ORF ISSUE BRIEF

FEBRUARY 2014 ISSUE BRIEF # 68

The UN and Cyberspace Governance

Rahul Prakash and Darshana M. Baruah

Introduction

Cyberspace and its various networks including the Internet have become central to several economies, businesses and militaries. According to Internet World Stats[1], there are nearly 2.5 billion people using the Internet across the globe today. While this unprecedented connectivity has provided numerous opportunities for individuals, businesses and governments to benefit from, elements threatening its stability are also increasing. Threats such as Distributed Denial of Service Attacks (DDoS) and malware, among others, are attempting to erode the trust that billions have put in these networks. While criminals and groups with malicious intent are spearheading this attempt, state or state-sponsored actions to disrupt these networks are also being identified as a potential danger. At the same time certain nations have felt that the free flow of information, considered to be the primary reason for the Internet's success, could disturb societal peace and harmony. Even though governments have attempted to address these issues by creating national-level mechanisms, the very transnational nature of cyberspace has forced the international community to debate and form norms or rules that should promote good behaviour in cyberspace. As in the real world, there are varying and sometimes opposing views held by nations when it comes to governing cyberspace.

The United Nations (UN) has been working for over a decade to eliminate these differences and create a mechanism to ensure the security and stability of cyberspace. The UN First Committee on Disarmament and International Security which deals with disarmament, global challenges and threats to peace has been discussing the issue of information security since 1998, when the Russian Federation introduced a draft resolution on "Developments in the field of information and telecommunications in the context of international security" in the General Assembly (GA). Since then, member nations have been submitting reports about their thoughts on information security to the UN Secretary General. The initial period was dull without much movement within the UN towards dealing with issues in cyberspace. However, mounting reports of disruptions and the

increasing potential of cyber attacks disturbing the peace in the real world led countries to examine these challenges more seriously within the UN. More substantial work began at the UN when it constituted a Group of Governmental Experts (GGE) in 2004 to "examine the existing and potential threats from the cyber-sphere and possible cooperative measures to address them".[2] Since then there have been three GGEs set up by the UN, gaining significant ground.

As witnessed during many other efforts by the UN to gain international consensus, the discussion on information security too has suffered due to geopolitical differences between major powers. Largely, the international community is divided into two groups–the West led by the US on one side and Russia and China on the other side. The West has supported the free flowing nature and functioning of the Internet whereas Russia and China are seeking a role for governments in controlling the information flow on the Internet–multistakeholderism versus multilateralism. Secondly, there is a divide when it comes to the primary challenges that the UN discussions are trying to address. While the US and the West seek to contain economic espionage and criminal activity in cyberspace, Moscow and Beijing are looking at broader rules that would restrict a State's ability to use cyberspace for offensive purposes. Moreover, Russia and China are seeking to formalise an international treaty to govern cyberspace– opposed by the US and other Western countries.

The First GGE

In 2003, Russia proposed "the establishment of the Group of Governmental Experts (GGE) on information security".[3] In its report to the UN Secretary General, Russia stated that the establishment of the GGE "will move international, multilateral discussion of this matter to a qualitatively new phase. The group will give the international community a unique opportunity to examine the entire range of issues involved".[4] The first GGE was convened in 2004 but due to disagreements within the 15-member expert group, no consensus was reached on the final report.[5]

The disagreement within the group was primarily over two issues. "The first issue was the question of the impact of developments in information and communications technologies (ICTs) on national security and military affairs".[6] The group could not agree upon the inclusion of "new threats posed by State exploitation of ICTs for military and national security purposes". Secondly, the group could not agree on whether the discussions should focus on "information content or information infrastructures". There were also significantly different opinions put forward by member states regarding the control of trans-border information content by States as a matter of national security.

Opposing calls for state control over information, Washington argued that "implicit in these proposals would be the extension to governments of the right to approve or ban information transmitted into national territory from outside its borders should it be deemed disruptive politically, socially or culturally".[7] The US apprehensions stemmed from concerns that authoritarian regimes would attempt to control the free flow of information using such a mechanism and restrict freedom of speech and expression. With respect to military applications of information technology,

Washington was of the view that "the law of the armed conflict and its principles of necessity, proportionality and limitation of collateral damage already govern the use of such technologies".[8]

Even after the failure of the first GGE to reach a consensus, Russia continued to push for international cooperation through the GGE and drafted a second resolution in 2005. The resolution was adopted by a vote of 163 to 1.[9] The US was the only country to vote against it and it maintained its stance till 2009. By 2006, Russia was no longer the lone sponsor for the resolution. It was co-sponsored by China, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Myanmar, Tajikistan and Uzbekistan. The sponsors also requested the UN GA to establish the second GGE in 2009 "to continue to study existing and potential threats in the sphere of information security".[10]

Changing Threat Perception

By the time of the second GGE in 2009-2010, there were significant events and developments which could have become drivers for increasing willingness in governments to cooperate on cyberspace. Estonia faced a barrage of coordinated cyber attacks in April-May of 2007, the first of a kind, crippling government websites and halting internet banking. Estonia accused Russia of the cyber attacks due to its conflict with Moscow over the removal of the 'Bronze Soldier' Soviet war memorial in central Tallinn. The attacks, which initially started as a nuisance to disrupt daily operations went on to cripple the State's cyber infrastructure including the banking sector for about a week. It also disrupted the functioning of news organisations and other communication services, which made updating the citizens about the situation a challenge. The incident highlighted that a disruption in communication between the government and its citizens using cyberspace, can severely impact governance and basic utility services infrastructure, leading to chaos and confusion. These attacks were taken very seriously by the western alliance as the North Atlantic Treaty Organisation (NATO) stepped up immediately to help Estonia strengthen its electronic defence.[11] Soon after, the 2008 cyber attack on Georgia, coinciding with the Russian military advance into the country, established the application of cyberspace at the time of a military conflict. In both the cases Russia denied any involvement.

The cyber attacks on Estonia and Georgia demonstrated the extent to which cyberspace can be used against a State. It established the role of cyberspace in the military domain beyond the conventional use of such technologies to assist communication, command and control. These incidents also brought up challenges such as accurately identifying the aggressor in such a scenario, given the possibility of use of a third party's information systems to mount an attack. Although today experts believe that attribution is not technologically a severe limitation, the question remains as to what sort of response a State could resort to in such a situation.

Second GGE

In the backdrop of these events, the second GGE was convened in November 2009 and consequently held four meetings before coming out with a report in 2010.[12] The report outlined the following recommendations for the international community to consider:

- Dialogue on norms for State use of information and communications technologies (ICTs),to reduce risk and protect critical infrastructures;
- Confidence-building and risk reduction measures, including discussion of ICTs in conflict;
- Information exchanges on national legislation and national ICT security strategies, policies and technologies;
- Capacity-building in less developed countries; the elaboration of common terms and definitions on Information Security

Although divided on their respective concerns over information security, a draft resolution was adopted once again at the 65th GA session (2010), but this time without a vote and no opposition from the US.[13] This shift in US policy which came after Obama took charge at the White House was possibly due to the new developments in the cyber domain. Along with the incidents in Georgia and Estonia, the West, particularly the US, was concerned by the increasing cases of cyber espionage against its government and industry. There were signs that Washington was willing to engage with other States to address the concerns it had over issues in cyberspace. Its support of the UN resolution of 2009 (co-sponsored with Russia) as well as the successful completion of the second GGE were signs indicating this change.

International Code of Conduct

In 2011 China, Russia, Tajikistan and Uzbekistan submitted a letter to the UN Secretary General requesting him to distribute the International Code of Conduct for Information Security drafted by them as a formal document of the 66th session of GA. The International Code of Conduct (CoC) was a step forward taken by Russia and China to regulate cyber norms and governance. Explaining the CoC, Beijing stated that:

> "The International Code of Conduct for Information Security raises a series of basic principles of maintaining information and network security which cover the political, military, economic, social, cultural, technical and other aspects. The principles stipulate that countries shall not use such information and telecom technologies as the network to conduct hostile behaviors and acts of aggression or to threaten international peace and security and stress that countries have the rights and obligations to protect their information and cyberspace as well as key information and network infrastructure from threats, interference and sabotage attacks".[14]

CoC reflected the major concerns of these countries regarding the use of information as a weapon and the potential hostile use of cyberspace by a state. The Code restricted its signatories from using "ICTs including networks to carry out hostile activities or acts of aggression and pose threats to international peace and security. Not to proliferate information weapons and related technologies".[15] Going against the western stance on the issue, the Code contained clauses that legitimised state control over the Internet. The Code suggested "that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues".[16] Additionally, calling for a change in the current Internet

governance structures, the Code also suggested creating a multilateral mechanism to manage the Internet. Clauses curbing "dissemination of information which incites terrorism, secessionism, extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment"[17] were also seen as a way to restrict freedom of expression and speech by many nations in the West.

The Code, due to its contesting views with the West on cyberspace, received little support. In response to CoC, Washington issued a statement saying:

> "...the introduction of a draft Code of Conduct for Information Security presented an alternative view that seeks to establish international justification for government control over Internet resources. At its heart, it calls for multilateral governance of the Internet that would replace the multistakeholder approach, where all users have a voice, with top-down control and regulation by states. It would legitimize the view that the right to freedom of expression can be limited by national laws and cultural proclivities, thereby undermining that right as described in the Universal Declaration on Human Rights."[18]

Reiterating its principle opposition to creating a new treaty to govern cyberspace to maintain peace and stability, Washington noted that,

> "...the draft Code appears to propose replacing existing international law that governs uses of force and relations among states in armed conflict with new, unclear, and ill-defined rules and concepts. Indeed, one of the primary sponsors of the draft Code has stated repeatedly that long-standing provisions of international law, including elements of jus ad bellum and jus in bello that would provide a legal framework for the way that states could use force in cyberspace, have no applicability. This position is not justified in international law and risks creating instability by wrongly suggesting that the Internet is an ungoverned space to which existing law does not apply.[19]

Despite sharply opposing views, the UN adopted another resolution in 2011 which constituted a third GGE which was given the mandate to submit its report to the UN Secretary General in 2013.[20]

The Third GGE

GGE, which met thrice, starting in August 2012 and ending in June 2013, submitted its report to the UN Secretary General in June 2013. Taking the process forward, the third GGE made significant progress in agreeing on some of the defining aspects. For the first time, the GGE agreed on the applicability of international law to cyberspace. "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment",[21] stated the report. The group also suggested that "state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory".[22] However, the report cautioned that actions taken by States to address

security concerns in cyberspace should go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments.

Additionally, the report urges States to cooperate to contain the use of ICTs by criminals and networks. In this regard, it was suggested that legal approaches adopted by States should be harmonised and "practical collaboration between respective law enforcement and prosecutorial agencies"[23] should be strengthened. It also restricted States from using "proxies to commit internationally wrongful acts"[24] and encouraged States "to ensure that their territories are not used by non-State actors for unlawful use of ICTs".[25] With regard to creating voluntary confidence-building measures, GGE suggested that States should enhance sharing of information on ICT security incidents, promote exchange of information and communication between "national Computer Emergency Response Teams (CERTs) bilaterally, with CERT communities, and in other forums".[26]

Underlining the importance of the UN and the third GGE report, UN Secretary General Ban Ki-moon stated "the United Nations plays an important role in promoting dialogue among Member States on the issue of security in the use of ICTs and in further developing international cooperation in this field....[and the third GGE report provides] a sound basis for future efforts to enhance security and stability in the use of ICTs".[27]

Conclusion

While the international community still remains divided over the approach to govern cyberspace– notably a multilateral versus a multistakeholder approach, the process under the aegis of the UN has gained substantial ground. From the US opposing the information security resolution in 2005 to co-sponsoring the resolution with Russia in 2010, and the successful completion of the 3rd GGE report are indicators that the international community has realised the urgency in establishing some rules regarding behaviour in cyberspace. However, the outcome is the least common denominator and the report needs to be more ambitious.

Future GGE meetings are perhaps the likely forum to iron out the differences in international cyber governance. However, current trends also indicate a move towards a few possible plurilateral arrangements. One, the major powers namely the US, Russia and China could agree on rules or norms that would suit their interests. These rules could be an outcome of an agreement reached upon by these nations bilaterally or trilaterally. Today, the bilateral interactions between the three nations on the issue of cybersecurity have gained significant prominence. While the US and China have established a working group on cybersecurity, the US and Russia have signed an agreement on cyber security to reduce the threat of conflict in cyberspace and to communicate with each other regarding incidents of national security concern.

This 'G3'mechanism, which may be along the lines of conventional arms control regimes,can have implications on the rest of the international community. Without an alternative, the international

community may have to adhere to these rules. Despite the sharp differences and divergent interests of the three parties, such a scenario is possible. The Arms Trade Treaty is an example where alignment of interests of a few nations has led to the creation of a legally binding document accepted by most of the international community.

Second, due to these differences, countries may adopt a model where they increasingly isolate themselves by putting in domestic controls to restrict cyber activity beyond their shores. An example could be what China has done by building the great firewall of censors and barriers that restricts domestic Internet users from connecting to websites hosted abroad. This scenario, though, will come at the cost of the interconnectivity that the cyber revolution has provided and is likely to have severe economic impact on all parties.

Third, the so called swing states in the debate on multilateralism versus multistakeholderism – India and Brazil, could decide the fate of the discussion within the GGE. So far, these nations have adopted a position where while they support the free and unrestricted nature of Internet, they have increasingly supported some role for governments in international cyber and Internet governance, citing legitimate security concerns. These nations could be pursued by the existing blocs by offering a mechanism that would address their primary concerns. Also, the possibility of these nations providing a third alternative cannot be ruled out.

Moreover, there is a strong possibility that nations may cooperate regionally and arrive at certain mutually acceptable norms or rules. Forums such as BRICS (Brazil, Russia, India, China, South Africa) and the Shanghai Cooperation Organisation (SCO) could find relevance in this regard. The SCO nations signed an agreement in 2007 called the "SCO member countries action plan to safeguard international information security".[28] The agreement stated that the SCO nations will cooperate to deal with the increasing network and information security threats. BRICS, on the other hand,has instituted a mechanism to discuss the issue of cyber security during the BRICS National Security Advisors meetings.

In all likelihood, all three scenarios will coexist concurrently–an arrangement by the three prominent players, parallel efforts by the UN and a mediation role by the swing states. However, this will make cyber governance tedious and complex.

ABOUT THE AUTHORS

Rahul Prakash is a Junior Fellow at Observer Research Foundation. His research interests include technology and security, Chemical, Biological, Radiological and Nuclear (CBRN) issues and security developments in Asia. He has co-authored a report on *Chemical, Biological and Radiological Materials: An Analysis of Security Risks and Terrorist Threats in India,* an outcome of a joint study conducted by ORF and the London-based Royal United Services Institute.

Darshana M. Baruah is a Junior Fellow at Observer Research Foundation, New Delhi. Her research focuses on Cyber Security and Maritime Security in the Asia-Pacific.

Endnotes:

1. World Internet Usage and Population Statistics, Internet World Stats, June 30, 2012, available at http://www.internetworldstats.com/stats.htm.
2. Fact Sheet-Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations Office for Disarmament Affairs, available at: http://unoda-web.s3.amazonaws.com/wp-content/uploads/2013/06/Information_Security_Fact_Sheet.pdf

3. "Developments in the field of information and telecommunications in the context of international security", Report to the Secretary General, United Nations General Assembly, 58th Session, Addendum, A/58/373, September 17, 2003
4. Ibid.
5. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", Report to the Secretary General, United Nations General Assembly, 60th Session, Addendum, A/60/202, August 5, 2005
6. Fact Sheet - Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations Office for Disarmament Affairs, available at: http://unoda-web.s3.amazonaws.com/wp-content/uploads/2013/06/Information_Security_Fact_Sheet.pdf
7. "Developments in the field of information and telecommunications in the context of international security", Report to the Secretary General, United Nations General Assembly, 59th Session, Addendum, A/59/116/Add.1, December 28, 2004
8. Ibid.
9. "Developments in the field of information and telecommunications in the context of international security", Report to the First Committee, United Nations General Assembly, 60th Session, A/60/452, November 16, 2005
10. Developments in the field of information and telecommunications in the context of international security", Armenia, Belarus, China, Kazakhstan, Kyrgyzstan, Myanmar, Russian Federation, Tajikistan and Uzbekistan: draft resolution, United Nations General Assembly, 60th Session, A/C.1/61/L.35, October 11, 2006
11. Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, May 17, 2007
12. "Developments in the field of information and telecommunications in the context of international security", Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly, 65th Session, A/65/201, 2010
13. "Developments in the field of information and telecommunications in the context of international security", Report to the First Committee, United Nations General Assembly, 65th Session, A/65/405, November 9, 2010
14. China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations, Foreign Ministry of People's Republic of China, September 13, 2011.
15. China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations, Foreign Ministry of People's Republic of China, September 13, 2011.
16. Ibid
17. Ibid
18. Statement by Delegation of the United States of America, "Other Disarmament Issues and International Security Segment of Thematic Debate in the First Committee of the Sixty-seventh Session of the United Nations General Assembly", November 2, 2013. Available at: http://www.state.gov/t/avc/rls/200050.htm
19. Ibid
20. "Developments in the field of information and telecommunications in the context of international security", United Nations General Assembly, Resolution, A/RES/66/24, December 2, 2011
21. Report of the Group of Governmental Experts on Development in the Field of Information and Telecommunication in the Context of International Security, submitted to the UN General Assembly 68th Session, June 24, 2013, available at http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98
22. Ibid
23. Ibid
24. Ibid
25. Ibid
26. Ibid
27. Ibid
28. "ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG) Global Strategic Report", International Telecommunications Union, 2008, available at http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapt_1_iframe.htm.

Observer Research Foundation,
20, Rouse Avenue, New Delhi-110 002
Phone: +91-11-43520020 Fax: +91-11-43520003
www.orfonline.org email: orf@orfonline.org