellites, we have radio spectrum, we have more and more mobile phones. As far as Russia is concerned, as Mikhail has said, the use of mobile phones in Russia is true as well for many other countries in the world. I am quite often located in East Asia and in many East Asian countries the mobile phone is really the way to connect to the internet, and not really a computer network. So the new technologies of course also address new security issues, which we have to take into account. Now, I think I would like to go back to the history for a short moment. Why do we have the internet? The main driver was the Department of Defense, the military services in the United States; I would just like to recall the ARPANET, which has been moved more and more to the civil or private sector and military services have stepped out. Somehow I have the impression it is almost a little bit of a surprise that the more discussions are held on defense, security-oriented issues, the more they lose in importance. They have not been so crucial anymore as they were at the beginning of the age of the internet when the internet, or the technical infrastructure of the internet, was invented.

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

INTERNATIONAL REGULATION OF CYBERSECURITY AND INTERNET GOVERNANCE

YAKUSHEV: There are some very interesting discussions on the principle of sovereignty. Does the state still conserve its sovereignty in the epoch of the internet, or is there something that changes the concept of political sovereignty making it just a notion, modifying it for example to the concept of shared sovereignty? This is a really difficult question to answer or to analyze because there is a wide international recognition that there should not be any interference or any intervention into the internal political affairs of any country and, for example, no one objects to the right of China, of Iran, or of Arab countries to impose certain limits on the internet, on access to the internet, on the distribution of certain information within such countries. However, we also see the examples of Libya or Syria where there are so-called interests of humanitarian intervention, where their violation of human rights is just an explanation for why certain countries, or why certain international organizations are interested to restore the situation and to stop such kinds of violations of human rights. We also see the appearance of different international documents, national documents with international coverage, like the United States Strategy for Cyberspace (2011), which describes and fixes the principles of American behavior in cyberspace, and this provoked fierce discussions worldwide. We also see the proposals of the Russian Federation, which I will cover a little bit later. But now, unfortunately, even with all the discussions within the United Nations, we do not see the possibility of a compromise. Unfortunately, all such issues are highly politicized, and the Arab Spring, the developments in different countries, the restrictions on freedom of speech etc. do not allow us to talk about the possibility to develop a document, an international document, an international legal instrument to fill the gaps and to answer all the questions. However, it is obvious that there are a number of issues of common interest that require solution now, and that we should not wait until these problems will somehow be solved in the future.

I would like to draw your attention to the activity which was undertaken by the Council of Europe, which unites almost all countries of the European Continent and whose documents are usually respected not only by European countries, but also by the transatlantic, American, African, and Asian countries as well. In September 2011, the Committee of Ministers of the Council of Europe adopted a number of very important documents, and these documents should be considered as part of the so-called ''information security soft law.'' It is not a treaty, it is not a resolution of the United Nations, it is not a resolution of the Security Council of the United Nations. However, as Russia and most of the European countries are members of the Council of Europe, such recommendations, and such soft legal documents, are an excellent example of the possible compromise on certain issues related to internet governance, namely cross-border harm and the cross-border consequences of the activities of the states. So the Council of Europe adopted the declaration by the Committee of Ministers on Internet Governance Principles and the recommendation of the Committee of Ministers to member states on protection and promotion of the universality, integrity, and openness of the internet. They are available online.

There are 10 principles of internet governance that are commonly accepted by all European countries, member-states of the Council of Europe, like protection of all fundamental rights and freedoms. This is the introduction of multi-stakeholder governance: there are now five groups of such stakeholders—governments, the private sector, civil society, the technical community, plus the internet users. There is a principle of the responsibility of states. Internet governance very often means the rights of the states. For the first time, the Council of Europe imposed responsibility in terms of prevention of any cross-border harm, if such harm can occur as a

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

result of the adoption of certain internal laws or regulations. There are a number of cases where internal acts did cause certain harm in other countries. For example, last year a Georgian lady managed to cut a fiber-optic cable somewhere in her village and this fiber-optic cable interrupted the connectivity to the internet of the state of Armenia. What should be done to prevent such cases in the future? I do not want to just enumerate all 10 principles, just maybe mention one of them. The ninth principle states that we should prevent any traffic measures, for example giving priority to certain types of traffic and limiting access to another type of resources for political or other reasons, if such measures do not meet the requirements of international law on the protection of freedom of expression and access to information. And the tenth principle is also very important: it is cultural and linguistic diversity.

There were different attempts to elaborate a kind of international document that would answer at least some of the open questions. Here in Geneva in 2005 a number of sessions of the Working Group on Internet Governance (WGIG) were arranged by the former UN Under Secretary General Kofi Annan. All Working Group members were appointed by the UN Secretary General. The final report of the Working Group was published in 2005 and it did contain certain solutions, explanations, and provisions that really tried to answer open questions of that moment and what we managed to elaborate on in our final report which is now being further discussed in the sessions of the International Governance Forums that are held annually.

In other proposals of countries like the United States or Russia the fundamental principles of international law should be implemented in all such proposals, because otherwise it will be very difficult to protect the main ideas of such documents. For example, if we are trying to prevent a cyber-war, we should prevent illegal activities of the internet users against the state (like a cyber-terrorism war, illegal actions of internet users against themselves, which is a cybercrime). The question is whether we should also prevent illegal activities of governments against internet users.

WEBER: Definitely, one of the key questions is, to what extent do we need regulations? At the very beginning, in 1996, John Perry Barlow said in his very famous manifesto that we do not need any regulations whatsoever; the cyber world is a completely different world which does not have to look to governments or to the private sector. Obviously this has changed very much. This process has led, as has been very nicely and extensively said by Mikhail, to the definition of multi-stakeholder governance. We do now have three pillars—the governments, the private sector, and the civil society—but we also now have the phenomenon that the private sector and civil society are looking more at aspects such as the domain name system, privacy, human rights, and censorship. If you look at the topics discussed during the Internet Governance Forums (IGFs) over the last six years, we only have very remote discussions on things like cyber-terrorism and cybercrime. I am not saying that there are no virtues at all, but cyber-terrorism and cybercrime are certainly not at the core of the IGFs, at least not for the first four IGFs. This is also not so much of a surprise because things like cyber-terrorism and especially cyberwars are largely the domain of governments while the participants of IGFs come more from the civil society sector. So perhaps for these people cybercrimes might play a certain role, but they still have other crucial concerns; that is why, for example, discussions about the Cybercrime Convention of the Council of Europe were embedded into the agenda of the IGFs only after a long time. Obviously, at the ICANN [Internet Corporation for Assigned Names and Numbers] meetings these aspects did not play any role whatsoever. As a consequence we seem to be going in the direction of some kind of compromise. Mikhail mentioned the attempt by the Council of Europe to come to terms as far as internet governance problems are concerned. A couple of other governments, for example the government of Brazil and other parties, have also worked on internet governance principles. We do have attempts to come to some kind of bill of human rights in the internet. Surprisingly enough, although now such an initiative is supported by Google through an institute in Berlin with quite large resources, I do not really see a lot of emphasis in the field of local and international security, and in my opinion this would really be a field which merits further attention and which should be tackled in the near future, and in principle I would say it should be tackled before it is too late. In other words, emphasis should now also be put on security measures. I would only like to mention that there are of course a couple of documents which could be used as a basic framework for discussions. For example, the OECD, which of course is not a worldwide organization, but has some 40 member-states mainly from the developed countries, has already published guidelines on information security in the year 2002, so it is a 10-year-old document that could be used as basis for further discussions.

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

CONSTANCE BOMMELAER (INTERNET SOCIETY): I would like to add to what Prof. Weber mentioned earlier. There are already some efforts going on at the international level; Interpol announced recently that it was creating a global sourcing system, so this would provide rapid identification of any authors of criminal acts in cyberspace. I do not know how much publicity is going on around these initiatives, but I do believe that some initial steps have been taken in terms of international cooperation. Of course, these initiatives need to be balanced by the fact that there are some privacy concerns, so it is important that any effort in this direction be taken cautiously. I think some efforts are starting and we can hope that some good things will come out of it.

ALEXANDER MATVEEV (WORLD INTELLECTUAL PROPERTY ORGANIZATION): One element to which I would like to draw your attention, since I see representatives of various state organizations here, is probably a problem that we experience in international organizations today, with ICANN for instance, and the lack of protection given by ICANN to international and intergovernmental organizations. Unfortunately, since last year, all the attempts we have tried have not been successful, and ICANN agreed to provide protection only to the International Red Cross and to the International Olympic Committee; something is being done with UNICEF, but for the rest of the United Nations family, unfortunately we might face a problem, a real problem, once these first-level names were introduced and I would think that it is a matter for governments, and a matter for the public at large to consider this issue and probably to make their own contribution to its solution.

WEBER: When I tried to anticipate what he would say, I thought maybe he would look at the most recent security problem which has occurred within ICANN. I would like to try at least to react to a couple of statements and thoughts made by Mikhail. Probably, we should start with the question: What should we really do if we look at internet regulation? Is there any reason to regulate at all? Who should set the rules? Whose interests are to be covered by rules, and do we need special mechanisms? If we look back at the last 15 years since ICANN has been established and since a large community has in fact been a position to participate in the cyber world, we see some remarkable developments. We see the development from private-centered regulation to state interests and to a multi-stakeholder approach.

Apart from that, and perhaps then coming a little bit more back to the aspects which I wanted to discuss with you originally, I also do think that we need a better structured ICANN. In connection with the applications for the new DNS system there was a major security problem and apparently it was possible for applicants to get data from other applicants who had already loaded their information. The way that ICANN has reacted was not really professional in my assessment. ICANN basically said that they were doing what they could to solve this problem with security. However, there was no clear guidance on how this should have been done, or who was responsible within ICANN. There was not even a clear allocation of powers, and finally it was completely opened up to an extent that liability rules could be not applied because nobody knew what kind of damage had been caused by this security leakage. So, there is also an additional need to look into global security aspects within the whole framework of ICANN. My proposal in this light was to try come to a strong constitutional framework which should govern ICANN, since legitimacy questions cannot any longer be overlooked. I have submitted a couple of ideas as to how the weaknesses of the present system could be overcome. I am not saying we should replace ICANN, but in my opinion ICANN should become some kind of a more public interest corrector and as a lawyer I cannot come around the observation that we do not even have a legal appeal system which merits the name. The structure we need to balance the system is by far not something that could be called a court, but still we are talking about some kind of an independent review body.

JAROSLAW PONDER (INTERNATIONAL TELECOMMUNICATION UNION): Cyber security is one of the integral parts of the outcomes of the Geneva Plan of Action and the Tunis Agenda, where the mechanism for implementation has been proposed. The ITU is making the necessary efforts in order to ensure that the Global Cybersecurity Agenda (launched already in 2007 in the multi-stakeholder set up) brings fruitful effects at the global level. In fact we are entering the phase of a world review of these processes: what was expected from the summit and what the countries would like to see beyond 2015 in terms of global actions, and what we did not know earlier that we might be confronted with. That is why the contribution from the multi-stakeholder community has an extremely huge value in this and many of those issues that have been mentioned today and which will be the subject of many sessions during the World Summit on the Information Society Forum.

The forum is not only a talk-show; it is targeted at actual implementation. Listening to today's discussion, I am happy that there are concrete proposals, and we hope that they will be tabled during that week. The Global Cybersecurity Agenda (GCA) proposes the framework, but there is a lot of ongoing work with the countries in order to ensure that the global response to national, regional, and global threats is there and no civilian is scared to open their mobile or computer. One particular direction within this broad framework is the international multilateral partnership against cyber threats. One hundred and forty countries have already joined this global initiative, and several countries are being assisted via the ITU to create computer incident response teams at the national level. Sometimes the task is to create the center from scratch, and we are happy that so many countries are committed to putting this at the top of their agenda. I think this is the moment to join forces and to discuss cooperation within the framework of the GCA at each level: of course at high level, but also at the operational level in order to ensure the global response can be effective.

MULTI-STAKEHOLDER APPROACH TO INTERNET GOVERNANCE

YAKUSHEV: The most important issue introduced in the final report of the Working Group on Internet Governance is the necessity of the so-called multi-stakeholder approach—the necessity to provide and include equal participation of at least three groups of stakeholders. There are three groups of stakeholders: the government, the private sector or business, and the civil society have prospective roles. This is the fundamental principle that should be used when talking about the future development of internet regulation and internet governance, as the specific nature of the internet already brings together millions and billions of users. We have to use the knowledge, experience, and power not only of sovereign states but also that of private-sector businesses that develop the technical standards of the internet, and the civil society which is interested in multiple issues such as human rights, consumer rights, etc. Now we have a system of organizations engaged in internet governance. The list includes among others ITU and ICANN. The latter could be hardly described in terms of whether it is an international organization or a public organization. It is a non-for-profit corporation based in California but it its activities have a very global magnitude, and it is ICANN that introduces new top-level domains and regulates very important aspects of internet governance.

There are a number of common problems that require joint solutions and cooperation. First, the multi-stakeholder approach is a must in all aspects of developing and implementing legal norms on internet governance and information security. We see the same story in outer space exploration, maybe even in the participation of private companies in nuclear power or in operating nuclear power sources. So a multi-stakeholder approach for internet governance is really a must.

MARKUS KUMMER (INTERNET SOCIETY): I was very pleased and very interested to see the emphasis on multi-stakeholder cooperation; this is something we as the Internet Society very much believe in. But yes, one correction, or addition: you both refer to the three stakeholder groups, but in Tunis we actually added a fourth stakeholder group, the academic and technical communities. ISOC feels part of the academic and technical communities.

BEN BASELEY-WALKER (UN INSTITUTE FOR DISARMAMENT RESEARCH): Just a few points I wanted to comment on. I love the idea of multi-stakeholders; my colleagues enjoy events that involve conversations on the global drollness of cyber comments, how we are going to govern it, how we are going to write up policies at the national and international level. I find that 99 percent of the time you put industry, academe, policy-makers, and business in the same room you have three very interesting conferences all taking place at the same time, and there is very little effective dialogue between those stakeholders, especially when it comes to the work, the area that Mr Vasilyev and I work in, which is specifically international security dynamic. I would also say the international security community, especially at the diplomatic level, is not used to dealing with nongovernment and with industry. When the issues of nuclear weapons are in focus, there is not such a necessity to engage nongovernmental actors in the process of negotiations and establishment of a new regime—however, the situation is completely different when we speak about the international information security and global Internet governance. It is important to emphasize how much of the internet is in private hands. There is no real effective mechanism for taking people who have grown up despising government in Silicon Valley and suddenly putting them in a room full of diplomats and saying, hey, how's this going to work out? So, I think that is something to bear in mind, to look at what sort of processes are going to be affected.

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

WEBER: I would like to come back to the term ''multi-stakeholderism.'' I think multi-stakeholderism cannot mean living without a legal framework. We need something which is legally stable, which is legally resilient; I am just drawing now from the terms which are usually used by technicians. Most likely, the only source from which we can draw some kind of legal principles is international customary law. In this field we also have a couple of ISOC principles which are generally accepted in a very broad legal community.

Mikhail mentioned the outer space treaty. It is a multilateral document, but the key principles contained in this treaty would also apply to other fields. We have certain laws governing traffic on the sea. We have laws for water courses (it has been accepted for much more than a hundred years now that somebody at the source of a water course does not have a right to poison the water course with detriment to a state adjacent to the water course at a later stage). So, most likely, if we look for future projects in national security law, we would have to go through international customary law to see what kind of principles are generally accepted. There is no more or less generally accepted cross-border harm or precautionary principle stated in the Rio Declaration on Environment and Development 1992, or in certain documents of the Council of Europe or any other international bodies. Starting from such kinds of principles we could try, somehow, to discuss a debate. What could be further developed? And what could flow into some kind of new international document? Most likely it would not be a treaty because I am not so optimistic as to believe the governments all over the world would agree on such a treaty, but we could perhaps think of soft law instruments, such as, I think, principles.

WALTER REID (PERMAMENT MISSION OF THE UNITED STATES TO THE CONFERENCE ON DISARMAMENT): During discussions and negotiations on confidence-building measures (CBMs) with Russia and some other countries (despite whether or not we have the perfectly agreed legal definition in common) we have found many cases where there is no definition. Measures that we can undertake in this respect in the cyber sphere are often enabled by public–private partnerships. Mr Yakushev has obviously run into this. It is certainly the case in the US cyber-world; we cannot do a lot before we talk with private stakeholders and private actors (who respond on a collaborative, voluntary basis) and try and find real-world solutions. I think this situation will prevail in the next 10, 15, 20 years, and that's really where the predominant amount of activity is going to be. Given the absolute necessity of the multi-stakeholder model, this is a very healthy thing, and it is good that governments are reminded of that on a regular basis. So we look forward in the international community to engaging in these discussions, and particularly in the security portion.

In Switzerland there is an operation to promote a public–private partnership between the private business community and the police, called MELANI (Reporting and Analysis Centre). It is a cooperative venture, a safe space between parts of the policy community and parts of the business community most affected by cyber-crime and cyber-abuse. It is probably not going to rectify what happened to you already, but it is going to help you develop an understanding of what is going on, how to protect yourself further, and involve you in a broader user community. It has elements of public and private buy-in, it is not an official government entity that may allow you to develop a deterrent so that this doesn't happen to you in the future, and this is going on at a provincial level, and at the municipal level in many countries around the world. In the United States we see this popping up as well, in Canada too, usually at the state municipal and the sub-national level. It is an ongoing experiment in the Swiss case, but it may be an opportunity for other states including Russia.

RUSSIA AND ITS PLACE IN CYBERSECURITY REGULATION AND INTERNET GOVERNANCE

YAKUSHEV: A few words will be said about Russia's position—what are the behavior, proposals, and possibilities for cooperation—and some conclusions which could be further discussed during our interactive communication.

Unfortunately, Russia has a so-called bad-credit history. It is a perception that with the censorship, and with the political limitations that are enforced Russia should not make any proposals or be active in any way in the field of cyber-security and internet governance. The cyber-attacks against Estonia, Georgia, and later against opposition internet sites in Russia have provoked many questions, and a large number of those questions are still unanswered.

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

However, not being a Russian official but an independent research expert, I would say that all such perceptions and rumors have nothing to do with reality. In fact, Russia has a very free system and very free regulation on the internet, especially compared with Kazakhstan, China, Iran, or Turkmenistan. There are no restrictions on the flow of information; there is no censorship in internet transactions, which can of course be different from what we have in TV broadcasting or radio broadcasting in Russia. In Russia the internet really is a zone of freedom. There are no restrictions, so in these terms Russia has a very good credit history when it comes to information security and internet governance. Moreover, political declarations of our leaders have also confirmed the readiness of the government not to impose any restrictions on the freedom of the internet, which is good because certain attempts to promote the ideas of such restrictions were discussed at a high political level.

There were no regulations, no restrictions, no laws that would in any case harm the principle of the free flow of information.

However, there are certain proposals made by the Russian government that are not unanimously supported in the world, namely the document called ‘‘The Concept of a Convention on International Information Security’’ and the proposed ‘‘Code of Conduct of States in Cyberspace.’’ They are sometimes considered somehow as a response to the American concepts and strategies of the last year, but if we study and analyze the document called ‘‘The Concept of a Convention on International Information Security,’’ I would say there is nothing really dangerous or strange or unacceptable in such proposals. ‘‘The Concept of a Convention’’ has a number of definitions: what a cyber war is, or, better said, information war, information weapons, information system, etc. Russians avoid using the word ‘‘cyber,’’ they prefer to say ‘‘information.’’ ‘‘The Concept of a Convention’’ enumerates many threats to international peace and security including destructive actions in the information sphere, subversive actions, psychological wars, and information expansion. Sometimes maybe it reminds us of the rhetoric of the Cold War, when we had a famous definition of ideological war, which Americans waged against the Soviet Union. Nowadays it is slightly different, but it is in the list of main threats. There are principles on international information law. The main principle is sovereignty over its national infrastructure. It means that everything that is technically and physically located within the Russian boundaries should be bound to Russian law and this is how Russia—or other countries—is ready to exercise its sovereignty over its own cyber-space or information space. There are also measures to prevent military conflicts, information wars, measures to counter terrorism in cyberspace, and measures to counter cybercrimes, including criminal and other legal measures.

Unfortunately, such proposals were not met optimistically or favorably by many states and many experts. What are the reasons for such a negative approach? Reason number one is the lack of a multi-stakeholder approach in both the very process of initiation and preparation of such proposals and also in the format in which they are discussed on the international level. The Russian internet community was not invited to participate in developing such proposals, and that is why there are certain mistakes, certain gaps, maybe even bad wording in terms of the legal purity of such proposals, which of course prevents people from the Russian expert community from supporting such ideas. However, I would like to stress once again that there is nothing substantially bad in what Russia proposes.

As for the sovereignty of Russia over technical infrastructure in its information space, further theoretical examination is required in order to understand whether such sovereignty should be absolute. For example, the Olympic Games is a totally a non-government activity which has a multibillion financial input for the economies of many countries. But if the Olympic Games are held in a country like Russia in Sochi in two years, people will use the infrastructure in Russia, and all technical equipment will be based in Russia. However, the rules of the games cannot be established by the Russian FSB [Federal Security Service] or even by the Russian government; they are established by the international Olympic Committee and all countries, including Russia, do recognize that there are certain rules of certain activities which cannot be subject to national law—otherwise such activities cannot be carried out at all.

Of course such kinds of proposals require discussions. We need to discuss the Russian proposals, maybe we need to discuss them in connection with the U.S. proposals on their national strategy for cyberspace. But there is also a very important question of whether such Russian proposals should be seen as a replacement or as a proposal to replace the Budapest Convention on Cybercrime, neither signed nor ratified by Russia. How could these documents

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

survive together; will they compete or will they add certain value to each other? This is an open question.

ORLOV: One of the points mentioned in Mikhail's keynote speech was about the balance of government and NGO discussions in Russia over the role of the internet, over the future of the Runet, and over information security. Of course, there are some wonderful Russian authors who suggest that in 20–30 years from now there will be no internet in Russia, there will be only ''inter-da,'' or ''inter-yes,'' which would only approve the governmental decisions. One of those authors is Vladimir Sorokin; he wrote brilliantly about that. From what we hear it does not seem like that gloomy picture, obviously. I would even put another sweetener here, mentioning that the Russian authorities and the Russian government now do quite a lot to listen to the views of the Russian NGO community. It is those who are knowledgeable and to a certain extent try to learn from their findings. Mikhail was modest enough not to mention that he participated in a four-hour meeting with then President Dmitry Medvedev on these issues, an exchange which you can find on the presidential website. For me it was very interesting reading: the president uses a lot of English words, because he cannot find the relevant Russian ones. There are also a lot of clashes which I would say were positive clashes.

VIKTOR VASILYEV (PERMANENT MISSION OF RUSSIA TO THE UNITED NATIONS): I have the right not to share some of the views that have been expressed previously. One of those is actually that Russia has a bad record on information security. I would claim that we have a good record on information security; it was Russia who raised the issue of information security in the international arena to solve it, and we were from that time co-sponsoring the resolution on information security in the General Assembly of the United Nations. Of course, we will have good discussions and our participants have already shared their views and we understand that the views may differ on various aspects, because the issues are very broad.

Of course, there is also a question of freedom of speech, freedom of information and so on and so forth. What is behind the Russian position is the attempt to initiate a discussion on those issues, even despite the fact that the Western states may not share the Russian positions stated in those two documents—the conception of a Convention and the draft Code of Conduct. So now Russia and its partners are laying grounds for such a discussion, presenting the Russian position on some of those issues, and we are co-sponsoring this discussion. We are also giving some money to UNIDIR [United Nations Institute for Disarmament Research] which will hold a group of governmental experts study meeting this year and will present their views to the General Assembly next year, held to address the issues of information security.

I believe the bigger issue must be to find the areas and to identify those areas of mutual concern. Of course, we will definitely disagree on some of those areas as a result of legal differences, logical differences etc., but there are areas on which we all can agree: terrorism, criminal use of the internet, and problems with credit cards. We have to establish those areas where we can cooperate on the international balance, where we can establish norms to prevent those cases from happening, and to help the broader discussion of those broad issues about the red button, and so on and so forth, within the international arena and in order to do so we need to have a forum. And we also need to look and to consider what forums will be the most appropriate ones, be it the United Nations, UNIDIR, the International Telecommunication Union, and WIPO, who are also discussing different elements of information security. Let's do it, let's think it over, and let's establish those areas where we can cooperate.

BASELEY-WALKER: I would like to refer to the comment by Mr Vasilyev that there is nothing substantially bad in the Russian conception of an Information Security Convention. I would not necessarily want to say that the Russian proposal is either good or bad, but I am pretty sure that the position of the American government and the position of the Russian government are vastly different from each other on a very basic conceptual level. When we try to examine this fact, we see two fundamentally different in their nature answers to the question as to whether information is a weapon or not. And what I would also stress is Victor's point, and that may be the case in today's conditions—unless you take off the table an issue like the Russian project for a global legally binding UN act regulating cyberspace, agreement is unlikely. There are still many specific things where agreement can be reached, and I think it is very important not to let certain major political questions dominate the whole set of potential options for soft law, CBMs, or codes of conduct.

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

REID: To pick up on what Mr Baseley-Walker just said, from the U.S. standpoint, I would mention the following points: certainly we come at a lot of security issues, we come at a lot of the cyber issues, we use a different term—information and communication technologies versus cyber—but I very much endorse the idea that different terminology or even conceptual understanding should not halt our cooperation. We welcome this conversation and we very much appreciate that the Russians brought the issue of global UN-based information security regulation over a decade ago to the UN agenda. That's something that we engaged in very happily at once. It is an area that has ballooned in U.S.–Russia bilateral relations—and this area has developed in the form of CBMs' discussion in our bilateral relationship. I think the spirit in which the United States is engaging with Moscow now should be not to let any terminological contradictions and discussions that could drag on for decades actually prevent us from coming to very real-world understanding of each other's intentions, of how to contact each other, about how to work in a lot of areas where we have mutual goals. That's why CBMs are, from my point of view, the step that we are looking at; it is where we hope that the G2G can support us—and it is certainly in our bilateral contacts that we see a very promising opportunity to work together.

CYBER THREATS AND CHALLENGES

YAKUSHEV: International forums on internet governance are held annually. There is a network of regional, local, and national internet governance forums which are held in different locations of the world, also in Russia. So let us just concentrate on one aspect of global internet governance—internet security. There are three or maybe four levels which should be regulated in different ways and have different implications when we are talking about global information security:

- □ The level of so-called *cyber wars.* Prevention of such cyber wars is at the level of international and intergovernmental relations and international public law.
- □ *Cyberterrorism* and countering attacks against the governments and public administrations with certain political motivations and reasoning.
- □ *Cyber-crimes*—crimes committed against ordinary citizens and internet users, including all illegal actions like fraud, identity theft, etc. which unfortunately are also a very specific feature of the present-day internet.

There are a number of developments that have already been noticed on the global internet over the last five years. We also see a necessity to do something to counter illegal use of the internet and to prevent the way the internet could be used to harm global security. In most cases people start talking about such issues as the cyber-attacks in Estonia which took place five years ago where a number of critical infrastructure objects and resources were damaged and shut down. There was an understanding that the attack came from outside so it was some kind of external intervention. The Estonians were suspicious that all these attacks were arranged by the Russian government.

BASELEY-WALKER: I support the breakdown to cyber-war, cyber-terrorism, and cyber-crime. However I think what both of the previous presentations demonstrated is that they all got mixed up. It is very easy to make these clear categories, but when we actually sit down to address these things, the boundaries become very blurred. That is certainly something that the international community is struggling with substantially, that is, where do you draw these lines? How does that translate into effective regulation and effective diplomatic interaction? How do we draw the line between a state-sponsored attack and terrorism, where legal regimes would necessarily come into play, and how do you differentiate between the two? All of these questions are still very unclear.

WEBER: I think we really should discuss common topics which are of interest to many countries. The difficulty is of course that everybody is saying we have to combat cyber-terrorism. Most likely I won't find anybody who would say: ‘‘Yes, cyber-terrorism is a good thing.’’ But it becomes very difficult as soon as we ask ‘‘What is a terrorist?’’ because the notion of terrorism is of course very different in different countries. The difficulty is in the discussion's very beginning.

ORLOV: Let me draw your attention to the Olympic Games, Sochi. This is definitely something very high on the agenda both for the President-elect Mr Putin, but also here for the Swiss companies which are very closely engaged in business preparations for the Olympics. This is an interesting question, whether it is a non-government, inter-government, or whatever activity, but there is already now a war around the Olympic Games going on. The official Russian website for the Olympics was attacked and paralyzed for a few days. It was a clear sign that, closer to the games, the cyber-war will be even hotter.

I want to send a message to our Swiss colleagues here who so successfully mediated the Russia–Georgia relationship. In cyberspace it is not that easy to actually mediate. How do we prevent those DDoS attacks, who owns those magic systems, magic walls against those attacks? I found out it is just one company, which is an American company, very closely linked to the Department of Defense, that really has the solution. Hopefully we will see more developments in Russia also for prevention such types of cyber-attacks.

The correlation between cyber-security and other types of security threats deserves some attention as well. What I have in mind is nuclear security and attacks on nuclear infrastructure in Iran that have taken place already and were very successful. The attacks scared Iranians and made Israelis feel proud of the result of the Stuxnet attack. Then a series of problems echoed from the Iranian nuclear infrastructure to Russian facilities; or at least the risk of proliferation from those attacks and of course the missile facilities of Iran also face significant challenges, not physically, but through cyberspace. This is only one example which is close to me and my own research, but for me it indicates the seriousness of that combination of cyber-war and nuclear security.

WEBER: It’s easy to find an IP address. The question is whether you can gain access to the person responsible for the IP address. At least, according to Swiss legislation, this is quite difficult; this is only possible if a criminal investigation is conducted. There are court decisions from the Supreme Court and from the Court of Appeals of the Canton of Bern stating that private organizations collecting data about IP addresses are basically not entitled to divulge these addresses for any reasons to other private organizations because this would be a violation of our data-protection rules. Under a criminal investigation this impediment can be put aside; the prosecutor/general attorney is allowed to try to get the person behind the address. But, frankly speaking, it is very difficult to make a decision regarding with whom you have to file a complaint. Would it be the canton of Geneva in Switzerland, would it be the federal general attorney, would eventually the foreign prosecutor be the appropriate person? When I know which authority is competent, then the next obstacle comes: would it really be Swiss law that applies? Difficult to say. Would it be the law of the nationality of the person?

There is a very large variety of questions and therefore it is not possible to find an easy answer. In the field of international criminal law we also lack binding international treaties with the exception of the Cybercrime Convention of the Council of Europe, which is applicable not only in Central Europe, but also in Eastern Europe, Central Asia, and even a couple of countries on other continents. But ultimately we have more problems than solutions in this field.

THE RED BUTTON PROBLEM—SWITCHING OFF THE INTERNET

YAKUSHEV: We also take into consideration the example of the Arab Spring where social networks played a certain role in bringing people onto the street and organizing actions which finally ended in a change of political regimes in these countries and political change. The Egyptian case raised once again the famous so-called problem of the red button.

How can the internet be disconnected? Can it be disconnected on a global level or are there possibilities to do it step by step on a national level? What are the legal, technical, and organizational levels to disconnect a country from the internet? Can fundamental human rights principles be applied in cyberspace? What kinds of activities should not be carried out? How can relevant regulation be made that takes into account the basic rules on fundamental human rights, for example freedom of speech, freedom of information flows, and freedom to access information and to access the internet? I would like to put these questions up for discussion.

VASILYEV: The problem of what Mikhail called the ‘‘red button approach’’ is who controls this red button, whether it is possible to push this red button or not, and under what conditions someone is pushing this red button. What is the threshold for this red button? If you have no political slogans like ‘‘be independent,’’ that human rights and so on supports, you cannot press this button. Is it

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013

only hooligans against whom you have a right to press this button? This subject is a big discussion.

While Prof. Weber raised the issue of access from cellphones to the internet, it just so happens that in many countries there is no need to control the connectivity between cellphones and website providers. But let's take Russia as an example, where terrorist attacks in the Caucasus happen more or less on a daily basis and where during the subway explosions in the Moscow subway our security service had to shut down access from mobile services to the internet only to prevent further explosions (some of those explosion devices had been initiated via cellphones).

WEBER: Perhaps only a very short comment on the very interesting intervention by the ambassador. I do not think that I ever mentioned any particular comparison between different countries, because I am well aware that it should not be the case that an expert is pointing to this country or another country. Still, as I am teaching in East Asia, I would like to comment to draw your attention to the situation with the red button in this region. I am usually saying, of course, generally it is China that is trying to push red button quite often. On the other hand, Singapore is also pushing the red button very often, and Singapore is not known to be a communist country. So, we have to be really careful with this kind of comparative assessment. Technologically it is easier to disconnect mobile phones than to disconnect traditional networks, at least if businesses are interested to cooperate with the government, as was the case in Egypt where the internet was disconnected because it was invited by the government at a certain time to disconnect.

YAKUSHEV: As for the red button, of course it is a fiction. I visited the headquarters of ICANN September 2011 and I tried to enter all the rooms of this headquarters; there are no red buttons for sure. People say that it is located in the Washington office, so maybe I was in the wrong office then—this was in California. As for the red button in Russia, I am sincerely very proud to live in a country where such technologies and such techniques have never been used, so there is no censorship and there is freedom of the internet in our country and we should be proud of this.

KUMMER: There was an interesting discussion on the red button and I think both Rolf and Vladimir gave the answer. We also refer to it as the ''killer switch,'' and this is how technical experts looked at why it was possible in Egypt to turn off the internet so quickly. Basically the internet was badly built: it was too centralized. If the internet is built properly, it is very well distributed and it proves to be very resilient. In fact, that comes back to the very original mission the engineers had, to build a resilient network to withstand nuclear attack. We have seen in cases adjusted to the tsunami in Japan or the earthquake in Haiti that the internet was the only functioning communication infrastructure; all other infrastructures went down, but the internet was still up and running and people could connect via the internet. So, if the internet is built properly there is no killer switch.

Cooperation is essential. We have to cooperate, we have to discuss. The problem is, again, just as with terrorism: there is no universally accepted definition on what terrorism is and the same goes for child pornography. We do not have a universally accepted definition concerning these problems. The Internet Governance Forum is the forum to discuss problems and definitions; it is under the flags of the United Nations, it is convened under the authority of the Secretary General of the United Nations and it is multi-stakeholder and it is important when addressing these issues to listen to all the stakeholders. Governments are not in the forefront of dealing with security concerns, but it is important for governments to listen to what civil society has to say; they usually have very strong human rights concerns and it is, of course, also important to discuss with the technical community whether proposed solutions are technically feasible, and obviously all stakeholders need to work and act together.

ORLOV: We would like to join forces and engage in further broad international discussion on the principal issues of cyber security and internet governance in the future. Several issues already touched upon here today require a rapid and well-elaborated contribution from the non-governmental community (including the PIR Center) in order to provide a sound analytical background for Russian policy-makers. Thus, national policy in the area of critical infrastructure protection is still to gain systemic ground—and it is still to be decided which approach should be adopted in this field. Besides, concerns over the rapidly expanding cyber-security market in Russia are also growing with the increasing sophistication, number, and scale of criminal activities both within and outside national networks. Here, as was mentioned by speakers and commentators, Russia needs to suggest its own approach towards effective transnational cooperation in countering cybercrime, as the Budapest Convention seems not to be treated as an optimal basis for Russian participation in such activities. During this round table we have gained a very detailed and comprehensive snapshot of strategic discussions concerning intergovernmental information security regulation and Russia and the SCO's proposals in this area. What is even more important, we surprisingly came to a very clear common understanding of what should be done in order to prompt cooperation between Russia and its Western partners even with certain contradictions remaining unresolved for some time. Transparency and confidence-building measures, step-by-step multi- and bilateral give-and-take, information sharing, and permanent intensive discussions with broad engagement of NGOs and expert communities are not a panacea but still they are a recipe that works. And here we are today to make it work. Now our ambition is to continue this positive process and I hope this discussion is an initial step in a long and systemic process bringing together Russian, Western, and many other experts and decision-makers for a safer cyberspace and hampered dissemination of advantages of information technologies all over the globe.

For more analytics on information security, please, visit the section ''International Information Security and Global Internet Governance'' of the PIR Center website:
net.eng.pircenter.org

Downloaded by [Center for Policy Studies in Russia], [Evgeny Petelin] at 00:12 19 September 2013