Confidential

RUSSIA

The circulation of this report has been strictly limited to the members of the *Trialogue* Club International and of the Centre russe d'études politiques.

This issue is for your personal use only.

Published monthly in Russian and in English by *Trialogue Company Ltd.*

Issue № 3 (253), vol.17. 2018

July 12, 2018

PIR Center experts report from Moscow:

CYBERSPACE: CONSIDERING THE PROSPECTS FOR COOPERATION AFTER THE US-RUSSIAN SUMMIT IN HELSINKI

SUMMARY

On July 16, 2018, the presidents of Russia and the United States will meet in Helsinki for the first US-Russian summit since Donald Trump assumed the presidency. The cyber domain is likely to be included in the agenda of the upcoming meeting.

Direct Russia-US cyber dialogue is currently suspended since the bilateral working group on cyber issues no longer exists. PIR Center Executive Board Member and Deputy Head of Kommersant Newspaper Foreign Policy Department Dr. Elena Chernenko and PIR Center Consultant Oleg Demidov give a brief overview of US-Russia cyber relations and examine the prospects for post-summit dialogue in this field.

Elena Chernenko on the dynamics of Russian-US cyber dialogue and the necessity for cooperation on cyber issues

One of the issues that might come up during the Russia-US summit in Helsinki is cyber security. Ahead of the summit the press-secretary of the Russian president Dmitry Peskov indicated that Moscow would like to bring up this issue again. Previously this topic had been discussed during the first meeting of Vladimir Putin and Donald Trump on the sidelines of the G20 Hamburg summit held in July 2017. Although those talks yielded no practical results (the two presidents announced a plan to create a mechanism for regular consultations but two days later Washington abandoned this idea) both sides understand that **the status quo in the US-Russia relations in cyber domain is deeply unsatisfying.**

Historically, the **preconditions for Russia-US cyber dialogue were not that bad:** in June 2013, the two countries signed the first ever bilateral package of intergovernmental agreements designed to build trust and to prevent cyber incidents from escalating. The deal provided for three channels of communication (between the Kremlin and the White House, between the national CERTs - Computer Emergency Response Team – and most important – between the Nuclear Risk Reduction Centers, which started to cover cyber aspects as well) and for a working group on cyber cooperation within the Bilateral Presidential Commission. The main goal of the group was to conceive how to deepen the interaction between Moscow and Washington on cyber issues – from crisis management and confidence building to true cooperation.

But then **the relations started to deteriorate quickly:** Edward Snowden landed in Moscow, Barack Obama cancelled a bilateral summit with Vladimir Putin, soon afterwards the crisis around Ukraine and Crimea erupted, the US imposed sanctions on Russia, and as if the things had not been horrible already – any hope for a restart under the new US administration was buried under the accusations of alleged Russian meddling in the 2016 presidential elections.

The working group on cyber issues ceased to exist as did the whole presidential commission in 2014. There were informal meetings between the government officials who deal with cyber issues, but they had no mandate and could not lead to concrete results. In February 2018, even such informal consultations were cancelled by the US side at the last minute.

The three channels of communication, established in 2013 and mentioned above, still exist but there is little information about their efficiency.

In March 2017, **Russia proposed a plan** in the format of a non-paper for a renewal of the dialogue and, as one of the provisions, suggested conducting consultations on a new agreement on cyber. This proposal was discussed during the first meeting of the presidents in July 2017. Initially both sides announced the start of a new mechanism with the aim of overcoming the existing problems, but then the US administration pulled back – the pressure from the Washington establishment was too high.

Why is it **so crucial that the two countries cooperate in cyberspace**? There are two reasons that are directly linked to strategic stability.

First, attribution of cyberattacks is sometimes extremely difficult. A third party, be it a country or a non-state actor, can put Russia and the United States on the verge of an armed conflict by attacking critical infrastructure of either of them and making it look as if the aggressor was the opposite side – in cyberspace this is possible. Both the Russian and the US cyber doctrines allow them to react to major cyberattacks with all military means. Therefore, effective direct communication and de-escalation channels, as well as trust building measures in cyberspace between the two countries are a priority.

Second, without a constructive dialogue on cyber issues between the US and Russia **the world will most likely be unable to agree on any norms of responsible behavior of states in cyber space.** Such basic norms are of crucial importance for global stability – that is why more and more nation states, IT giants and civil organizations are calling for them. Recently this idea was for the first time publicly endorsed by the UN Secretary General Antonio Guterres who said that global rules are needed to minimize the impact of electronic warfare on civilians as, in his opinion, "the next war will begin with a massive cyberattack to destroy military capacity... and paralyze basic infrastructure such as the electric networks."

Bearing these reasons in mind, one can outline **two recommendations for Russia and the United States.**

First, the US and Russia should **give the bilateral working group on cyber a chance** – as it was announced after the July 2017 meeting of the two presidents. Critics might say that, given the accusations that Russia used ICTs to meddle in the US presidential elections, no new agreements are possible between Moscow and Washington. However, US-Russia cyber negotiations still make sense for at least two reasons:

- **Russia is also accusing the United States of improper behavior in cyberspace** – in particular, of using ICTs to achieve its geopolitical goals (the Snowden-files give plenty of arguments to build the case).

- **Russian and US political tensions could not serve as a pretext for not developing cyber policies.** In 2015, Xi Jinping and Barack Obama signed a cyber accord in difficult political circumstances: after the United States was close to imposing broad sanctions against China because Chinese hackers (allegedly supported by the Chinese government) were stealing industrial secrets and causing the US economy billions of dollars of damage.

There is no need for the new US-Russian working group on cyber to have a strict mandate for negotiations, but officials must start discussing difficult issues to see if any trust can be restored.

Second, the US and Russia should **take the lead in restarting the consultations of the UN Group of Governmental Experts** on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), which have been paralyzed since June 2017. Since 2004, the UN GGE has attempted to develop a common approach to the way governments behave in cyberspace, and it had a notable achievement. Its 2013 and especially the 2015 reports laid the ground for a first step toward an internationally recognized governmental code of conduct in cyber. In this consensus document, existing and emerging threats were spelled out; basic norms, rules, and principles for responsible behavior of

states were proposed; and confidence-building measures, international cooperation, and capacity-building were given the well-deserved attention.

The UN GGE decided that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs, that states should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure, and that states should take steps to ensure supply chain security as well as should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions. In total, there were 11 very basic yet crucial and depoliticized recommendations in this paper.

However, in 2017, the group did not reach a consensus on what should be the follow up on the 2015 report and failed to produce a new paper. This should not mean it is a dead end. **The mechanism should get all the international support and encouragement possible to regroup and restart its activities.** Absent the consensus on further steps, it could be efficient to give the consensus report a stronger official status within the UN instead of trying to expand the norms of the 2015 report. No doubt, such an initiative would get broad support.

Oleg Demidov on the prospects for Russian-US post-Helsinki cyber dialogue

American foreign policy line can hardly be forecasted now: the political setup presupposes that the **president is limited in his decision-making powers.** Besides, the consensus on the alleged Russian meddling in the 2016 US presidential elections has been already reached. Having got familiar with the secret part of the US intelligence report on cyber interference, Donald Trump acknowledged in public that the Russian interference did take place. *Highly unlikely* that the US President would be able to turn the blind eye on the allegations and suggest lifting the sanctions, signing an agreement on cooperation in cyberspace, and relaunching the mechanisms on information exchange.

In this sense, it is improbable that the summit would drastically impact Russian-US dialogue in cyber sphere. The summit can result in some declarations on paper: for instance, a declaration confirming intentions to develop cooperation mechanisms in cyberspace – before all, mechanisms of trust and conflict prevention as part of the OSCE track. However, the direct cooperation in the format that was conceived in 2013 is unlikely to be resumed.

The best outcome of the summit could be achieving of **a kind of agreement on the mutual approach**, on the similar position **on relaunching the format of the UN Group of Governmental Experts** on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), which failed to release a substantive report in 2017 and consequently ceased to exist. This format should be relaunched and modernized – it should be more rapid and effective. The working period of the group (13 years) was marked by the adoption of non-binding norms that did not produce a significant influence on the US-Russia cooperation in this area. Thus, if during the summit Russia and the US find common approaches to relaunching of at least such a non-binding international dialogue on the norms in cyberspace, in the current situation it will already be considered a success. The prospects of this success are quite slim because, first, Trump is skeptical about the UN, and, second, the general

context of the Russian interference in the US elections is overloading the entire cybersecurity agenda.

As for cybercrime, the ground for a serious progress is also absent: Russia and the US have different approaches to this domain. Besides, this issue was not included separately in Trump's election campaign program nor in his post-election plans and orders regarding cybersecurity. In relation to cybercrime, the US continues to successfully participate in the mechanism established by the Budapest Convention of the Council of Europe. The country is also augmenting its potential for ensuring the security of critical infrastructures and resisting serious mass cyberattacks. Conversely, Russia is planning to promote its project of a UN convention on countering the cybercrime, which was developed two years ago – it is unlikely that Russia and the US will achieve mutual understanding in this regard.

In terms of his approach to Internet governance, **multi-stakeholder community** and the balance of actors' involvement in the Internet technical infrastructure management are **of little value for President Trump**. Conversely, Russia supports the IANA transition that was launched under the Obama administration, so Donald Trump is not a beneficial partner for Russia, and a global breakthrough in this domain is not likely to be achieved.

Currently, the development of the Internet and cyberspace governance policies are at the stage when major economic and integration groups are rushing toward different models of regulation. The EU proposes aggressive regulations in copyright sphere with a strong protection of personal data (GDPR). The US rejected the concept of net neutrality and, in many respects, denies its role of the proponent of free access to information and the Internet all over the world. Russia and China are pursuing their own paths.

Now **it is not the best moment to reach arrangements on the international level and develop common approaches to the regulation and protection of cyberspace**. In the coming two or three years, international cooperation is not likely to become a modus operandi in this sense. Private companies' initiatives offer much more hope. The latest critical move in this domain – a transition towards encryption by-default in the Internet as well as the introduction of HTTPS (HyperText Transfer Protocol Secure) and Internet traffic encryption – was proposed by global technical community in reaction to Snowden's disclosures of the American surveillance programs and the challenges that are increasingly posed by states.

This article is written by Elena Chernenko, PIR Center Executive Board Member, Working Group on Strategic Stability and De-Escalation in US-Russian Relations Member, and Oleg Demidov, PIR Center Consultant

Editor: Yuliya Seslavinskaya

Dear members of Trialogue Club International,

The 2018 Club season has started, and we kindly **invite you to extend your membership in the Club for 2018 or for the 2018-2019 period.**

In 2018 Club members will continue to receive exclusive analytics on Russian foreign policy priorities and key challenges and threats to international security. We have scheduled **six meetings of *Trialogue* Club International** in 2018. Club Members will receive a series of articles in electronic form, **eight issues** of the Russia Confidential analytical bulletin, as well as other information and analytical bulletins.

As always, specialists of *Trialogue* Club International and its partner organization PIR Center are open for exchange of opinions on key international issues.

In **2018**, membership fees are the same as in previous year:

Period	Individual	Corporate
01.01.17 – 31.12.17 (1 year)	50 000 roubles	80 000 roubles
01.01.17 – 31.12.18 (2 years)	90 000 roubles	140 000 roubles

We operate a **1+1 arrangement** for **corporate members**, whereby each corporate member is entitled to have **2 representatives** participating in Club events.

For all membership issues, please email us at secretary@trialogue-club.ru or call +7 (985) 764-98-96.

Sincerely,

Evgeniy Buzhinskiy

Chairman of the *Trialogue* Club International