NIDS 防衛研究所
The National Institute for Defense Studies

Dispute over Governance of Cyberspace

Yu Harada, Global Security Division, Policy Studies Department

NIDS Commentary No. 43 June 3, 2015

1. Introduction

Cyberspace can be defined as "global virtual spaces such as the internet, composed of information systems, information communications networks and similar systems and which circulate large quantities of a large variety of information." [1] Regarding cyberspace governance (regarding the Internet in particular), there is a variety of views which can be divided roughly into two groups.

First group, mainly led by Western countries, has been advocating for not only the freedom of information, but also significance of collaboration between the governments and the private sectors (a multi-stakeholder model). By contrast, the latter group, led by some emerging states, authoritarian states in particular, emphasizing both the government's dominant role in cyberspace and the necessity of the government's control of the information which seems to include even censorship of communication.

The differences between the two standpoints have become apparent in various international discussions over cyberspace. Above all, the Group of Governmental Experts (GGE) of the United Nations General Assembly First Committee (Disarmament and Security), World Summit on the Information Society (WSIS) and Global Conference on CyberSpace (GCCS) have been a significant international conferences which tackled the issues.

This year, a report submission by the fourth GGE and the review of achievements concerning WSIS are scheduled at the UN General Assembly. Furthermore, the fourth GCCS will take place in Hague, the Netherlands this April. Accordingly, it is worth to look back at the discussion which has advanced so far at these conferences.

2. Group of Governmental Experts (GGE)

The GGE, constituted by the United Nations General Assembly First Committee, has been discussing cyberspace related issues primarily from the perspective of international security. This originated with the resolution on "Developments in the Field of Information and Telecommunications in the Context of International Security,"[2] which was a resolution based on the proposal of Russia, adopted by the UN General Assembly without a vote in December 1998. Since then, the GGE has been constituted regularly in order to "consider existing and potential threats in the area of information security and possible joint measures to eliminate such threats, to examine relevant international concepts aimed at strengthening the security of global information and telecommunication systems."[3]

In contrast to Russia, which supported the UN as an arena for discussion, the reaction of the Western countries was not so affirmative. One of the reasons of this reaction arose from Western countries' concerns that "information security" could include censoring of communication content by the government which would be threatened the freedom of communication.

For example the United States expressed views that although some countries claim advantages of setting an international rule for securing information network and

infrastructure, it would enable the censoring of communication content by governments, contrary to the principle of the freedom of telecommunication which is vital for the growth and prosperity for all countries.[4] Furthermore, with regard to international rules, the United States advocated for applying already existing rules such as the UN Charter and the Universal Declaration of Human Rights instead of creating new ones.[5]

The first GGE was constituted in June 2004.[6] Unfortunately, due to difference of views among participants, the first GGE failed to adopt a consensus report. As the reason of this failure, the representative of Russia who chaired the session raised time restrictions and lacking of definitions of terms regarding cyberspace. However, more crucial reason is assumed to be that the United States and European countries' stance was differ from Russia, China, Brazil and Belarus which not only favour the government's dominant role to ensure their own information security, but also consider the adoption of new rules.[7]

After the first GGE, cyber-related issues have become hot topics in international security arena. Increasing the number of co-sponsor states of the resolution on "Developments in the Field of Information and Telecommunications in the Context of International Security" shows this fact.

Since Russia opened the resolution for co-sponsorship in 2006, the number has been on the increase including the members of the Shanghai Cooperation Organization such as China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. The United States, which has been critical, has also become one of the co-sponsors in 2010.

There are several reasons in the background of this change of trend.[8] First, the continuous large-scale, organized cyber attacks since the 2000s. For example, DDoS attacks targeted Estonia in April 2007 and Georgia in August 2008. In 2010, Stuxnet Attack was also reported. Furthermore, one can observe growing interest in Internet regulation in certain countries as a result of the full-scale movement towards democracy in the Middle East and North Africa ("The Arab Spring") since early 2011. In addition, what led to the policy shift of the United States was the arrival of the Obama administration (January 2009), which has since its early days shown a strong interest in cyber security, and have been actively engaged in international discussions.

In this light, the second GGE was constituted from November 2009 to July 2010. At this time, GGE succeeded in adopting a consensus report.[9] The report confirmed the necessity of a further review of the guidelines for the protection of critical infrastructure, confidence building measures, capacity building, and a clarification of terms and definitions.[10] Though, progress has been made in the discussion, the main points, such as government's role in cyberspace and what kind of rules should be applied, have yet to be settled.

Significant progress in discussions was made at the following third GGE (August 2012 to June 2013).[11] The consensus report after the session affirmed that "International law, and in particular the Charter of the United Nations, is applicable" and that "State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in Universal Declaration of Human Rights and other international instruments."[12] Specifying the adoption of existing international laws advocated by Western countries in the report is viewed as an important achievement of the third GGE.

Nonetheless, this does not mean that the differences in views between the countries have been resolved.[13] What comes to our attention is the term, "applicable." This term may indicate there are cases where they are not "applicable," and a possibility of making new rules cannot be denied. Moreover, also noteworthy is that the third GGE mentioned "International Code of Conduct for Information Security," which was proposed to the UN jointly by Russia, China, Tajikistan and Uzbekistan (Kazakhstan and Kyrgyzstan have joined since 2013) in September 2011, in the report. This is because although

this document is set out to respect the rights and freedom in the information space, it also specifies the compliance with relevant national laws and regulations as a prior condition, which might advocate the governments' dominant role in cyberspace and the possibility of the censorship of telecommunication content.

It could be concluded that while some progress was made in the discussions at the third GGE, its actual results did not do away with the issues. Thereafter, in December 2013 the UN General Assembly approved a resolution calling for the fourth GGE. The fourth GGE is currently underway and new reports are expected to be released within this year.

3.World Summit on the Information Society (WSIS)

The trigger to hold the World Summit on the Information Society was a resolution made at the Plenipotentiary Conference of the International Telecommunication Union (ITU), held in Minneapolis in 1998, to hold a world conference in light of the arrival of the information society. Based on the ITU's resolution, the UN General Assembly adopted the resolution on the "World Summit on the Information Society" in December 2001. Under the leadership of ITU, it was decided that WSIS was to be held in two phases. The first phase was to take place in Geneva in 2003 and the second was to take place in Tunis in 2005.[14]

Initially the Summit put emphasis on economic development utilizing ICT, and focus on dissolving the digital divide between advanced states and emerging states. However at the Preparatory Committee for the Geneva phase of WSIS, Internet Governance surfaced as a focus for controversy. Some emerging states have started to call for the multilateral management or management by international institutions of Internet resources such as IP addresses and domain names.[15] At present, in terms of resource management, ICANN, a non-profit organization based in California, serves a central role basing on contracts with the US Department of Commerce (DOC). Given this fact, some emerging states expressed concerns that the United States are in an advantageous position in terms of resources management, and advocated that multilateral management or management by international institutions would be more appropriate. For this reason, the Internet Governance instantly became the main agenda at the WSIS.

At the Geneva Summit in December 2003, discussions fell in disorder over Internet Governance.[16] Countries such as China, Brazil, and South Africa have all raised an objection against the current resource management system with the ICANN at the center. Conversely, the United States and the European countries generally supported the current system, and opposed the excessive government intervention with regard to governance based on the fact that the Internet expansion has been led by the private sector. The Geneva Summit highlighted the lack of a consensus among the countries pertaining to Internet Governance.

The argument continued at the summit in Tunis (November 2005). Although at the Preparatory Committee for the Tunis phase changes were seen where the EU began to show a positive attitude towards internationalization of resource management, but the Tunis Summit resulted in favour of maintaining the status quo of the system centred on ICANN.[17] The Tunis Agenda for the Information Society which collectively summarizes the past discussions and future issues was confined to requesting the UN Secretary-General to establish the Internet Governance Forum (IGF) in 2006 and seeking continuous discussions. Furthermore, the IGF is positioned as no more than a place for communication and not a place to adopt a binding resolution. Since the First IGF in Greece in October 2006, it has been held annually.

Discussions and initiatives concerning WSIS are ongoing after Tunis Summit. This year, not only will the WSIS outcomes implementation be reviewed by the

UN General Assembly, but it is also expected that IGF's continuance beyond 2016 will be decided.

Under these circumstances, the DOC issued an important statement in March 2014. The department announced that it was prepared to transfer the authority of Internet resources management which the DOC had outsourced to ICANN, to a global multi-stakeholder community.[18] Taking into account the past events that the relationship between DOC and ICANN has been criticized by some countries, it can be understood that this statement carries a significant meaning.

Why was the statement made at this timing? Some reasons can be pointed out. Since the establishment of the ICANN, the US government have been expressing its view that its authority was time-limited, and that once the private sector could appropriately conduct the resource management, it is prepared to transfer the management. Therefore, it can be said that such an opportunity arose. However, a more important factor was the Edward Snowden incident in June 2013. This incident, which was a whistleblowing event that accuses the US government for telecommunication surveillance, denounced the US government's stand point as being critical of excessive government intervention in telecommunication. Therefore it can be assumed that the US government timed the announcement to ensure the management by the multi-stake holders.

4.Global Conference on CyberSpace (GCCS)

Discussions regarding Governance in cyberspace are also being conducted outside the United Nations arena. Such an example is the Global Conference on CyberSpace initiated by the UK government and first held in London in November 2011. After London, the conferences have been held in Budapest (Hungary, October 2012) and Seoul (South Korea, October 2013). One of the characteristics is that there are many participants not only from the governments, but also from the private sector and nongovernmental organizations (NGOs). GCCS can be described as an exemplar of the conference that embodies the multi-stakeholders model.

Main objectives of the conference are to achieve the simultaneous pursuit of a stable cyberspace and economic expansion and development, to take measures towards international security, promote measures against cyber crimes and to foster international norms. According to Britain's' Foreign Secretary William Hague who chaired the London conference, discussion at the conference should be based on existing work, undertaken by the Geneva and Tunis Summits of the WSIS, Organisation for Economic Co-operation and Development (OECD), the Council of Europe the Association of South East Asian Nations (ASEAN), etc. In addition, it was stated that GCCS's aim was not to bring the discussion back to the starting point or to create new institutions.[19]

Accordingly, at the Seoul conference, the "Seoul Framework for and Commitment to Open and Secure Cyberspace" was adopted sustaining the previous discussions. This framework is based on the United Nations General Assembly resolutions, reports generated at the GGE, and fundamental principles confirmed at the WSIS Geneva Summit.[20]

At GCCS, different opinions with regard to the government roles and appropriate regulations still exist. For example, Russia and China call for discussion based on "International Code of Conduct for Information Security."[21] Moreover, at the Seoul Conference, China asserted that the suitable place to debate global cyber issues is the United Nations.[22] Thus, arguably, GCCS seems to be discussing very similar issues to GGE and WSIS.

However, holding GCCS has significant meaning since it can show the importance of multiple actors joining the debate, and the possibility to develop transparency and openness of cyberspace, and polices to firmly maintain freedom. The importance of GCCS will be emphasized considering that some emerging states prefer for the discussions to be held mainly at UN

organizations whose participants are primarily states. Further progress of discussions is anticipated at GCCS 2015 in Hague, the Netherlands to be held this April.

5.Conclusion

At the moment, various discussions are taking place with respect to the foundation of norms and rules in the governance of cyberspace. Due to the apparent difference of views among states, it is reasonable to organize different international conferences which would allow to approach the issues from different angles. One such example is the World Internet Conference held in November 2014 by the Chinese government.

The issue of cyber governance is not something that can be solved in a day, but something that will develop over time through an accumulation of discussions. For that reason, discussions at various occasions will help deepen the substance of the debate. On the other hand, so-called "forum shopping," the situation where the actors select meeting bodies that satisfy their needs, runs the risk of hindering the cohesion of cyberspace, for instance the Internet which has brought significant benefits to the global society. Further developments will come under focus from here on out.

(Completed on March 12, 2015)

---

[1] Information Security Policy Council, *Cyber Security Strategy: Towards a World-Leading, Resilient and Vigorous Cyberspace* (June, 2013), p. 5 <http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf>, accessed on March 12, 2015.
[2] UN General Assembly (UNGA), A/RES/53/70.
[3] UNGA, A/C.1/60/PV.13.
[4] UNGA, A/59/116/Add. 1.
[5] Masaru Fujino, "Internet Freedom: Pursuit of an International Norm," *Internet and the US Politics* (The Tokyo Foundation, October 2013), pp. 5-6 <http://www.tkfd.or.jp/research/project/news.php?id=1195#>, accessed on March 12, 2015.
[6] Member states of the GGE are selected on the basis of equitable geographical distribution. 15 states took part in the first GGE which were Belarus, Brazil, China, France, Germany, India, Jordan, Malaysia, Mali, Mexico, the Republic of Korea, the Russian Federation, South Africa, the United Kingdom of Great Britain and Northern Ireland and the United States of America.
[7] Eneken Tikk-Ringas, *Development in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012* (Geneva; ICT4Peace Publishing, 2012), pp. 6-7 <http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf>, accessed on March 12, 2015.
[8] Ibid., pp. 7-8.
[9] Member states of the second GGE were Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, Qatar, the Republic of Korea, the Russian Federation, South Africa, the United Kingdom of Great Britain and Northern Ireland and the United States of America.
[10] UNGA, A/65/201.
[11] Member states of the third GGE were Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland and the United States of America.
[12] UNGA, A/68/98.
[13] Regarding the third GGE, refer to the following. Motohiro Tsuchiya "Cyberspace Governance," *Rising Challenge for the Japan-U.S. Alliance in the Global Commons: Cyberspace, Outer Space and the Arctic Ocean* (The Japan Institute of International Affairs, March 2014), pp. 35-36 <http://www2.jiia.or.jp/pdf/resarch/H25_Global_Commons/04-tsuchiya.pdf> accessed on March 12, 2015.
[14] UNGA, A/RES/56/183.
[15] For example, in the "Beirut Declaration" that was adopted at Western Asia Preparatory Conference for the WSIS, it was stated that a suitable international organization should manage the domain names. Western Asia Preparatory Conference for the World Summit on the Information Society, *Beirut Declaration: Toward an Information Society in Western Asia* (Beirut, February 2003) <http://www.escwa.un.org/wsis/conference/outcome/beirut.pdf>, accessed on March 12, 2015.
[16] Milton Mueller, John Mathiason, and Hans Klein, "The Internet and Global Governance: Principles and Norms for a New Regime," *Global Governance*, No. 13 (2007), pp. 238-243.
[17] Lennard G. Kruger, *Internet Governance and the Domain Name System: Issues for Congress* (Congressional Research Service, November, 2014), pp. 11-12 <http://fas.org/sgp/crs/misc/R42351.pdf>, accessed on March 12, 2015.
[18] National Telecommunications and Information Administration (NTIA), *NTIA Announces Intent to Transition Key Internet Domain Name Functions* (DOC, March, 2014) <http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>, accessed on March 12, 2015.
[19] Foreign & Commonwealth Office and The Rt Hon William Hague MP, *Announcement London Conference on Cyberspace: Chair's statement* (U.K. Government, November, 2011) <https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement>, accessed on March 12, 2015.
[20] Seoul Conference on Cyberspace 2013, *Seoul*

Framework for and Commitment to Open and Secure Cyberspace
<http://www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf>, accessed on March 12, 2015.
[21] The Ministry of Foreign Affairs of Japan (MOFA), "Budapest Conference regarding Cyberspace" (October 2012)
<http://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/cyber_1210.html> , accessed on March 12, 2015.
[22] MOFA, "Seoul Conference regarding Cyberspace" (October 2013)
<http://www.mofa.go.jp/mofaj/gaiko/page18_000084.html> accessed on March 12, 2015.

Profile profile

Global Security Division, Policy Studies Department

Researcher

Yu Harada

Field of Study: Maritime Security, Cyber Security

Planning and Coordination Office, The National Institute for Defense Studies

Telephone: 03-3713-5912 Fax: 03-3713-6149

E-mail: nidsnews@inds.go.jp Website: http://www.nids.go.jp