Dr. Elena Chernenko

CYBER SPACE: A NEW BATTLEFIELD BETWEEN THE US AND RUSSIA OR A NEW AREA OF COOPERATION?

On July 16, 2018, one of the issues that might come up during the Russia-US summit in Helsinki is cyber security. This topic was discussed during the first meeting of Vladimir Putin and Donald Trump in Hamburg in July 2017. Although those negotiations yielded no practical result – 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 when it comes to cyber, the status quo in the Russia-US relations is deeply unsatisfying. Ahead of the summit the press-secretary of the Russian president Dmitry Peskov indicated that Moscow would bring up this issue again.

Devolution of dialogue

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

However, the relations began to deteriorate quickly: Edward Snowden landed in Moscow; Barack Obama cancelled a bilateral summit with Vladimir Putin; the crisis around Ukraine and Crimea erupted soon afterwards; the US imposed sanctions on Russia, and if things were not 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 ceased to exist as did the whole presidential commission. There were informal meetings between the government officials who dealt with cyber issues, but they did not have a mandate and did 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 do exist, but there is little information about their efficiency.

In March 2017, Russia proposed a plan for a renewal of the dialogue in the format of a non-paper whose provisions included consultations on a new agreement on cyber. As mentioned above, 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 strong.

Doomed to cooperate

Why is it crucial that the two countries cooperate in cyber space? Out of many reasons, I would highlight two that are directly linked to strategic stability:

1. Attribution of cyberattacks is sometimes extremely difficult, and **a third party, be it a country or a non-state actor, can put two super powers 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 other one. In cyber space this is possible. Both the Russian and the US cyber doctrines allow them to react to major cyberattacks with all military means. Therefore, an effective direct communication and de-escalation channels, as well as trust building measures in cyberspace between the two countries are a priority.

2. Without a constructive dialogue on cyber issues between the US and Russia, **the world will most likely fail 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 an increasing number of 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 were 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.

Action plan

Bearing in mind those two reasons, I would propose two things Russia and the US should do.

1. **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, there are at least two reasons why Russia-US cyber negotiations still make sense. First, Russia is also accusing the United States of using ICTs to achieve its geopolitical goals, and the Snowden-files give plenty of arguments to build this case. Second, Xi Jinping and Barack Obama managed to sign a cyber cooperation agreement even after the United States was close to imposing broad sanctions on China as the Chinese hackers, allegedly supported by the Chinese government, had been stealing industrial secrets and caused the US economy billions of dollars in damage. The new US-Russian working group on cyber does not have to operate based on a strict mandate, but officials must start discussing difficult issues in order to see whether any trust can be restored.

2. **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 (UNGGE), which have been paralyzed since June 2017. Since 2004, the UNGGE has attempted to develop a common approach to the way governments behave in cyberspace, and it has achieved a notable result. Its 2013 and especially the 2015 report laid the ground for the first step toward an internationally recognized cyber code of conduct for governments.

In this consensus-based document, existing and emerging threats were spelled out; basic norms, rules, and principles for the responsible behavior of states were proposed; confidence-building measures, international cooperation, as well as capacity-building were given the attention they deserve. The UNGGE 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 the supply chain security, as well as seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions. There were 11 essential, 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 the group is at a dead end.

This mechanism should get all the international support and encouragement possible to regroup and restartits 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 a broad support.

This memo is prepared as part of the activities of the Working Group on Strategic Stability and De-escalation in U.S.-Russian Relations.