Norms in Cyberspace: United Nations Group of Government Experts and Diplomatic Stasis

Ms Natallia Khanijo[@]

Introduction

There has been a seismic shift in technological advancement in the last few decades. The proliferation of cyber networks, and their resultant impact on Information and Communication technologies (ICT), has pervaded almost every aspect of human functioning. The recent shifts in ICT functioning and the emergence of increasingly interconnected cyber networks have reduced metaphorical distances across the globe and potentially changed the ways in which nation states conceptualise their role in an increasingly hyper capitalised, multicultural, global order. The current framework of legality and ethical norm enforcement – by its very essential emphasis on lived exchanges in real time – is ill-equipped to deal with the hyper reality of alternative spatial and temporal constructs of existence. There is a need, therefore, to construct alternative methodologies of applying available normative/regulatory frameworks onto cyber discourse. The construction of such a framework is linked to the need for "including increased predictability, trust and stability in the use of ICTs, hopefully steering states clear of possible conflict due to misunderstandings. Additionally, norms [can also be seen] as guiding principles for shaping domestic and foreign policy as well as a basis for forging international partnerships."[1]

To this effect, several global bodies have been constituted aimed at multilateral, multinational and multi-stakeholder based 'regulation' of cyberspace. These include the creation of transnational forums for diplomatic dialogue such as the United Nations Group of Governmental Experts (UN GGE), the International Telecommunications Union, the Internet Governance Forum, the Shanghai Corporation Organisation, the Tallinn Manual, etc. whose primary motive is the theorisation, collaboration and regulation of norms and laws concerning Cyberspace. Currently, at the international level, at least 19 global and regional organisations are actively involved in the security and governance of the cyberspace. One of these bodies is the UN GGE instituted to deliberate on the 'Developments in the Field of Information and Telecommunications in the context of International security'. The UN GGE had its latest meeting over the course of 2016-2017 but due to the inability to conclude with a consensus, the expert body has been unable to release a consolidated report regarding the application of International Law to cyberspace. The lack of concrete norm formation and regulatory security architecture for an interconnected cyberspace is difficult to envision due to the amorphous nature of the realm itself. The ease of access to cyber technology, and the versatile nature of emergent threats – 'Lone Wolf' terrorists, 'Black Hat' hackers, non-state actors, geopolitical rivalries – cumulatively remain at the edge of transgressing State thresholds and the creation of the GGE was aimed at navigating this terrain of militarised cyberspace and infringement retaliation. This article attempts to examine the functioning of norms in cyberspace, the UN GGE as a process and specifically India's functioning with respect to the GGE, the reasons for its failure and what might potentially lie ahead.

Norm Cycles and the UN GGE

The creation of a Norm Cycle for Cyber Discourse is primarily overseen by the United Nations. The debate concerning the emergence of ICTs and their impact on State sovereignty had first been introduced in the UN General Assembly (UNGA) regarding the field of Information and Telecommunication. As Roxanne Radu states, “In what concerns security in the cyberspace, three resolutions have been on the agenda. The First Committee of the UNGA discussed the resolution on ‘Developments in the field of information and telecommunications in the context of international security’ on a yearly basis starting in 1998; the Second Committee of UNGA discussed the ‘Creation of a global culture of cybersecurity and the protection of critical information infrastructures’, introduced in 2002 and adopted in 2005, and ‘Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical informational infrastructures’, adopted in 2010".[2]

Two key bodies that have been linked to the creation of a Norm Framework have been the UN established Group of Governmental Experts which has served as the theorising body debating the modalities involved in the establishment of a Norm framework; and the International Telecommunications Union that is primarily concerned with the implementation of Norm Frameworks. The GGE emerged as a result of Russia’s first proposition in 1998, regarding the establishment of a Group of Governmental Experts, who could examine the issue of Information Security. The General Assembly passed a resolution in 2002 concerning the “Creation of a Global Culture of Security”,[3] and it outlined nine important elements that needed to be followed before engaging in the process of norm emergence. These elements are “awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management and reassessment.”[4] Furthermore, the Assembly also outlined the need for a resolution that determined the elements aimed at protecting ‘Critical Infrastructure’. In its 11-point recommendation list, (that included Confidence Building Measures (CBMs), emergency/crisis communication networks, training exercises etc.), the assembly’s resolution extrapolated on a lot of concerns that would form the basis of the various forums examining Cyber Discourse over the years.

Iterations of the UN GGE

There have been five iterations of the UN GGE thus far. These have taken place in 2004, 2009, 2011, 2013 and 2016-2017 respectively. India has been involved with every single one except for the 2013 version. The first GGE was set up in 2004 by the First Committee[5] of the United Nations, however given the drastically divergent perspectives,[6] a consensus regarding the need for a normative framework could not be reached. The report concluded by saying that “given the complexity of the issues involved, no consensus was reached on the preparation of a final report.”[7]

The second GGE was held in 2009 and there was a shift in global perception following the distributed denial of service (DDoS) attack on Estonia in 2007. While the constituent members were the same, there was a drastic change in the power discourse. The US stance regarding Cyber Discourse had altered in the interim and there was finally a consensus of sorts surrounding the need for a Cyber Security Architecture. The 2010 report concerning the proceedings, codified and extrapolated on a lot of the basic elements aimed at securing cyberspace. These measures included the need to identify malicious actors/victims/vulnerabilities and threats. The report concluded with five recommendations, namely :-[8]

(a) State Dialogue

(b) Implementing CBMs

(c) Information Exchange

(d) Capacity Building

(e) Clarification of Terminology describing Cyberspace

The third GGE took place between 2012-2013, with the intent to carry forward the discussion that began with the 2009 GGE and its 2010 report. The mandate for this third iteration was the need to examine potential threats in the realm of information security and collaborate on cooperative mechanisms to address the dangers of 'transnational anarchy'. The Group submitted its report in June 2013, wherein it made several recommendations and continued with the five-point agenda. Two major points that emerged were:-

(a) Application of International Law to Cyberspace. A breakthrough recommendation, this was one of the first concrete steps towards the establishment of a security architecture dealing with Cyberspace.

(b) Maintenance of human rights and fundamental freedoms.[9]

The fourth iteration of the GGE that took place in 2013 increased the membership from 15-20 states. The recommendations laid out by the Group followed the pattern of the previous two GGEs of creating a peaceful ICT environment through the establishment of secure sustainable architectures, protecting ICTs from National Security Adviser (NSA) intervention, implementing CBMs, etc.[10] Further the group also observed:-

(a) A need to follow international law while also recognising the State's right to take measures to secure its critical infrastructure keeping in mind four legal principles, i.e. humanity, necessity, proportionality and distinction.

(b) The question of attribution of blame and sustainability of evidence was also raised given the amorphous nature of cyber crime. The group noted that mere geographical indicators of State infrastructure being used to perpetrate malicious activities might be insufficient evidence as the State might be a victim as well. The need for substantiation to avoid wrongful condemnation on circumstantial evidence was also raised.

The GGE was working towards the establishment of a normative framework that could capitalise on mechanisms that were already in place in order to regulate inter and intra-state cyber behaviour to prevent the escalation of conflicts. As Roigas and Osula state "The text clarifies that the UN GGE is seeking 'voluntary, non-binding norms for responsible State behavior' that 'can reduce risks to international peace, security and stability"[11] The question that emerges therefore, is what went wrong? And, why did the GGE devolve into its erstwhile state of fragmented partisan politics?

The 2016 GGE

The 2016 GGE was purported to deal with the impasse of norm applicability, multi-stakeholderism, legality and the militarisation of cyberspace. It was "tasked by the UN General Assembly with the study *of existing and potential threats in the sphere of information security and measures to address them, including norms, rules, and principles of responsible behaviour of states, confidence-building measures, and capacity-building."*[12]

While the earlier reports merely took note of the GGE proceedings, the 2015 report called upon Member States to follow the recommendations in their use of ICTs. Furthermore, while debating future topics of research and reference, the group also stated that "The United Nations Institute for Disarmament Research, which serves all Member States, is one such entity that could be requested to undertake relevant studies, as could other relevant think tanks and research organisations." [13] *What needs to be noted is the fundamental ideological disjunct between the United States and its allies on the one hand and Russia and China on the other regarding the creation of a cyber normative discourse. The former were primarily keen on setting up principles to form a structure that would streamline the implementation of International Law of Cyberspace – including but not limited to the Laws of Armed Conflict and International Humanitarian Law which would inevitably lead to a kind of militarisation of cyberspace. Russia and China on the other hand, were more interested in protecting State sovereignty and autonomy. The nail in the coffin for the expert body, interestingly, came from the Cuban representative who stated that "it would legitimise a scenario of war and military action in the context of ICTs."*[14] *The US representative proceeded to claim that this wasn't true and that such a stasis would undo the groundwork of consensus formation that had been formed thus far, but the lack of a consensus and consequently a resolution meant that the body was unable to come up with a concrete report regarding the navigation of cybernetic terrain and fell back onto the earlier impasse regarding problems of attributability, minimum credible force, and military retaliation. The key disagreement revolved around the question of self defence in cyberspace and the applicability of legal frameworks regarding the same. While the previous iterations had approved of the applicability of International Law of Cyberspace, "the right to self-defence as enshrined in Article 51 had been a source of heated debates in all of the sessions leading to their adoption."*[15]

India and the GGE

India has been a member of all the GGEs barring the 2013 one. India has played an important role in facilitating cooperation and bridging the divide between polar ideological stances – particularly so in the 2011 GGE. Furthermore, "India has also acknowledged the seminal 2015 GGE report, with its cyber norms being endorsed in the India-US Cyber 'Fact Sheet' that was released during Prime Minister Narendra Modi's visit to Washington DC".[16] *The question of access and inclusion are constantly raised with regard to the GGE given the discourse of power that emerges out of the tension between information rich and information poor nations. The politics and intersections of inclusivity in norm formation processes need to be examined in more detail given the fact that ICTs in particular are not just individual tools of state functioning but indispensable global architectures with interstitial, multi-pronged consequences. Being a part of the 2016 GGE was seen as an opportunity for India to navigate the politically complex terrain between developed and developing countries, and demonstrate its commitment to the creation of a peaceful, non-intrusive, collaborative ICT architecture. Even though several theorists believe that this would be the last GGE.*

GGE Limitations

The 2016-17 GGE might possibly be the last meeting of the group, and it was primarily constituted on Russia’s insistence. Over the years, the GGE has certainly made certain important changes in the discourse surrounding cyberspace and ICT usage, but it needs to be noted that “cyber-space is a singularly complex setting within which to understand and try to shape norms. The problem is not simply the nature of cyberspace, (although, acknowledging the unique characteristics of cyberspace is crucial when exploring norms in this realm). Rather, the challenge lies in the often over-looked nature of norms themselves *and how their defining features render them especially difficult to decipher – and, by extension, to attempt to design – in the context of cyberspace.”*[17] *While the lack of consensus regarding cybernorm formation is disappointing, it cannot be considered a surprise given the variant constructions of sovereign ICT frameworks that differ from State to State. The Cuban representative raised a valid point with respect to negotiating/implementing a norm framework in cyberspace when there was such a drastic imbalance of power among the constituent countries. While cyberspace cannot be conflated with geopolitical complexities, it cannot be divested from them either. It is precariously balanced on the cusp of traditional warfare and even manifests in espionage, low grade phishing attacks and other such information warfare tactics.*

There are several key issues that emerge in the aftermath of the proceedings that are worth examining. Firstly, one major limitation of the GGE is the lack of inclusivity in its constituent body. While increased inclusivity is considered a problem given the statistical certainty that the larger the base of the group, the harder it might be to broker a unanimous agreement on practicable issues. The exclusivity paradigm of geographical rotation is not really an acceptable alternative either. The current discourse regarding cyberspace, norm formation and ICT security architectures, stem from a predominantly western discourse which is tremendously problematic given that these legislative frameworks affect everyone in a globally interconnected world. Furthermore, the problem of inclusivity is twofold. Not only is there a problem with the horizontal axis of cyber discourse – wherein the academic predominance of the West stems from an inherent advantage in terms of access and technological superiority; but there is also a problem with the vertical axis of cyber norm formation wherein any constitutive body needs better representation at the level of the individual, private stakeholder and the country.

A legislative framework that might potentially constitute global norms with far reaching effects needs adequate representation from all stakeholders involved for the sake of ensuring that every single concern is engaged with. The need for a more inclusive set of discussants as well as the need for multi-stakeholderism in an increasingly globalised world order is something that needs to be considered. There are several other bodies, treaties and groups attempting to pursue research in cyberspace and affect a secure architecture. Some key bodies are the International Telecommunications Union, the Internet Governance Forum, the International Committee of the Red Cross, the Shanghai Corporation Organisation, the United Nations Institute for Disarmament Research, etc.

It would be foolish to assume that geopolitical frameworks would not colour a country’s approach to the implementation of cyber frameworks. As the Cuban representatives point out “an endorsement of the ‘right to self-defense’ [would] undermine asymmetric advantages which States that do not enjoy conventional superiority over their adversaries may have in cyberspace. So, Russia, which may be concerned that the United States will retaliate conventionally in response to a cyber operation that it *deems to be an armed attack, would have concerns about including the phrase. On the other hand, India, which would want the option to respond to Pakistan's cyber operations through conventional means, may welcome the express affirmation of a right to self-defense."*[18] *This bias is intrinsically tied to complicated issues of deterrence in cyberspace and the establishment of retaliatory thresholds that vary from one geopolitical situation to the other. The variability of contexts, the subjectivity of thresholds and the anonymous/amorphous nature of the threat all collusively point towards a volatile and unstable geopolitical scenario which could become a hotbed for escalatory conflict on the basis of a country's interpretive retaliatory action. These scenarios do not even take into account the question of rogue states and non-state actors all of whom would lie outside the purview of global norm formation but possess the power to destabilise any fragile consensus that might be established.*

The major issue of attrition and culpability remain unresolved as there is no established definitive understanding of the key terms of cyber norm formation. While there are theories of cyber deterrence, variant definitions of threats/actors, there is no consensus regarding mechanisms of attrition or investigative mechanisms that can be employed in these scenarios. Furthermore, as mentioned earlier, given the ease of access to cyber technology, and the relative ease with which attacks can be carried out and blame misdirected, there needs to be a concrete system in place that can deal with such dangerous liabilities without infringing on personal rights.

Keeping all these factors in mind, it's not surprising that the UN GGE reached such an impasse. The various other international bodies that exist need to collaborate towards addressing the key insecurities that permeate the amorphous fabric of cyberspace and contextualise threats in a systematic manner that is inclusive, equitable, consensus driven and maintains global peace.

Conclusion

Totalitarian frameworks would be ill-equipped towards dealing with cybernetic transgressions and current legal architecture cannot just be placed onto cyberspace without modification and engagement. There is a need to reconfigure our epistemological frameworks to create a new sociological and geopolitical theory of knowledge regarding cyberspace and then work towards the implementation of particularised norms, tailored towards the specific contours of cyberthreats and cybernorms. There are several institutions and research organisations that attempt to do so such as the Tallinn Manual, that "address two subjects – the *jus ad bellum,* which regulates the use of force by States, and the *jus in bello,* the law that governs how States may conduct their military operations during an armed conflict and provide protection for various specified persons, objects, and activities."[19] While the Manual is not a legal document that is enforceable, it nevertheless provides an overview of potential ways in which Legal frameworks can be collated with cyber architecture. Compiled by lawyers and academics, the Manual provides a welcome first step towards engagement with the issue, but the levels and layers of inclusivity remain limited. True engagement with the complications of cyberspace would require re-engagement with the geopolitics that drives it as well. One cannot theorise the construction of cybernorm formation without examining the geopolitical realities within which it exists. Furthermore, given the rapid pace of technological proliferation, and the increasing vulnerabilities that are being capitalised on by rogue actors – such as the Wannacry ransomware attack and the Petya attack - it is absolutely essential that earnest measures towards cyber collaboration begin as soon as possible to prevent the devolution of the geostrategic world order into an apocalyptic cyber wasteland.

Endnotes

[1] Osula, Anna-Maria, O. Rõigas, *International Cyber Norms Legal, Policy & Industry Perspectives.* CCDCOE, NATO CCDCOE Publications, Tallinn 2016.

[2] Radu, Roxanne, Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace. In J.-F. Kremer, & B. Muller, *Cyberspace and International Relations,* Berlin: Springer, 2016.

[3] Resolution - 57/239 Creation of a global culture of security, adopted by the General Assembly, 2002, Available at https://www.oecd.org/sti/ieconomy/UN-security-resolution.pdf, Accessed on 06 Sep 2017

[4] *Radu, Roxanne, Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace. In JF Kremer, & B Muller,* Cyberspace and International Relations, *Berlin: Springer, 2016.*

[5] Disarmament and International Security.

[6] Russia and China disagreed with the United States' ideas as they believed those ideas would lead to the militarisation of Cyberspace.

[7] *Report of the Secretary General, United Nations, Submitted by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 05 Aug 2005, Available online at https://disarmament-library.un.org/, Accessed on 09 Sep 2017.*

[8] Report of the Secretary General, United Nations, 30 Jul 2010, Available online at http://www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf

[9] *As set forth in the Universal Declaration of Human Rights and other international instruments.*

[10] Ibid.

[11] Osula, Anna-Maria, O Rõigas, *International Cyber Norms Legal, Policy & Industry Perspectives.* CCDCOE, NATO CCDCOE Publications, Tallinn 2016.

[12] Korzak, E (2017). *UN GGE on Cybersecurity: End of an Era.* Available at The Diplomat: http://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ Accessed on 10 Sep 2017.

[13] Report of the Secretary General, United Nations, 22 Jul 2015. Available online at http://www.un.org/ga/search/view_doc.asp? symbol=A/70/174&referer=http://giplatform.org/actors/united-nations-group-governmental-experts-developments-field-information-and&Lang=E Accessed on 08 Sep 2017.

[14] *Korzak, E (2017).* UN GGE on Cybersecurity: End of an Era. *Available at The Diplomat: http://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ Accessed on 10 Sep 2017.*

[15] Michael N Schmitt, Vihul Liis, (Ed.), *Tallinn Manual 2.0 on the International Law applicable to Cyber operations,* Cambridge University Press, (2017)

[16] Sukumar, UN Reconstitutes its Top Cyber Body, This Time with India at the High Table, 2016, Available at The Wire: https://thewire.in/44696/un-reconstitutes-its-top-cyber-body-this-time-with-india-at-the-high-table/ Accessed on 09 Sep 2017.

[17] *Osula, Anna-Maria, O Rõigas,* International Cyber Norms Legal, Policy & Industry Perspectives. *CCDCOE, NATO CCDCOE Publications, Tallinn 2016.*

[18] Sukumar, A M, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?* 2017, Available at Lawfare: https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well Accessed on 08 Sep 2017.

[19] Michael N Schmitt, Vihul Liis, (Ed.), *Tallinn Manual 2.0 on the International Law applicable to Cyber operations,* Cambridge University Press, (2017).

@**Ms Natallia Khanijo** has done her graduation from Lady Sri Ram College and post-graduation from Miranda House, University of Delhi. Currently, she is researching on 'Cyber Issues' in Institute of Defence Studies and Analyses (IDSA), Delhi.

Journal of the United Service Institution of India, Vol. CXLVII, No. 609, July-September 2017.