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 № 10 (226), vol.14. October 2015

6 November 2015

Oleg Demidov reports from Moscow:

RESPONSIBILITY OF STATES FOR WRONGFUL ACTS IN CYBERSPACE: DISCUSSION IN THE WORLD AND IN RUSSIA

ANNOTATION

According to Oleg Demidov, PIR Center Consultant, by 2015 the world had finally recognized that states should develop binding norms of conduct in cyberspace. The article examines how the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) initiated by Russia contributed to this process. It looks into the key issues of this discussion, the attribution of cyberattacks and possible responses to them, as viewed by the leading Russian and international experts.

The author warns that unless states and regional alliances harmonize their efforts to interpret international law as applied to cyberspace, the world runs the risk of international legal anarchy in this sphere, which is fraught with international crises and even armed conflicts. The author believes that the mentioned United Nations Group of Governmental Experts would be the most suitable forum for elaborating a common consensus interpretation of the Charter of the United Nations and other key international legal norms as regards cyberspace.

UN GGE: FIRST STEPS TOWARDS THE REGIME OF RESPONSIBLE CONDUCT IN CYBERSPACE

On 22 July 2015, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) published its new report. That was the result of a year's work of the fourth session of GGE founded in 2001, and contained a set of political norms suggested to the UN members as a first step towards establishing the regime of responsible conduct in cyberspace.

Although the GGE in itself is perceived controversially by the West as Russia' initiative serving first and foremost Moscow's interests, its activities have been attracting increasing global attention. In particular, it was the focus of the fourth Global Conference in CyberSpace that took place in April 2015 in the Hague, Netherlands.

As Western diplomats and expert community, including private and government sectors turned towards the GGE in the Hague, two trends manifested themselves:

- ***First, the very discourse on the need for the states to develop norms of conduct in cyberspace has finally established itself prevailing over the alternative opinion that cyberspace needed no binding norms.***
- ***Second, it became obvious that despite long-standing contradictions on key issues among the GGE members (primarily between the representatives of the U.S. and Russia), the Group was working fruitfully and largely had no alternative, as the United Nations is the only global forum where common rules for trans-border cyberspace should be agreed.***

The increased global focus on GGE's activities was also due to the fact that as far back as when the third Group was convened, a fundamental task was included in its agenda: adapting the existing norms of the international law, including the UN Charter, to cyberspace. In its 2013 report GGE stated for the first time that the UN Charter was applicable to cyberspace, and in the 2015 Report the Group managed to agree on a number of key premises for the application of international law to cyberspace:

- A state has sovereignty over ICT infrastructure located within its territory;
- Such key principles of international law as State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States, should be observed in cyberspace;
- States have the right to take measures of unspecified nature consistent with the Charter of the United Nations in the context of cyberspace;
- A state should not use proxies to commit internationally wrongful acts in cyberspace and should not provide its territory to them;
- States should be held responsible for wrongful acts in cyberspace when the accusations are substantiated and such acts are properly attributed.

Although important, these premises are certainly but general starting points, and more complicated tasks of application are yet to be addressed. Those include attribution of cyberattacks and agreeing on responses to cyber operations recognized as acts of use of force (including the criteria for recognizing them as such).

ATTRIBUTION OF AND RESPONSE TO CYBERATTACKS. DISCUSSION IN RUSSIA AND THE WORLD

It is obvious that attributing cyberattacks involving states only makes practical sense if possible responses against the perpetrator of the wrongful acts in cyberspace are specified.

By way of example one can cite a well-known *Stuxnet* case. Today, as expert community believes based on David Sanger's investigation and Edward Snowden's statements,

there can be no doubt that the development of the *Stuxnet* worm and its use against the Natanz facility was the doing of the U.S. and Israeli special services. Let us imagine that back in 2010 Iran had engaged external experts and started trans-border investigation, managing to obtain technical evidence of the involvement of the National Security Agency and Mossad in the cyber-sabotage at its nuclear facilities. What could Iran do with the information it obtained? And how the international community represented by, for example, the UN Security Council or General Assembly, could qualify the actions of the U.S. and Israel even if Iran had presented convincing evidence of their involvement?

It is indicative that both Russian and NATO countries' leading experts and diplomats cannot answer this question. It won't be possible until there is clear interpretation of the key concepts of international law as applied to cyberspace. Leading Russian experts **Alexander Krutskikh and Anatoly Streltsov** in their article published in 2014 in the *Mezhdunarodnaya Zhizn'* magazine and the authors of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* prepared by **NATO** Cooperative Cyber Defense Center of Excellence (CCDCOE) list almost identical notions, including three most important ones:

- threat or use of force (Article 2(4) of the Charter of the United Nations);
- act of aggression (Article 39 of the Charter of the United Nations);
- armed attack (Article 51 of the Charter of the United Nations).

In the Stuxnet case, the major questions are as follows. If there is evidence of the U.S. and Israel's involvement in the development of Stuxnet and its use against Iranian nuclear facilities, should these actions be considered as use of force, act of aggression or armed attack within the meaning of the relevant articles of the UN Charter? And can Iran use its right to self-defense? No answer has been given so far, as there is no common interpretation of the UN Charter for cyberspace.

Of all the mentioned terms from the UN Charter, aggression is the clearest one, with special UN General Assembly resolution 3314 of 4 December 1974 devoted to it. The resolution contains a list of seven types of action qualified as aggression, which is followed by a language that the list is not exhaustive and can be amended by the UN Security Council resolution. At present this option becomes increasingly relevant, as the resolution adopted 41 years ago naturally makes no provision for actions involving ICTs and aggression in the context of cyberspace.

The resolution was analyzed in great detail in a recent publication by a group of authors from the Russian Ministry of Defense. **Russian military experts** suggest adjusted interpretation of the resolution applying it to operations in cyberspace potentially falling within the scope of definition of aggression, rather than amending the text. In particular, they suggest that the use by a state of proxy servers situated in the territory of another state for committing attacks against the third state, should be considered as an act covered under the scope of paragraph f) of article 3 of the resolution (State allowing its territory to be used by other State for perpetrating an act of aggression against a third State). They also suggest that paragraph g) (the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State) should be applied to hacker proxy groups.

At the same time, the MoD experts acknowledge that the UNGA resolution has a major disadvantage: it is not binding. In this context, these authors had previously proposed a noteworthy option of incorporating a definition of aggression adjusted to cyberspace in **the Rome Statute of the International Criminal Court** (ICC). In 2011, the Review Conference of the Rome Statute of the International Criminal Court adopted a resolution on incorporating the definition of *crime of aggression* from the UNGA resolution 3314 into the ICC Statute. Yet a corresponding decision of the next Review Conference of the

Rome Statute scheduled for January 2017 is required to complete this process (which may also be postponed until later). It would be advisable to stimulate international debate on adjusting the text of resolution 3314 (and at the same time the definition of the crime of aggression in the Rome Statute of the ICC) to cyber operations. The fifth UN GGE, which is to be established in 2016, appears to be the best suited forum for this debate.

POTENTIAL PROSPECTS AND RISKS FOR RUSSIA AND THE INTERNATIONAL COMMUNITY

Although the members of the GGE, including Russian diplomats have repeatedly stressed that the Group's mandate does not include in-depth revision of the norms of international law for adjusting them to cyberspace, it seems highly probable that the Group will not be able to avoid this task completely. The longer GGE tries to refrain from it, the more probable it is that the leading nation states will develop political and military policies as regards cyber operations relying on interpretations of international law agreed at other fora, or adopted unilaterally and agreed with no one.

To some extent, this has already been happening.

- The recent (June 2015) issue of the US *DoD Law of War Manual* provides a clear list of criteria and conditions under which a cyber operation is qualified as illegal use of force within the meaning of Article 2(4) of the Charter of the United Nations. Although the Manual is not a legal source and is not binding, its provisions are intended as practical instructions for the servicemen of the U.S. Army, including such structures as the U.S. Cyber Command.

- At the same time, the conclusions made when working on the *Tallinn Manual*, despite its exclusively expert non-official status, have already been built on in NATO's strategy. NATO Wales Summit of September 2014 reviewed the Enhanced Cyber Defense Policy of the Organization. As a result, a political decision was made that NATO member states' right to collective defense enshrined in Article 5 of the Washington Treaty applies to certain cases when NATO members are attacked in cyberspace. From now on, a cyberattack against a NATO member causing fatalities or large-scale infrastructure damage and deemed by the Alliance to be committed by a state — directly or through proxies — may bring about NATO's armed response using all its military capabilities and not confined to cyberspace. In such cases, the attribution of cyberattack capable of triggering collective defense mechanism will be decided by the NATO military command on a case-by-case basis.

> ***Potential risks of this approach are vividly illustrated by the 2007 example of Estonia hit by a wave of cyberattacks in the heat of the 'Bronze Soldier crisis'. It asked NATO leadership of possible application of Article 5. In that case Estonia, despite the lack of credible evidence, considered Russia to be the aggressor and accused it of organizing and perpetrating the cyberattacks. Should similar situation occur today, after the new NATO cyber defense doctrine has been adopted, it might bring about the escalation of the crisis between NATO and Russia.***

As various states and regional alliances advance at different pace and in an uncoordinated manner in interpreting international law as applied to cyberspace, the international community is running the risk that in the absence of a single forum the opportunity to elaborate a common approach or at least effectively harmonize their approaches will soon be lost. As a result, the world can face a situation in which numerous government actors will engage in trans-border cyber operations across the world guided solely by their own or by some limited groups' visions of what is acceptable in this field. One can imagine that such international legal anarchy multiplied by trans-border nature of almost any operation in cyberspace can very soon lead to international crises and even armed conflicts. Indeed, states' response to hostile actions in cyberspace in the absence of a transparent and generally accepted international legal mechanism for resolving difficulties may not be confined to cyberspace.

From this perspective, the elaboration by the GGE of 11 'voluntary, non-binding norms, rules or principles of responsible behavior of states' even as general and exclusively voluntary proposals to the international community, is a considerable step forward in the context of strengthening the debate on responsible conduct of states in cyberspace. Today, GGE appears to be the only relatively inclusive, authoritative and compromise forum to try to elaborate a generally acceptable consensus interpretation of the UN Charter and other key norms of international law as applied to cyberspace and thus prevent the scenario discussed above.

Author: Oleg Demidov, PIR Center Consultant.

Editor: Julia Fetisova

Excerpts from the Membership Terms and Conditions at the Trialogue Club International

[…]
3. The rights of the Club members
3.1. Individual club members are entitled to:
3.1.3. Receive a copy of the Russia Confidential exclusive analytical newsletter by e-mail in chosen language (English or Russian). According to the Club Terms and Conditions, the transfer of the bulletin to third parties is not allowed.
[…]
3.2. Corporate Club members are entitled to:
3.2.3. Receive two copies of the Russia Confidential exclusive analytical newsletter by e-mail in chosen language (English or Russian) or in both languages simultaneously. Share the bulletin with the other representatives of the corporate member. According to the Club Terms and Conditions, the transfer of the bulletin to third parties is not allowed.
[…]
4. The duties of the Club members
4.1. All members of the Club must:
4.1.6. Not to share the Russia Confidential analytical newsletter, as well as the Password to the Club section of the PIR Center web-site with individuals and legal entities who are not members of the Club.
[…]
6. Russia Confidential
6.1. The Russia Confidential exclusive analytical newsletter is issued by the Trialogue Ltd for the Club members' private use only.
6.2. The newsletter contains exclusive analytical materials on international security, foreign and domestic policy of Russia and the CIS, prepared by the leading experts specially for Russia Confidential.
6.3. The newsletter materials are confidential and must not be quoted and transfer to the non-members for at least 30 days since the day of issue.
6.4. 30 days after the day of issue the Trialogue Ltd can remove the exclusive and confidential status of the material, after which in such cases it can be published in other editions and can be used by the Club members for quoting.
6.5. The newsletter is disseminated via e-mail between the Club members once a month in Russian or in English, depending on the choice of the Club member.
6.6. The Club member can also receive a paper copy of the newsletter in chosen language.

Dear members of the Trialogue Club International,

We continue 2015 Club season and are glad to **invite you to prolong your membership for 2016 or 2016-2017**, if you have not done so yet.

In 2016, the *Trialogue* Club members will continue to receive our exclusive information on the foreign policy priorities of the Russian Federation, and on current threats and challenges to global security. **Five meetings of the *Trialogue* Club International** are planned for 2016 (four in Moscow and one abroad); Club members will receive 4 issues of the Security Index quarterly journal in electronic form and 2 issues in print (in 2016 only in Russian), **12 issues of the *Russia Confidential* exclusive analytics bulletin**, our informational and analytical newsletters.

As before, experts of the *Trialogue* Club International and of its partner organization PIR Center are open to an exchange of views on key international problems.

Fees for the *Trialogue* Club membership since 2016 are as follows:

Period	Individual membership	Corporate membership
01.01.16. – 31.12.16. (1 year)	50 000 rub.	80 000 rub.
01.01.16. – 31.12.17. (2 years)	90 000 rub.	140 000 rub.

We would like to remind you that the corporate membership is based on **"1+1" scheme** when **two representatives** of the organization participate in the work of the Club.

Please note that when paying membership fees no later than 30 November of the year preceding the year of membership that is paid for, a 10% fee discount is applicable.

On all questions concerning the *Trialogue* Club Internationsl membership, please contact us by the e-mail secretary@trialogue-club.ru or by phone: +7 (985) 764-98-96

Sincerely,

Chairman,
***Trialogue* Club International**

Dmitry Polikanov