RUSSIA

The circulation of this report is strictly limited to 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 № 5 (255), vol.17. 2018

November 14, 2018

Oleg Demidov and Margarita Angmar report from Moscow:

AMERICA'S NEW CYBER STRATEGY: OUTLOOK FOR RUSSIAN-US RELATIONS IN CYBERSPACE

ANNOTATION

In September 2018, after several months of pressure from Congress, the White House released a new US strategy for cyberspace. The media have described the document as the new administration's shift towards a more aggressive and offensive cybersecurity policy.

Several clauses in the new Cyber Strategy genuinely appear to suggest that Washington intends to step up preventive offensive operations against its adversaries in cyberspace. Oleg Demidov, a PIR Center consultant, and Margarita Angmar offer a more in-depth analysis of the document and reflect on how these plans could affect Russian-US relations on cybersecurity issues.

Highlights of the new strategy: did Trump have a hand in this?

The National Cyber Strategy proposes that the federal government, in cooperation with the private sector and other stakeholders, step up efforts in four key areas (pillars):

1. Defend the American people, homeland and the American way of life (bolstering security of information networks operated by the federal government, strengthening cybersecurity of critical infrastructure, fighting cyber crime, promptly responding to cyber incidents, etc.)

2. Promote American prosperity (by nurturing a secure digital economy and fostering strong domestic innovation in IT, etc.)

3. Preserve peace through strength (strengthening stability in cyberspace, attribution and deterrence of "unacceptable behavior" in cyberspace)

4. Expand American influence in cyberspace (support for an open, reliable and secure Internet, international strengthening of capability and resources in cybersecurity)

In his public statements, President Trump completely ignores the cyber strategies approved under Barack Obama. Nevertheless, looking at most areas of the new strategy, the signs of the new administration's and Donald Trump's influence are few and far between. The new strategy does not formulate a coherent new vector for all the government actors involved – rather, it describes the already existing policies (including those drawn under Obama) and the working agenda already pursued by individual federal agencies.

For example, almost the entire first pillar of the new White House Cyber Strategy, and to a large extent the second, constitute a mere rehash of the policies outlined in the Cybersecurity Strategy released by the Department of Homeland Security on May 15, 2018. That paper is depoliticized and based primarily on implementing and expanding several long-term initiatives, many of which were launched under Obama.

Also, the section of the new strategy on promoting and supporting a free Internet repeats, word for word, the clauses and the general direction of the strategic documents and statements made by the US leadership under Obama. Surprisingly, the strategy still contains a clause declaring a US commitment to the Internet governance based on the multi-stakeholder model – even though during the presidential election campaign, the Trump HQ insisted that he would not "allow Obama to cede control of the Internet to foreign states" (referring to the proposed transfer of the coordinating role in the Internet Assigned Numbers Authority – IANA – from the US government to a global community of stakeholders).

Stability in cyberspace and cyber defense: a hawk's flight

All of the above does not mean, however, that the new strategy does not contain any changes in the new administration's policy on cyberspace. The media and the expert community are focusing in particular on the third pillar, which is the new

US strategy to strengthen stability in cyberspace and protect America from external cyber threats.

In fact, much of the media attention has focused not on the strategy itself but on a remark by the US national security advisor John Bolton. Announcing the strategy on September 20, he had this to say: "We're not just on defense. We are going to do a lot of things offensively. Our adversaries need to know that."

One of the key steps by the Trump administration – a step that **"unties America's hands on preventive action in cyberspace"**, according to John Bolton – has been the cancellation of the Presidential Policy Directive 20, PPD 20, which was adopted in October 2012 as a top-secret document and leaked in June 2013 by Edward Snowden. The directive sets out the control mechanism for decision-making on offensive cyber operations (any such operations must be specially authorized by the US president) and for responding to malicious action in cyberspace (any such response requires inter-agency coordination).

Now, according to Bolton, all the requirements for inter-agency coordination before conducting cyber operations are lifted to reflect the new situation. The potential audience of that message was clearly outlined in the strategy itself, in Bolton's own statements, and in White House press releases: that audience consists of Russia, North Korea, Iran, and China.[1]

But apart from the statements by Trump and Bolton, is there any reason to believe that the new strategy is more hawkish and offensive than the previous version? It is true that the latest US strategic documents demonstrate a shift towards more offensive and preemptive action in cyberspace – but the White House strategy is not the most hawkish among them.

Shortly before the Trump cyber strategy was unveiled, the Department of Defense released a summary of its own Cyber Strategy on September 18, 2018. The priorities of that paper are clear:

- The DoD strategy states that the United States **"is engaged in a long-term strategic competition" with China and Russia**, and that actions by these two states in cyberspace represent a long-term strategic risk for the US nation and its allies.
- The DoD intends to conduct cyber operations in order to gather intelligence and bolster its military capability to prepare for the possibility of a full-blown crisis.
- The DoD intends to conduct operations as part of **proactive cyber defense** in order to preempt, defeat or deter hostile activity in cyberspace, even if such activity falls below the threshold for the use of force as specified in international law.
- The paper also says that "in wartime situation", the joint US forces **will employ "offensive cyber capabilities" and "innovative solutions"** to wage cyber operations in all theaters of military conflict.
- According to the new DoD Cyber Strategy, the main DoD goal in cyberspace is to ensure proactive defense, operate in the conditions of day-to-day competition with strategic rivals, and be prepared for war. That includes

[1] *Quote from the Strategy: "Russia, Iran, and North Korea conducted reckless cyber attacks that harmed American and international businesses and our allies and partners without paying costs likely to deter future cyber aggression. China engaged in cyber-enabled economic espionage and trillions of dollars of intellectual property theft."*

preparations by building more "deadly" armed forces capability in cyberspace.

Additionally, the DoD Cyber Strategy (and, to an even greater extent, the White House strategy) address the **challenge of hostile information operations**, such as online propaganda campaigns and efforts at spreading false information and manipulating US public opinion through cyberspace – especially by Russia. The two strategies propose to counter that threat through a combination of force, sanctions, and other instruments of pressure on the source of "hostile information activity".

This strategic vision by the DoD fleshes out the White House cyber strategy's provisions on stepping up measures against America's rivals in cyberspace, ensuring inevitable consequences for their actions, and effective deterrence of "unacceptable behavior" in cyberspace.

Commitment to rules and alliances

One of the radially new initiatives outlined in the Cyber Strategy is the international **Cyber Deterrence Initiative**. Its goal is to build a coalition with all states that share America's values and approaches to cybersecurity in order to ensure a decisive and effective response to hostile action and "unacceptable behavior" in cyberspace by third countries.

Judging from the proposed format of the coalition, Washington wants to build a bloc that will mount a coordinated response to cybersecurity threats and undertake collective action against hostile cyber actors. The only difference of this approach from the NATO cyber defense policy is its greater emphasis on political and diplomatic mechanisms rather than pooled military capability and joint military response. This does not mean, however, that the proposed coalition will be a paper dragon that poses no real threat to the potential offenders. Apart from cooperation in sharing intelligence data, the coalition can also pursue collective sanctions mechanisms. In theory, it can even legitimize military response if other members of the coalition can confirm cyberattack attribution conclusions reached by one of its members.

Outlook for Russian-US relations on cyberspace: nothing good in store

First, as Washington seems determined to promote voluntary rules of responsible conduct in cyberspace, we have to consider the future of the UN Group of Government Experts (UN GGE) on IT in the context of international security. This group, established more than a decade ago at Russian initiative, has been the main platform for multilateral efforts at developing and coordinating proposals for such rules. The UN GGE's 5th session ended in a painful fiasco in June 2017; for the first time since 2005, its members failed to reach a consensus and adopted only a progress report demanded by the protocol.

Speaking about that session on June 26, 2017, Thomas Bossert[2], US homeland security advisor at the time, said that the UN GGE format had reached its limits, and that it was time to consider other options. He added that "*While not abandoning our multilateral efforts, the United States will move forward internationally in meaningful bilateral efforts, such as the one we enjoy with*

[2] Thomas Bossert served as presidential homeland security advisor until April 2018

Great Britain and now Israel, while continuing to build a likeminded coalition of partners who can act together."

Trump has been deliberately and aggressively revising all multilateral cooperation mechanisms. He believes that they should either be made to serve US national interests (or rather his own interpretation of those interests), or be abandoned altogether. He might well pursue the same approach on the UN GGE.

There are two possible strategies of US involvement with the UN GGE:

1.The United States (and its key allies) may pull out of the Group and focus their efforts on the Cyber Deterrence Initiative.
2.Alternatively, an attempt can be made to re-boot the Group in a new format – for example, as a permanent working mechanism at the UN, with its own secretariat, regular working meetings, and decision-making on responses to cross-border cyber incidents or cyber threats.

The first option would largely delegitimize and devalue the GGE for all its remaining participants, especially if the US decision to pull out is followed by other key NATO allies and G7 partners. The second option, however, is likely to meet with resistance from Russia and several other key members since they may not necessarily be invited to take part in the putative new mechanism.

The GGE initiative was essentially an attempt at overcoming the initial (and deepening) rift in the values and approaches of different states to cyberspace regulation. At present, the Trump administration may – deliberately or not – serve as a catalyst of change, or even as a detonator for the entire current architecture of international dialogue and cooperation on stability and security in cyberspace. The likely outcome for Russian-US relations is the loss of the only universal and functioning UN mechanism for multilateral dialogue on cyber issues.

Recent developments make this scenario more likely, albeit in a rather surprising way. The United States has chosen an unexpected third option, essentially trading places with Russia in terms of the two countries' positions on the UN GGE. On November 9, Russia and the United States submitted two rival drafts of a UN General Assembly resolution at the First Committee. Both drafts have been accepted by members of the Committee. Both of them center on the future of multilateral dialogue on rules of responsible state conduct in cyberspace, and more specifically, on the future of the UN GGE:

- The Russian draft (A/C.1/73/L.27*) calls for a comprehensive re-launch of the Group in 2019 and for changing its format to include a broader range of participants. First, the text of the draft suggests that Russia wants the UN GGE to include more member states so as to ensure a more balanced geographic and regional representation. (The last few convocations of the Group included experts from 25 states, who were supposed to represent the entire international community). Second, the Russian draft calls for making the GGE more open to all stakeholders, including the private sector, experts, and technical organizations.
- The United States (as well as its NATO partners and members of the Five Eyes alliance) refused to back the Russian draft and submitted their own (A/C.1/73/L.37), which essentially calls for resuming the Group's work in more or less its previous format, with a few fairly minor changes.

The United States has effectively made a U-turn on its previous position regarding the UN GGE. In the 2004-2009 period, Russia was the main advocate and lobbyist of the Group (which was established at Russian initiative), while Washington was lukewarm and even sabotaged efforts to produce the GGE's first report in 2005. But now Washington itself wants the GGE to resume its work, and the text of its draft resolution highlights the importance of the proposals developed by the Group in 2013-2015, when its participants managed to agree the first proposed voluntary code of responsible conduct in the IT sphere, as well as basic principles on the applicability of international law to activities in cyberspace. Russia, meanwhile, insists that the group it helped to create back in 2004 has become ineffective in its current format and needs a radical transformation.

Be that as it may, these diplomatic games all lead to the same result: there is now a deep rift in the once-united platform for multilateral efforts on cyberspace regulation. The international community's two main ideological "cores" are pulling further apart. The exact composition of these two cores is illustrated by the list of co-authors of the two rival resolutions:

- The US-led core consists of the United States, NATO members, Australia, and Ukraine.
- The Russian-led core includes China, other SCO states, some of the CIS states, North Korea, Latin American states with leftist governments (Bolivia, Venezuela, Cuba and Nicaragua), Syria, and various African states.

Of course, the conflict is not over the format or principles of the multilateral mechanism's work. The real problem is the radically different ideological and doctrinal views on the application of international law in the IT sphere, the limits of national sovereignty in cyberspace, states' rights with regard to content control, and ultimately, the deep mutual mistrust and even confrontation in the global arena.

Furthermore, discussions of the two draft resolutions proposed by the United States and Russia almost coincided (with a difference of only 3 days) with a third independent initiative proposed by France. On November 12, President Macron announced The Paris Call for Trust and Security in Cyberspace. The text of the declaration contains no mention of the UN GGE, but the proposed nine priorities largely coincide with proposals developed by the Group in 2013 and 2015, with a somewhat greater emphasis on the private sector (IT corporations) and the technical community.

There is no real point trying to compare the nine priorities of the Paris Call with the list of voluntary rules drawn up by the UN GGE. The French initiative is not about proposing something genuinely new or innovative. Paris is merely trying to secure a more prominent role for itself as a mediator and engine of progress in developing universal rules for cyberspace. The French are making use of the split at the UN GGE and the collapse of the US-Russian dialogue. Macron is trying to reclaim France's role as a great diplomatic power in a new, critically important area of international relations, and to bring back the times when Paris acted as a respected and reputable mediator between the diametrically opposed positions of Washington and Moscow (now backed by Beijing).

Nevertheless, a French diplomatic triumph is not the most likely scenario for the foreseeable future. A far more likely outcome is Paris, Washington and Moscow pulling in three different directions on rules of responsible state conduct in cyberspace. We now have three different national initiatives that ostensibly aim to resolve the same issues, but are being positioned by their proponents as rival alternatives. This shows that genuine global dialogue on rules, codes of conduct, and regulation of cyberspace is falling apart.

A fragmentation of cyberspace, which has long been used as a bugbear by Russia, the United States, and other powers has now spread to the level of international diplomatic discourse and global dialogue on how to regulate cyberspace and this entire sphere of international relations. With each individual actor pulling in their own direction, the chances for any meaningful progress are slim.

Second, the prospects for the IT confidence-building track in the **OSCE** framework seem somewhat brighter. There are no particular reasons to destroy this particular mechanism, and in the current situation, confidence-building measures remain a more valuable and useful instrument than voluntary norms that everybody seems to ignore. There is, however, no reason to expect any tangible Russian-US cooperation in implementing confidence-building measures (such as cooperation between the national CSIRT/CERT authorities) in the OSCE framework. The two countries remain locked in a vicious circle whereby any confidence-building between them requires some minimum initial level of trust that is sadly lacking.

Third, there is the **bilateral** format of cooperation, which has yielded nothing constructive since 2014, when Russian-US agreements on confidence-building measures (signed by Putin and Obama the previous year) were frozen. Trump is unlikely to try to resurrect the 2013 mechanism, primarily because of the strong bipartisan pressure on the White House. Both the Republicans and the Democrats are pressuring him to pursue a more hawkish course on Russia, and calling for more measures to counter the "Russian threat in cyberspace". Besides, the existing package of confidence-building measures is also part of the Obama legacy, one of the final fruits of the Reset (a policy that was already crumbling in 2013), so Trump won't spend any political capital on trying to revitalize it.

What, then, are the options? In the immediate term, the current situation leaves no window of opportunity for any grand bargain on meaningful deal on sticking to the "rules of the game". Any constructive cooperation is out of the question. It is not even clear who could possibly benefit from such a grand bargain, or how. No bargain could possibly reverse the long-term processes such as the build-up of reconnaissance and military cyber capability by both parties, growing protectionism in their domestic IT markets ("import substitution") under the pretext of national security, or the growing emphasis on coalition formats to promote national initiatives and approaches to cybersecurity and cyberspace (with Russia showing a preference for acting via the Shanghai Cooperation Organization or BRICS, as well as via bilateral initiatives with China).

Now that Russia stands accused of launching massive cyber attacks against critical infrastructure in the United States and Europe, any attempts at overcoming the logic of confrontation are very unlikely to succeed in the next few years – not in Washington, at any rate. The new Cyber Strategy released by the White House is a case in point.

Bilateral scenarios for the next two years

- The most realistic format for any exchanges between Moscow and Washington on cyber security and cyber stability for the next two years boils down to **working visits and secret meetings** between armed forces and secret service representatives, arranged on an ad hoc basis.
- The issues on the agenda might include various technical formats and military-to-military communications to notify each other of any ongoing or scheduled cyber operations – including those likely to cause unintended (collateral) damage to one of the parties.
- Such mechanisms could be especially useful as an instrument of preventing a direct military confrontation or escalation in third countries and territories where the two sides are involved, directly or indirectly, in military operations or long-term conflicts (such as the one in Syria).
- The parties might also discuss ad hoc, informal agreements to **restrict cyber operations** against some categories of critical infrastructure (military or dual-use satellites, strategic C&C infrastructure) **on a mutual basis.**

Authors: Oleg Demidov, PIR Center consultant; and Margarita Angmar, graduate of the Applied Political Sciences Department at Moscow Pedagogical State University

Editor: Yulia Seslavinskaya

Dear members of Trialogue Club International,

The 2018 Club season continues, 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