Alexandra Kulikova
Program Coordinator
"Global Internet Governance and International Information Security", PIR Center

GCCS 2015: Groping for Rules of (Non-) Engagement in Cyberspace

The 4th Global Conference on Cyberspace, which took place in the Hague, the Netherlands, on 16-17th of April, left mixed feelings. The Dutch government has clearly put a lot of effort into getting the most burning issues of cybersecurity into its agenda, enlarging the participation of stakeholders in the dialogue by inviting representatives of the civil society. However, many participants of the GCCS left the Hague with a feeling that there was an elephant in the room.

"London process" 4.0

Without going deep into the history of the GCCS format, it should be mentioned that the GCCS 2015 is the 4th conference in what is known as the "London process". It started in 2011 with the first Global Conference on Cyberspace in London which put the cybersecurity agenda on the global scale for the first time. During the conference Igor Shchegolev, Minister of Telecommunications and Mass Communications, highlighted the Russian initiatives to ensure international information security, with emphasis on the Russian initiative of the UN Convention on ensuring international information security. In particular, the initiative was aimed at curbing the abuse of information technologies against interests of individual states and the modern world overall. This initiative was negatively perceived as an attempt to legalise instruments to combat dissent in the global network.

The following conferences in Budapest (October 2012) and Seoul (October 2013) showed no breakthrough by not reaching any real agreements. However, the framework agreement following the results of the Seoul meeting stating adherence to open and secure cyberspace reflected the report of the UN Group of Governmental Experts on the applicability of norms of international law, including the UN Charter, to cyberspace. There was no room for breakthrough decisions in the autumn of 2013

after Snowden revelations: the session of Internet Governance Forum of the UK on future Seoul conference seemed quite strange. The burning issue of electronic surveillance and tensions in relations of governmental partners was not included in the agenda of the event. Unsurprisingly, the conference series wasn't continued into 2014.

Nevertheless, the growth of cybercrime at the global level and geopolitical tensions revealed the necessity to discuss and come to an agreement on states' behavior in transborder and incoherently regulated cyberspace. In 2015, the government of the Netherlands made a big effort to revive the forum, which had somewhat lost its authority, by putting together a busy programme of events prior to the conference and on its sidelines, and particularly by making it open for the representatives of civil society.

On 14-15th of April the civil society pre-event (about 40 people) took place, representing civil society organisations from all over the world, in particular from Asia, Latin America, Middle East, Africa (so-called Global South countries). Taking into account the diverse level of competence in the subject among the participants, a series of webinars was conducted on the key GCCS issues. The training itself consisted of role games and brainstorm sessions in small groups in order to get understanding of where and how the voice of the civil society is incorporated in the context of the conference (announced topics: freedom, development, security). Above all, it is the human rights domain: privacy protection and protection of freedom of speech. The participants had an opportunity to come up with suggestions to be submitted for the official statement of the Chair of the conference. Bert Koenders, Minister of Foreign Affairs of the Netherlands, visited one of the sessions of the pre-event functions. Moreover, one of the sessions of the GCCS was dedicated to the issue of privacy protection online.

The conference itself saw a number of bold statements by state representatives of participating countries. In particular, Federica Mogherini, High Representative of the European Union for Foreign Affairs and Security Policy, said that states should undertake responsibilities to prevent their territories from launching cyberattacks against other countries. The necessity to set up a list of objects of critical infrastructure, against which it would be prohibited to conduct computer-sabotage, was highlighted. However, the calls for reaching agreements on the norms of conduct in cyberspace were fruitless. One of the main reasons behind this is that parties again didn't reach an agreement about the usage of key definitions and legal notions in the field of cybersecurity. Moreover, the nuances of the applicability of international law (e.g. international humanitarian law) to cyberspace still are a stumbling block and an area of ongoing debates. The principle of responsible behavior of states in order to prevent conflicts in cyberspace still is a vague "grey area".

Good intentions

Many participants pointed out the scope of the conference and its top level technical and content preparation. The number of participants was impressive (about 1800 people), as well as the number of events on the margins of the conference and a couple of months prior to it. According to mass media reports, the organisational cost of the conference amounted to €15 million. At the same time, the economic effect of the deals made on the margins of the GCCS 2015 is yet to be assessed in the future.

Participants' impressions are very different regarding the content of the conference. Besides undoubtedly good opportunities to communicate behind the scenes, establish new contacts, and meet partners, many participants noted a shallow level of discussions in some sessions and a similarity with the IGF format regarding the absence of concrete binding results from discussions.

The key message of the Dutch government at the conference was a call for countries to start making agreements about the code of conduct in cyberspace, which would minimise the risk of conflicts in cyberspace and curb the growth of cybercrime. The necessity of such norms is imminent. The necessity to define conditions for a "new social contract" between governments and citizens of different states balanced between "security" and "privacy rights" in the context of the information society was also highlighted. Such a social contract would be helpful to divide the notions of personal and national security and to ensure users' security in the Internet. For that purpose, a great emphasis is put on confidence-building measures between different actors in cyberspace, as well as capacity building in those societies, which face the most serious threats.

As one of the outcomes, the Global Forum on Cyber Expertise was established and headquartered in the Hague. It was an initiative of a number of states (including the USA, the UK, Canada, Switzerland, Vietnam, Bangladesh, Mexico, etc.), private companies (including Miscrosoft, HP, Huaiwei and others), and international organisations (ITU, Europol) to create a platform for the exchange of experience and building competences? in the field of cybersecurity all over the world to combat cybercrime and other cyber-threats. Christopher Painter, Coordinator for Cyber Issues of the U.S. Department of State, has mentioned in his blog, which summarises the results of the GCCS, the agreements the USA reached at the forum on the development of legal framework for ensuring cybersecurity and raising awareness about the existing threats on the African continent and in Southeast Asia. However, the description of the project's mandate is quite sketchy and it is not very clear how the project will work in reality. It is hard to expect any exchange of advanced experience and top technologies in context of the low level of confidence among cyber-powers, while it's obvious that all the technologies passed on to worse equipped countries will be sponsored by certain players interested in the advancement of their products to underdeveloped markets. Seen in the context of overall militarisation of cyberspace, this initiative would hardly contribute to deterrence of cyber-weapon build-up. Russia has not joined the initiative of the Forum yet.

The problem is still there

As for the Hague, it has clearly strengthened its position not only as an international diplomatic and legal hub, but also as a global center of cybersecurity competence. This fact, without any doubt, reinforces the ambitions of the Netherlands to secure a non-permanent seat in the UN Security Council for the term 2017-2018. This could explain such close attention to the activities of the UN Group of Governmental Experts on developments in the field of information and telecommunications, which, by the way, originally initiated on the Russian side. For the first time in the framework of the GCSS global format, organised in the first place by western countries, the work of the GGE in the field of acknowledgement of the applicability of the UN Charter and international law towards cyberspace was publicly highly

appreciated, while understanding the necessity of further work on the adaptation of their provisions. What is more, the priority of the UN GGE activities was emphasised as one of the key points in the preliminary draft of the statement of the conference's Chair. In many respects, it's a milestone given that the role of the GGE activities much driven and inspired by Russia, even if acknowledged earlier, has never been promoted openly at the global level, especially on the western platforms.

At the same time, the parties are not yet ready to sign a new agreement on the code of conduct in cyberspace. The existing international legal framework partially allows for regulation of states' behavior in cyberspace, but requires significant revision and precision, primarily in the field of *jus ad bellum* and *jus in bello.* At the same time, the states' behaviour in the pre-threshold period remains "a grey area". In addition, an updated draft of the Code of conduct in the field of ensuring international information security submitted to the General Assembly in January 2015 by the Shanghai Cooperation Organisation countries, developed to prevent international conflicts in cyberspace, was ignored at the conference. At the GCCS the document was mentioned only by Vladimir Lapshin, representative of the Department on New Challenges and Threats of the MFA of Russia, in his address during the plenary meeting, and by Chinese Ambassador to the Netherlands during one of the sessions of the conference.

In other words, one may agree about the principle of the applicability of the norms of international law to cyberspace, even though admitting the necessity to specify a number of details, while it's still hard to agree on "what is bad or good" in cyberspace prior to the escalation of conflict even on the level of *soft law*.? It was evident both during the main sessions of the GCSS 2015 and the discussions of civil society representatives. Conceptual disagreements on the issue of cybersecurity and information security still seem to be insurmountable, but it is not worth simplifying them to confrontation fix of authoritative regimes with the western world. Normative contexts in the world are far more divergent and the visions of what is allowed or not and where civil rights are limited by national security concerns are different at the national level in various countries. That is why confidence-building measures and cyber-potential build-up are naturally feasible exactly at the national level, activities should be concentrated on it prior to fix harmonise approaches at regional and global level. Geopolitical tensions in Europe over Ukraine clearly impede such an approach.

Nevertheless, it can be assumed that the presence of a new emerging threat, the Islamic State, and the problem of radicalisation of cyberspace on the global scale could push participants to the rapprochement of their positions, given their goodwill. While being unwilling to use the term "information security", many western countries are busy implementing it in their information space – it's seen from both statements on countering Russian propaganda in social media and laws on online extremist content filtering. At the very least, Russia is known for its large experience in this field.

The task of global norms creation is complicated as well by the fact that, even if led by the states, the combating cybercrime and cyber-weapon nonproliferation activities are impossible without the private sector, which generates the necessary technologies and is interested in the continuity of business processes. In that sense, business becomes a far more significant partner of governmental actors than could be assumed,

notably regarding the code of conduct in that very "grey area", prior to the direct conflict. In that sense, six norms of state behavior to prevent conflicts in cyberspace by Microsoft are worth mentioning. The company presented this project in December 2014 and has been actively promoting it since then on many platforms, including the GCCS. The attitude towards it as a precedent initiative, addressed in particular to the states and introduced by a non-state actor, could be ambivalent. The company is tackling its business-tasks against the background of its ongoing case against the US government, specifically as it concerns the norm number one on the inadmissibility of introducing bookmarks in the products of private companies in the IT industry. Nevertheless, if this initiative is supported by a coalition of other big private players, it could have an interesting development.

In this context, agreements on the elaboration of the code of conduct in cyberspace to ensure security and resilience of global infrastructure of the Internet are the most probable as it is the least politicised issue in this field. Reaching an agreement between Russia, the USA, China and other major cyber-powers on non-interference in the work of the Internet's system of unique identifiers (DNS, the system of the distribution of IP addresses and Autonomous System Numbers). For example, in the framework of expert round table in the Hague Institute for Global Security on the margins of GCCS Dr, Dennis Broeders, senior research fellow at the Netherlands Scientific Council for Government Policy and professor at the department of Sociology of the Erasmus University Rotterdam, called for the assignment of the status of global public good to the global infrastructure of the Internet. He also called for the elaboration of the code of conduct, which would guarantee its inviolability and would allow for separation of security problem-solving of the Internet itself from policies to ensure national security in the digital age. Similar ideas were expressed many times in various interpretations on the margins of the GCCS and were mentioned in the Chair's concluding statement.

Besides mentioned issues, following provisions in the Chair's concluding statement should be pointed out:

- The GCCS expressed its support of the transfer of the stewardship of the functions of the IANA to the global multi-stakeholder community and calls for paying due attention to ensuring stability, security and resiliency of the Internet.

- The Internet Governance Forum (IGF), whose mandate will be reviewed in December 2015 during the WSIS + 10 meeting, should remain a global platform for dialogue on the issues of Internet governance (at the same time, the creation of an enforcement mechanism for its decisions to become binding wasn't mentioned). It is recommended that the event itself be conducted with the inclusive participation by all stakeholders, including non-governmental organisations.

- Special attention is paid to the Public Private Partnership in the field of ensuring the security of critical infrastructure and the global Internet infrastructure both at the national and international level through the mechanisms of best practices exchange, as well as through the framework created at the Global Forum on Cyber Expertise conference. The importance

of mature mechanisms of the development of Internet technical standards (IETF standards) and their successful use was highlighted.

- Great responsibility is imposed on governments in the field of creation and development of national systems for ensuring security of critical infrastructure and capacity building in the area of defensive measures, as well as in the field of exchange of experience and mutual help.

- The necessity to respect and protect human rights in the process of policy-enforcement in the field of national security in the context of cybersecurity was mentioned separately. However, human rights activists were not satisfied with the scope of the discussion regarding the issue of privacy protection and its indistinct formulation in the final document of the conference.

The next GCCS 2017 will take place in Mexico. In two years the activities of the created forum GFCE should give, at least, the first results. A certain impulse towards a real rapprochement can be expected from the UN GGE in case of stabilisation of geopolitical tensions unless its reduction.? Finally, mutual confidence of the parties, which still is lacking, remains the key element for any progress in the field of cybersecurity and information security.