RUSSIA-CHINA-UNITED STATES: SETTING THE GLOBAL RULES OF THE GAME IN CYBERSPACE

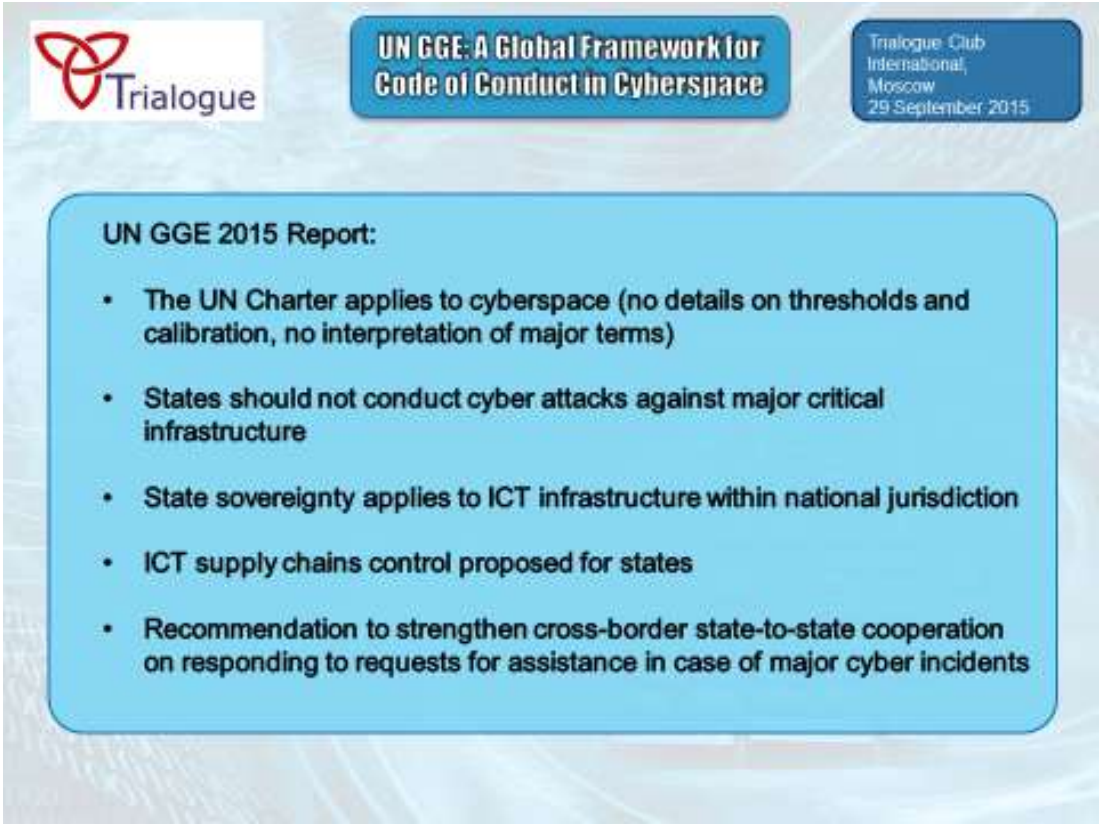
Demidov Oleg V., expert, Global Commission on Internet Governance's Research Advisory Network (GCIG RAN); consultant, PIR Center

Stenogram of the Trialogue Club International meeting
September 29th, 2015

O. V. Demidov: Distinguished colleagues, distinguished participants of the *Trialogue Club International*, good morning. I would like to say that I am really proud to be speaking here. I used to be at the Club meetings in capacity of a guest or of PIR Center's employee, but now this is the first time I am the speaker. Thank you.

I would like to make a short introduction why I am going to speak about this issue right now. Development of international process, international negotiations and international norms of conduct in cyberspace lasts for at least 15 years. Only this year we are witnessing subscription of certain documents and conducting certain negotiations creating preconditions for real breakthrough in this sphere. Key events, key progress is made at the instigation of three cyberstates in the world — namely Russia, the US and China. It is quite ironic that, contrasted with the bilateral negotiations between Russia–China, Russia–US, US–China, there is no real international legal mechanism, neither any platform that would allow these countries to negotiate their cyber policies in tripartite format. I will try to discuss certain issues that could become common for these three countries, the ways to establish this tripartite negotiation and co-operation in cyberspace.

I would like to start with introduction to the issues discussed at the global level — at the UN and other international panels. This summer the UN Group of Governmental Experts presented a report that for the first time ever proposes specific set of rules that could establish limitations for the countries in the cyberspace. The key provisions of the report are generalized on the presentation slide.



I will concentrate on problems and contradictions of this report that vector the further work of the Group, which is to meet again in 2016.

First, notwithstanding the fact the Group says the UN Charter is applicable to cyberspace, the way it is applicable is not clear, in particular in regard to three key terms defined in the UN Charter. They are *use of force* or threat of use of force in the international relations, *act of aggression* upon the UN member state and *"armed assault"*, as defined in Article 51 of the UN Charter. This question is of practical significance because the US and its NATO allies are developing their own approaches and present their conditions of such approaches practical application in the critical situation in cyberspace.

One of the sources of expert knowledge that forms NATO's approach to this problem are scientific papers of Cooperative Cyber Defence Centre of Excellence situated in Tallinn — especially *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. On the other hand, such states as the USA develop and enshrine in the law their own outlook on the development in this field. In 2015 for example, the Pentagon's Law of War Manual lists preconditions to qualify the cyberattack as the use of force or the armed assault.

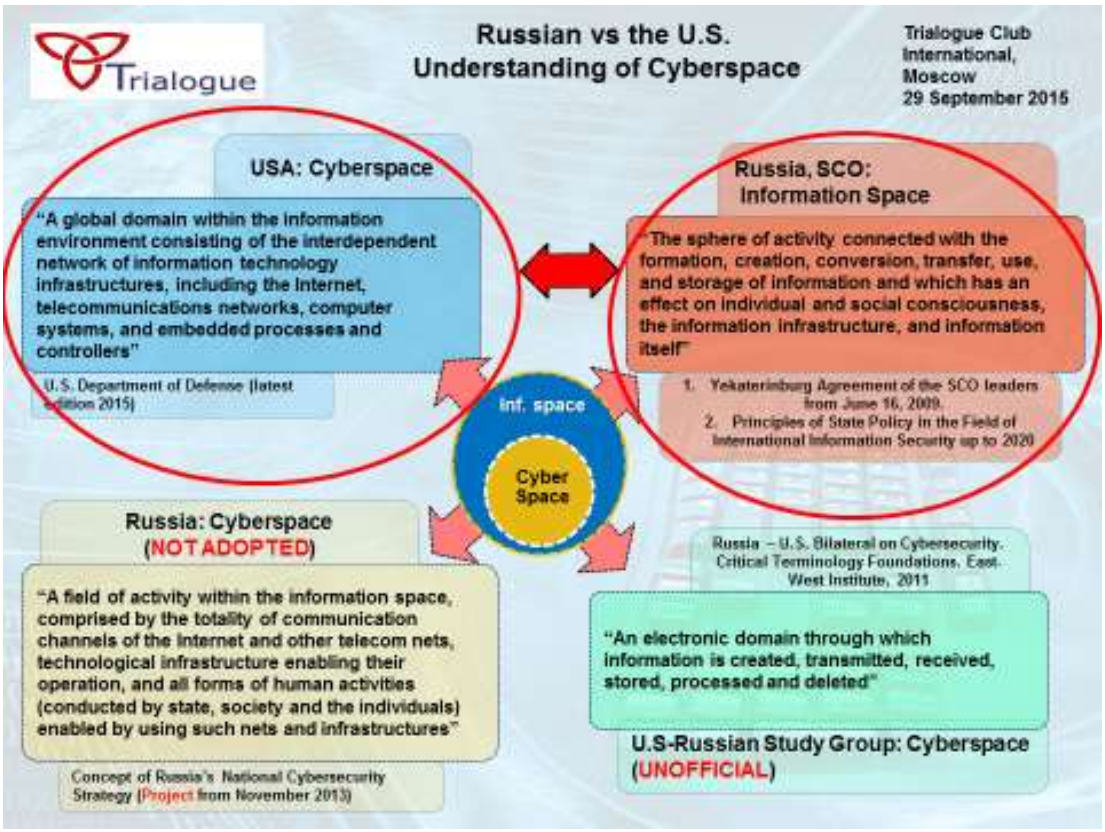
It is also worth noting that though such papers as *The Tallinn Manual* and *The Tallinn Manual 2.0* that is to be published in the second half of 2016 are the expert papers, they become the cornerstones of the practical approaches of certain organizations — NATO

among them. In particular, at the NATO summit in 2014 in Wales as part of discussion of the NATO Cyber Defence Concept allies decided to regard certain situations and incidents as an armed attack against the party to the Washington Treaty, which allows to use the Article 5 and exercise the right of collective cyber-defence.

Therefore, the development of theoretical knowledge and outlooks on the preconditions for enforcement of the international law to cyberspace crisis in some countries and regional associations gets ahead of the exploratory work of the UN Group of Governmental Experts. Some representatives of the Group and some members of the international community do not consider that a problem. Other states' position — like Russia's and China's — as well as position of some other member of the Group differs from the approach provided in *The Tallinn Manual* and the NATO's approach indoctrinated in its Cyber Defence Concept.

Position of Russia is quite well known. Russian diplomats state that cyber space is a unique space that requires additional international regulations and establishing of new mechanisms, new treaties, new conventions, better elaborated through the offices of the United Nations as one of the most respected and legitimate international organizations. Russia presented the draft of Convention on international cybersecurity in 2011, and twice — in 2011 and in 2015 — in co-operation with the Shanghai Cooperation Organisation sent a letter to the UN Secretary General. All those documents reflect the key provisions that are promoted by Russia. Russia and to some extent China attempted to put these provision at the UN Group of Governmental Experts.

What are these provisions? **First**, the right of the state to sovereign control over its own segment of cyberspace, which is the IT infrastructure within its jurisdiction. **Second**, mandatory prohibition of cyber conflicts including cyberwars and offensive cyber operations. **Third**, insufficiency of existing international law instruments and therefore necessity to outline new international binding legal agreements enshrining the rules of conduct of states in cyberspace. **Fourth**, the emphasis on control of content, transferred across the borders of the states through cyberspace and impact of this information on political and social processes. On the slide you can see the difference in technologies and terminology difference in approaches of the US and Russia. The key difference is the emphasis on content and its influence on the mindsets of people.



I will summarize the set of rules that experts managed to elaborate regarding their contradictions and the differences between the key participants of the Group — the US and Russia, which have always been the most active and the most different Group participants. Non-aggression to the critical infrastructure and mutual assistance in case of cyberattack of the critical infrastructure is the crucial issue that all experts agreed. That's a breakthrough and a significant step, but problem is the key definitions and the details of such an assistance are not clarified. The definitions of critical infrastructure are very different in China, Russia and the US. Forming an international classification of critical infrastructures is a highly important issue — that, in my expert opinion, is one of the future aims of Russia, China and the USA. Progress in this regard requires at least minimal lift of level of trust for the relationship of this potential *triangle*. For instance, now the Russian-American cyber dialogue is frozen despite previous significant achievements.

The last word to say on the outcome of the work of current UN Group of Governmental Experts: on one hand, Russia and its allies managed to get into the report the concept of national sovereignty applicable to national ICT-infrastructure within its jurisdiction; on the other hand, a bright idea brought by Russian delegation was not supported in the integrated report. They proposed a particular provision on states' cyber non-aggression in relation to the ICT-infrastructure of banks. A rumour ran prior to the Chinese leader Xi Jinping's visit to the US, that the same provision in the forthcoming agreement is discussed by the parties. But it didn't appear in the final communique. I pinpoint it by only one reason: that would have established a certain critical infrastructure object class, and that would have been a dramatic step forward in relation to international

legislation. States' responsibilities remain abstract as long as they talk on non-aggression upon critical infrastructure at large — the objects are not clear. Defining infrastructures as critical — e.g. banking, telecommunications, nuclear, any — establishes an obligation for the states and a common ground for the technical staff. The last one interesting provision in the report: the governments must control the IT-products supply chain in order to exclude *hardware Trojans, backdoors* and use for a purpose other than stated before.

From the UN Group of Governmental Experts report I would like to come to special bilateral relations between Russia–China, Russia–US and US–China. Now I would like to remind you what Russia and the USA have achieved in this respect at this time. The key achievement was the set of agreements signed by presidents Vladimir Putin and Barack Obama in 2013. Those agreements provided confidence-building measures and propelled the relationships in this field to the new level. One of the achievements is establishing a data exchange channel operated by high-level officials in case of potential grave crisis such as an attack of Russian critical infrastructure from the US territory or the other way around. In addition to this express channel for high-level officials another 24/7 channel based on National Nuclear Threat Reduction Center was established. The infrastructure of the cold war served the purpose of providing cyberspace security. In addition, there was a provision on exchange of information on cyberspace problems between national Computer Emergency Response Teams (CERTs). The document also created a bilateral working group for developing the agreements, its expansion and evolution as well as strengthening confidence-building measures. I have to say that Russian diplomacy in the name of Andrey Krutskikh, special representative of the Russian president for international cooperation in the field of information security, recognized the significant practical usefulness of these agreements to the Russian Federation. Mr. Krutskikh in his interview mentioned that the emergency information exchange channel was in high demand during the Sochi Olympics in February 2014 when the Olympics infrastructure was being under cyber-attacks. Unfortunately shortly after the Olympics the working group and then the whole set of measures was frozen due to the Crimean crisis and then the Ukrainian crisis. The US Department of Defence issued the latest Cyber Strategy in Spring 2015, and this strategy reflects this fact. It says dialogue on strategic stability in cyberspace is frozen with Russia and continues with China. The strategic aim in Russia–US bilateral relations for the moment is reestablishing the level of trust that existed in February 2014. Moreover, the logic and the essence of the set of measures that existed in Russia–US relations could serve as a model for other bilateral and multilateral agreements. Firstly, the summarized version of the Russia–US agreements excluded all disputable points, namely content issue, information impact on political processes and so on, concentrating on infrastructure issues. That is the field for the technical staff that easily finds common ground and sees the threats. The 24/7 work of the information exchange channel is crucial as it establishes constant co-operation of technical experts, and they establish atmosphere of credibility. The trust is being fortified while they work together. That drastically differs from the treaties that in black and white articulate some interaction mechanisms that in fact are used only from time to time.

Let's consider Russia-China agreement signed on the 8th of May 2015 as an illustration of my previous statement. The agreement has a long list of different measures for safety cooperation and governance in cyberspace — some 15 points. Some of them are presented on the slide.

In technical sense, Russia-China agreement is wider and more intricate than the Russia-US one of 2013. On the contrary it is just a framework deal that is not loaded and doesn't have any technical co-operation mechanisms. That is the fundamental difference with the Russia-US agreement. The other difference is that the Russia-China agreement is highly ideological. It delivers the parties mutual outlook on the international legislation in regard to the cyberspace, like internationalization of global internet governance, in other words, brining key internet infrastructure under control of intergovernmental organization. Therefore the Russia-China agreement is more of a declaration of the identity of views of two states on international cyber legislation. On the other hand, the document signed is a good background to develop a practical measures set. They might appear as specific documents signed as part of the wider agreement. That will be a lengthy gradual process, which cannot stay within one document as the Russia-US agreement.

We briefly reviewed Russia-China and Russia-US co-operation in cyberspace governance and cybersecurity. The third element of this *big triangle* is China-US co-operation. The agreement the parties came to recently is a breakthrough, and I suppose the those here present are aware of why it is. The US have always been thought to separate the cyber espionage and cyber operations motivated with national security, or

with economic reasons — that is stealing certain commercial secrets, intellectual property that could be later used in international trade in the work of corporations or governments. Of course the most painful issue in the US relations with China was the industrial espionage. Chinese hackers are behind some 80% of attacks on American networks according to the statistics. China is thought to be the main beneficiary of hacking activities against trade secrets of American companies, and the damage from these activities could be counted in billions of dollars every year. At the same time it is quite difficult to prove from technical and legal points of view those facts, and it was considered that it was impossible to pressure China in this respect. That's why the agreement concerning the industrial espionage was not an expected outcome of Obama and Xi meeting. The agreement concerning non-aggression to the critical infrastructure, cyber assaults was more anticipated. So much the more surprising was the mutual understanding of Barack Obama and Xi Jinping on this issue. The ground for this understanding can lie in the threat of imposing sanctions against Chinese companies and citizens for economic espionage. Information on such sanctions appeared in August 2015. The legal mechanism of these sanctions could be based on presidential directive against American citizens that could be changed and used against Chinese citizens and companies. The mechanism considers four reasons for sanctions imposing:

1) Attacking American critical infrastructures.
2) Attacking key American computer networks.
3) Stealing trade secrets and intellectual property of American companies and government.
4) Direct benefit from stealing trade secrets in a cyber-operation.

The last point is the most interesting and the most powerful from the practical point of view.

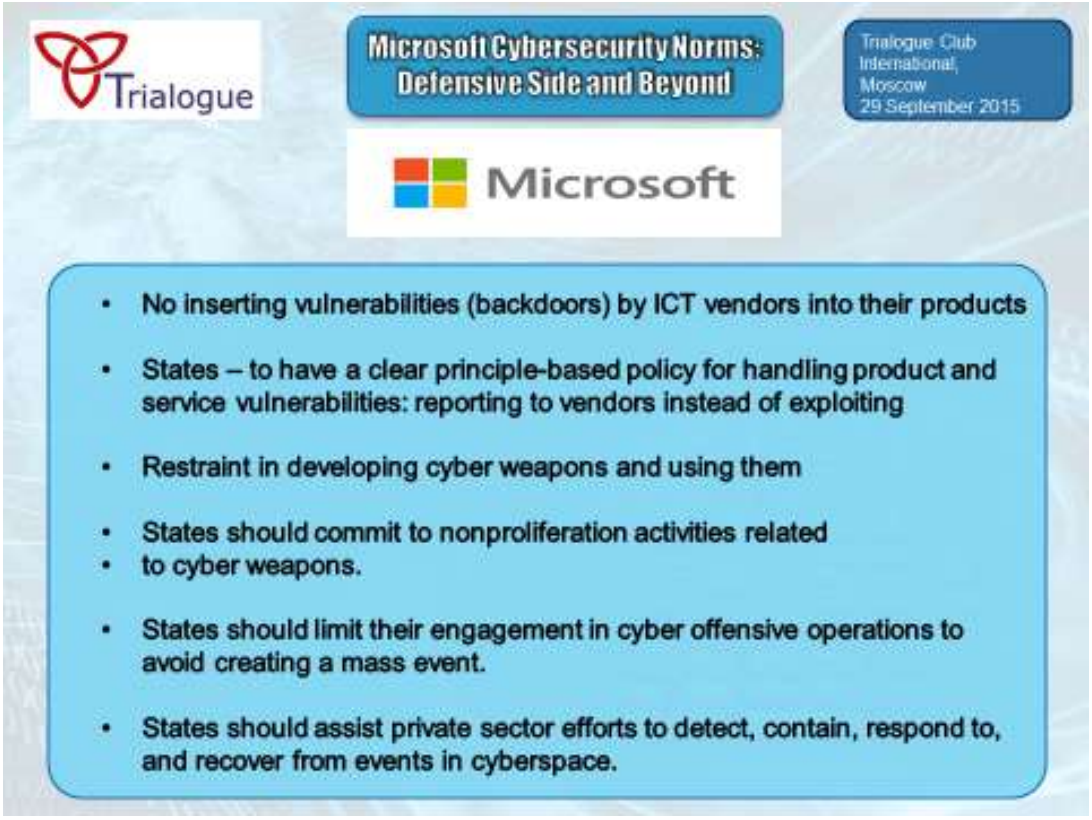
It looks like the real prospect of introducing such mechanism against Chinese companies, suspected by American intelligence agencies in economic cyber-espionage, threatened China enough to abide by an agreement that prohibits large-scale industrial cyber-espionage. The agreement fuels lots of debate on the real value of the deal, which virtually is no more than declaration of intentions and is not supported by any monitoring mechanisms or other verification measures. I take the liberty of assuming that even as a declaration of intentions this agreement is an important breakthrough for the White House and a step forward, and it is assured by economic deterrence instead of monitoring mechanisms. China will deter from economic espionage due to the perspective of imposing sanctions.

I'd like to fix your attention on this once again. Pundits and governmental experts longtime thought that military deterrence worked in cyberspace, saying the states would deter from the largescale cyber-operations against each other as soon as their own military facilities in this case became vulnerable. This deterrence though does not work as well as it thought to do. The economic deterrence is much more efficient. An example: In 2012, only the Pentagon networks were reported to withstand 8-10 million tests for security gaps. Those were not attacks but simply test for the perimeter

vulnerabilities. The figures grow every year. Someone tests vulnerabilities of American networks and Americans test strategic networks of other states in the same way. The intelligence services confrontation is very dynamic but it is concealed from the strangers, and the critical infrastructure never is destroyed. It is easier to follow the economic-reasoned attacks due to their aftermath. During Barack Obama and Xi Jinping's meeting international cybersecurity companies noticed the sharp decrease in number of such attacks. In other words, even with no technical support the China-US agreement affects the situation.

Those are the bilateral relations between the parties to the *big triangle*, but there are no tripartite relations as such. Why should we distinguish this *triangle*? Because China, Russia and the US together as the participants of the international dialogue in the field of cybersecurity have such force and wield such influence that any agreement among them could become a real precedent and a signal to the international community. They are the minimum critical group that could change the international regime of the conduct, and it could influence the situation in cyber security. Unfortunately or fortunately, neither India, nor Japan or the EU are needed that much. Speaking on the EU it is not so regarding issues of privacy and personal data but regarding military security, these three players are enough.

This way, there is a chance to conclude an agreement inside this small group when there is no chance to reach an agreement in a wider group — e. g. The UN Group of Governmental Experts. Private sector could be very effective mediator that covers up the contradictions and differences between states. The private sector activity in international disputes on states' conduct in cyberspace grew drastically in 2015. For instance, a list of norms presented by Microsoft last spring is presented on the slide and I would say they are good enough to be concerned.



The private sector indeed is entitled to participate in these disputes. In September 2015, at the Global Cyberspace Cooperation Summit in New York one of the Microsoft top-level managers mentioned that it is the private sector to suffer the most from the cyber-operations conducted by the states using highly developed, complex malware. Thus, the Microsoft had to reinstall software on almost all working stations in the world to deal with the zero-day vulnerability used by the computer worm *Stuxnet.* That cyber-operations worth *Microsoft* and other IT-companies millions of dollars, which makes them rightful party to the discussion.

As a result, in my opinion, we get a rather modest composition of international dialogue. Three countries compose a *large triangle,* in which they cooperate bilaterally, and a separate party to this dialogue — the private sector — that could broker the deal.

Finally, I would like to present my expert vision of a potential negotiations between the US, Russia and China with the participation of the private sector. **First**, it would be highly valuable for the participants to elaborate a classification of critical infrastructure objects and to adjust differences in that field. **Second,** a tripartite initiative on cyberattacks attribution would be reasonable in case the attack passes through several states or through a number of command-and-control servers and the origin of the operation is vague. A tripartite co-operation of Russia, the United States and China is very important from this point of view. These three states possess strong technical competence, a high-level technical expertise for investigation and cyberattacks attribution. On the other hand, these three countries appear to be the source of many cyber-incidents. Many cyberattacks are allegedly conducted with the use of

infrastructure or with the participation of persons based within the territories of these countries. Moreover, cyber-attribution co-operation involves CERTs co-operation. That co-operation existed between Russia and the US, China and the US, and China and Russia are setting it now, but a tripartite co-operation would be much more helpful. **Finally,** a long-term and an ambitious aim for the three countries would be voluntary negotiations on self-limitation of offensive cyber operations. That would help these three countries exceed the bounds of previous agreements, which is very important assuming the fact that Russia, the US and China are the major cyber-powers, and the military potential of these powers is aimed at each other. Just to be clear, I have to say that though Russian and China are thought to be the ideal partners and to refrain from attacking each other in cyberspace, that is not quite the case. At least, the *Kaspersky Lab* experts repeatedly report on dealing with Chinese malware and numerous network attacks of Chinese origin. To conclude, every participant of this *triangle* has plenty to negotiate with others regarding self-restraint in cyberspace.

I would like to stop my presentation now and answer your questions.

Tomáš Zipfel: I am from the Embassy of Czech Republic. You mentioned three major nations in cybersecurity. Are there other nations effective in terms of making effort towards the agreement or some other regulations in cybersecurity?

O. V. Demidov: Most of European nations are quite active now in the field of international dialogue on cyberspace and on cybersecurity. The UK has been very active in setting very high standards for technical cooperation between cyber emergency response teams. In addition, it has its own national cyber security strategy, which has been permanently updated and provides the set of provisions for international co-operation on exchange of data to fight cybercrime, to exchange information on cyber incidents among technical specialists from cyber emergency response teams and so on. Russian diplomats including Mr. Krutskikh whom I mentioned previously have been reporting that they have been conducting negotiations with a number of European nations on the issue of bilateral agreements on cyber cooperation more or less similar those one we have with the US. If I am not mistaken France was mentioned among potential partners of Russia in this field. Among European nations, the cooperation has been taking place within the framework of the Council of Europe where they have the Budapest Convention on cybercrime. Starting from 2012, the work has been going on within the framework of the OSCE on the set of confidence building measures for cyberspace.

As for other regions and other non-European nations, in recent years India has become a very significant player in the field of global cyber policies. In 2013, there was some memorandum of understanding with regard to international cyber security policies between Russia and India. While India is also promoting its own view and its own approach to the issue of norms and rules of behavior in cyberspace in the UN. Starting from 2013, from Snowden revelations on global electronic espionage, Brazil has become an active participant of the global dialogue on protecting privacy on the internet and setting standards for encryption of data, for cybersecurity and countering global

electronic surveillance. Brazil supported th UN GA resolution on protection of privacy in the digital age in the end of 2013. In addition, Brazil hosted several major conferences on the issues of just and transparent internet governance and privacy protection. Brazil adopted a major piece of national legislation on internet governance and protection of privacy protection and cyber security in some aspects such as encryption of data and fighting cybercrime which is known as *Marco Civil da Internet*.

In fact many dozens of nations have become proactive participant of international dialogue on cyberspace but it is not always enough to be active. You need to have considerable military potential in cyberspace, you need to have considerable economic and technological potential. The highest concentration of all three kinds of such potential we have when we deal with Russia, China and the US.

Nurlan Alkenov: I represent the Kazakh embassy. I would like to thank Oleg for a very useful report. Last week I participated in the research and application conference dedicated to shielding youth from extremist and terroristic ideology. One of the reports presented said, that nearly 1,900 young people left Russia for Syria over the last years, and they fight for the ISIS, and they did that affected by numerous disruptive websites. I have to mention that the Kazakh population is ten times less than Russian, and some 400 Kazakhs are now in the ISIS, so for it is the urgent problem. The report at the conference said also, these websites use super-high technologies to influence people's minds. I would like to know what we could do to counter with this phenomenon.

O. V. Demidov: First, there are no efficient international mechanism to ban websites that promote extremist ideology. There are some limited measures regarding the content of the websites. If I am not mistaken, in mid-2000s, an additional protocol to the Budapest convention, regarding websites distributing extremist and xenophobic data, was adopted. Meanwhile it was easier to agree on the definitions of extremism and xenophobia than on banning extremist and xenophobic content. That became an issue of interpreting national legislation. The threat you've mentioned, the threat of the ISIS, might stimulate the European Council to develop the Convention mechanisms this way. I am not sure for what it's worth.

Other regional co-operation formats exist, that have less contradictions on terrorism and extremism definitions. The CSTO is one of them. In the framework of the CSTO, law-enforcement agencies annually conduct combined operations to unravel and ban websites distributing illegal content, e.g. extremist. "Weed" and "PROXIE" combined operations are the example of such reciprocity. However, the regional co-operation is not sufficient to fight the problem. Those who produce extremist information and the very websites that distribute this information commonly are not situated at the territory of the CSTO member states.

Two ways exist here; one is not exclusive of the other. Diplomatic efforts could be invested in adoption of international agreements countering extremist and terroristic information in the broadest framework, if anything, at the UN. In the meantime, effective information war forces are to be established the sooner the better. These forces

should carry on counterpropaganda through the same channels that the ISIS recruiters use.

You've mentioned, the extremist and terrorist recruiters use super-high technologies to reach their goals. That is not quite true. What they use is software for instant communication: social networks, messengers, video streaming — the channels that are the most popular among youth and that allow in several seconds spread any multimedia content. The Islamic State learnt the rules of the new media genre, it creates appealing shocking content targeted at its core audience — the things that distinguish social networks from the Web 1.0. Law-enforcement agencies alone would face serious difficulties fighting with extremists in the internet as soon as the counterpropaganda has to involve core audience studies, creative work of young people and some inventiveness. I consider the funny videos shot in the US, parodying the ISIS, to be a good example in his case. The videos make the ISIS' thought-to-be appealing ideas ridiculous, and laughing at something means destroying it.

I will repeat myself; this should go hand-in-hand with national policy, diplomatic efforts to create co-operation mechanisms, international legislation and criminalization with following criminal indictment of the people involved.

A. F. Zulharneev: The Western countries are known to repel Chinese government offer to limit the content distribution. Does the new situation change the position of American and European officials and pundits concerning the content issue?

O. V. Demidov: The question is very interesting and tricky. I see this as rethinking the requirements with emerging understanding of necessity of officially enshrined in the legislature joint efforts to fight with clearly illegal and extremist content. The realization of insufficiency of narrow regional measures and agreement appears, they see they have to work with the countries that pursue other approaches. However, there is incomprehension of developing of this issue without betraying the principles — e.g. the freedom of access and distributing of the information, the freedom of expression on the internet. It is not clear yet, how the extremist and terroristic content can be criminalized without betraying these principles. This brings us back to the definitions issue. To find the definition of extremist and terroristic content that would suffice Russian, American and the EU law-enforcement agencies and wouldn't be considered the infringement upon freedom of speech, is horribly difficult. The tremendously increased efforts of extremist and terroristic ideologists, in my point of view, will stimulate Russia, the EU and the US to overcome the divisions and embark on long, scrupulous and nettlesome work on developing those definitions.

Jeffrey Valdez: I am from the Economic Sector of Embassy of the Republic of the Philippines. During the presentation, I have wanted to ask a question on qualifications of these three countries. The representative of Czech Republic asked the same question on the *great triangle*. You have said it is primarily about their technical capabilities, responding to and possible carrying out attacks, especially in the military sector. I recall many content providers are based in the US and overwhelming number of websites.

China has the largest number of internet users. As for Russia, it is about its technical capacity, especially in the military. My question is: is there any danger in that *great triangle* in cyberspace about intellectual property and content?

O. V. Demidov: I thank you for your question. Speaking on the concept of the *great triangle*, I take the premise that this triangle is based on technical and military potential of its players. If we tried to build another configuration of states, based on their contribution to intellectual property assets production or their contribution to the world internet economics, there would be another composition of participants. The EU would appear in the list ousting Russia; India would join to the list formed on the contribution to the software developing, etc. Japan would appear in the list in some case. Nevertheless, the proposed list of participants of the *great triangle* is not random as long as the discussed question of voluntary norms of conduct in cyberspace bumps into the international legislation, particularly into the UN Charter. Such notions as *use of force*, *act of aggression* upon the UN member state and *armed assault* play a high priority role there. That brings us to technical and military potential, the necessity to estimate, interpret it and put restrictions on it in the cyberspace.