INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

IDSA

Issue Brief

Destination India for Global Conference on Cyberspace 2017

Cherian Samuel

January 18, 2017

Summary

The moribund London Process has acquired a fresh lease of life with India taking on the mantle of holding the next iteration of the Global Conference on Cyberspace (GCCS), after the original hosts expressed their inability to hold the conference. The 2017 Conference also comes at a time of increased turbulence in global affairs which can also have an impact on collaboration in securing cyberspace, and increasing threats from a variety of threat actors ranging from state-sponsored actors, to criminal syndicates, to hactivists. As the previous editions have shown, the host country has a unique opportunity to shape the global conversation on cyberspace, provided the necessary groundwork is done.

The moribund London Process has acquired a fresh lease of life with India taking on the mantle of holding the next iteration of the Global Conference on Cyberspace (GCCS), after the original host, Mexico, expressed its inability to hold the conference. The conference is expected to take place in November 2017. This would be the fifth in the series, following conferences in London (2011), Budapest (2012), Seoul (2013) and The Hague (2015).

Earlier Iterations

The London Process began as a conference on cyberspace hosted by the British Foreign Office following a proposal by the country's Foreign Secretary William Hague at the Munich Security conference in 2011 for an international meeting to discuss "rules of the road" in cyberspace. This was in response to efforts by Russia and China to develop an alternative model for cyberspace governance that stressed on national sovereignty in cyberspace and which had culminated in the tabling of an "International Code of Conduct for Information Security" at the United Nations in 2011 by China, the Russian Federation, Tajikistan and Uzbekistan. The narrative put forward by the London Process emphasised a cyberspace that was "open, global, safe and secure", the specifics of which were to be developed through consensus on various principles and norms amongst the various stakeholders. In his opening statement, the architect of the Conference, William Hague identified the objectives of the conference thus: "We want to widen the pool of nations and cyberusers that agree with us about the need for norms of behaviour, and who want to seek a future cyberspace based on opportunity, freedom, innovation, human rights and partnership, between government, civil society and the private sector."[1] Accordingly, the themes of the conference were Economic growth and development, Social benefits, Safe and reliable access, International security, and Cyber crime.

The Budapest Conference in the following year saw European countries highlighting the human rights aspects of cybersecurity, based on their characterisation of internet freedom as a fundamental right. That drew an acerbic reaction from China, with the Chinese representative asking whether he was at a human rights conference or a cybersecurity conference. In his speech at the conference, the Chinese representative reiterated the principle of "network sovereignty" and highlighted the need to balance the free flow of information against the potential for threats to national security and social order. He also called for equal rights in managing the Internet and equitable distribution of the critical resources of the Internet. However, the British continued with their stewardship of what was now becoming known as the London Process by announcing the establishment of a Centre for Cyber-Security Capacity Building at a cost of two million Great British pounds.

[1] London hosts cyberspace security conference," *BBC*, 1 November 2011, www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement

The Korean iteration was meticulously conducted in 2013, with the hosts preparing a statement before the Conference and which was subsequently discussed and agreed to by the participants, making it more outcome oriented and easier to manage. The "Seoul Framework for and Commitment to an Open and Secure Cyberspace" added a sixth theme, "Capacity Building" to the existing five. This presumably followed on from the 2013 Report of the UN Group of Governmental Experts (UNGGE), which also highlighted capacity building. The Conference themes also seemed increasingly aligned with the US International Strategy on Cyberspace, the US State Department's 2011 blueprint on how it intended to approach and promote its vision for cyberspace internationally.

While cast in the multi-stakeholder mode, there was an increasing tilt towards state participation, with both the Budapest and Seoul Conferences being criticised for being too state centric as well as being dominated by Western countries, with little participation from the developing world. Although the Seoul Conference in 2013 had as many as 43 participants at the official Ministerial level, the Snowden revelations took off much of the sheen of the Seoul Conference and detracted from the main objectives of gaining consensus on contentious issues.

The Dutch Model

The process itself seemed to have begun to lose steam when it was announced that the next Conference would take place only after two years and be hosted by the Netherlands. In the intervening two years, the Dutch government expended a considerable amount of energy and resources on shaping an agenda and gathering support for a successful outcome. The Conference was conceived as the culmination of a two-year long process of consultation, both on regional and functional lines, rather than as a one-off event. The stumbling blocks of low multi-stakeholder participation and low participation from the developing world were sought to be mitigated through support for a series of regional conferences to provide inputs to the larger summit with no less than 13 preparatory events being held in different parts of the world on varied issues related to cyberspace. Other governments supporting these events included Switzerland, South Korea, the United Kingdom, and Germany. The Dutch budgeted 15 million Euros (Rs.100 crores) for the conduct of the Conference, with their Foreign Affairs, Security & Justice, Economic Affairs, and Defence ministries being the joint organisers. Uri Rosenthal, a former Foreign Minister, was appointed as Special Envoy for the GCCS.

Civil society participation in the preparatory process and in the Summit was carried out by instituting a Global Advisory Board taking into account "availability, expertise, geographic and gender balance". Amongst other things, the Advisory Board recommended 110 civil society representatives, selected through an application process, to attend the Summit. Despite the attempts to include civil society participation, there was criticism that selection of the members of the Advisory Board etc. was done through an opaque process.

The declared purpose of the Summit was to move from abstract to practical discussion in order to find solutions. The key objectives were: 1) Support practical cooperation in cyberspace; 2) Promote capacity building and knowledge exchange in cyberspace; and, 3) Discuss norms for responsible behaviour in cyberspace.

The various sessions of the Conference were centred on the main themes of freedom, growth and security. While some of the sessions were focused on exchange of ideas between the various sets of stakeholders and these sessions included representatives from government, the private sector, civil society and developing world representatives, other sessions focused on popularising and socialising certain norms such as those related to privacy or dual use restriction on cyber technologies. The latter were primarily composed of representatives from the developed world.

The conference operated at many levels, ranging from Track 1 level bilateral discussions to sessions at the Track 1.5 and Track 2 levels. As many as 21 countries sent representatives at the Ministerial level. On the other hand, Russia and China played a very low key role, with hardly any representation other than in-country diplomats or from neighbouring countries, though the Chinese did send delegations of academicians and domain experts. The majority of the participants, on the whole, were government officials from various countries. The outcome statement of the Conference was in the form of a Chairman's statement, which summarised the two days of discussion.

The Global Forum of Cyber Expertise (GFCE) was launched with much fanfare during the Conference. Its 42 members included 29 countries, seven private-sector entities, and six intergovernmental organizations. Though initially meant to be an adjunct to the Global Cyber Capacity Centre (GCCC) set up by the United Kingdom with a corpus of 200 million Great British pounds after the Budapest Conference, at some point, the Netherlands changed tack and made it a Dutch-led and Dutch-hosted initiative. The Dutch government also used this as an opportunity to showcase the prowess of its industry in the technical domain. While the actual Summit took place over one and a half days, the Hague Cyber Week was held at The Hague Cyber Delta.

India's Imperatives

India has been a participant in all the Conferences of the London Process, though it sent a diminished delegation to the Seoul Conference due to an unscheduled cabinet reshuffle. In his Ministerial address at the London conference, Sachin Pilot, Minister of State for Communications and Information Technology, called for global coordination on "on multiple fronts including setting standards, safeguarding digital intellectual property rights, sharing best practices, capacity building of developing countries, providing critical intelligence information, and establishing relevant security parameters."[2] *Inter alia*, he also noted that India had been calling for a discussion on "whether laws covering international armed conflict, such as those under the Geneva Convention can also cover cyber attacks." Pilot also delivered a key note address at the Budapest Conference the following year where he called for internet governance to be made more equitable and effective. At the 2015 Conference too, India sent a high-level delegation and joined the Global Forum of Cyber Expertise (GFCE) as one of the founder members.

While hosting the Conference provides a unique opportunity to direct and contribute to the global conversation on cyberspace, the time available is very limited in which to do the necessary groundwork. While the Netherlands had all of two years, we are already into the first month of 2017.

India's approach to the internet has hitherto been tech-centric and free of ideological overlays. Nonetheless, the announcement in June 2015 that India now officially supported the multistakeholder model was taken to mean that India had joined the US bandwagon, notwithstanding its nuanced interpretation of the multistakeholder model. India perceives a leading role for governments in cybersecurity in national security related issues.

This also brings up the issue of the nodal Ministry for the Conference which presumably is the Ministry for Electronics and Information Technology (MEITy). Given the major themes of the Conference, there would have to be close and sustained co-ordination between the Ministry and other nodal agencies, including the National Security Council Secretariat (NSCS) and the Ministry of External Affairs (MEA), to ensure a successful outcome. If India is to walk the talk on multi-stakeholderism, there would also have to be interactions with other stakeholders by the organising agencies. Unfortunately, there is a dearth of NGOs, civil society organisations and other "norm entrepreneurs" that the Netherlands used with great effect to expand the dialogue amongst the stakeholders.

The private sector, which has played a leading role in other countries in the process of formulating approaches on cyberspace, is not enthused about playing a similar role here, seeing very little returns on investment. Whilst civil society forms the third leg of the triad, there are comparatively few civil society organisations and NGOs that have the necessary expertise or focus on cyberspace. As a result, there has only been desultory participation from these two sectors in international gatherings, whether it be academic, industry, or governmental, and even less in the policy space. There was an attempt to have an Indian Internet Governance Conference in 2012 with all the stakeholders, but that proved to be a one-off event.

[2] Speech of Mr. Sachin Pilot, Minister of State for Communications and Information Technology at the London Conference on Cyberspace, *IDSA Task Force Report on India's Cybersecurity Challenge (*2012*)*, Appendix 3, p.66. http://www.idsa.in/book/IndiasCyberSecurityChallenges

Turbulence on the Global Stage

The 2017 Conference also comes at a time when the existing international discourses on securing cyberspace, whether it be the UNGGE process or the Internet Governance Forum (IGF), seem to be unable to cope with the accelerated developments in cyberspace. Increasingly, their utility is being called into question as they are unable to provide effective ideas on how to deal with the threats in cyberspace, whether they be state-sponsored, or from criminal actors, or hactivists. Recent cybersecurity events making headlines range from attempts at manipulating the outcome of the US Presidential elections to recurring data breaches worldwide and the attempted siphoning off of almost USD one billion from the Central Bank of Bangladesh. Whilst the UNGGE process was renewed again with an expanded membership, it has been criticised for being a multi-lateral process. Further, its success is also dependent on the largesse of participating governments. As for the IGF, its mandate was renewed by the United Nations General Assembly for a further ten years in 2015, but nothing was done to remediate problems of under-funding that have bedevilled it for much of its existence.[3]

Another set of factors to be considered, heading into the Conference, are the global headwinds that portend a potential change of course with the Trump administration taking office in the US . Early pointers indicate that the Trump Administration would be less amenable to follow the existing policies of the Obama Administration on cyberspace. There is even speculation that the so-called Big 3, Russia, China and the United States, might collectively decide to impose a cyber-security regime for “the greater good”.[4] While it remains unlikely that such an endeavour would succeed, Middle Powers such as Australia, the Netherlands, Singapore and Germany have been steadily pushing for an interdependent and collaborative framework in cybersecurity. Countries like Germany and Australia are simultaneously strengthening their offensive and defensive capacities.

On the flip side, despite the emphasis on human rights in previous editions of the Conference, which has been a red flag for authoritarian countries, many other countries are resetting their positions following the increased use of cyberspace for terrorism related activities, ranging from radicalisation to publicity to recruitment and resource mobilisation. This provides an opportunity for countries to overcome ideological differences and work on practical issues provided the necessary groundwork is done.

The various Conferences that have taken place under the aegis of the London Process are themselves models of the approach India could follow. While the London and Budapest Conferences took the shape of one-off events, the Seoul Conference was largely a state-led multilateral initiative, and the Hague Conference

[3] "Despite Renewal, the Internet Governance Forum Is Still on Life Support." *Council on Foreign Relations*. Council on Foreign Relations, 12 December 2016. http://blogs.cfr.org/cyber/2016/12/12/despite-renewal-the-internet-governance-forum-is-still-on-life-support/

[4] Belam, Martin. "We're Living through the First World Cyberwar – but Just Haven't Called It That." Guardian News and Media, 30 Dec. 2016. https://www.theguardian.com/commentisfree/2016/dec/30/first-world-cyberwar-historians

came closest to the Holy Grail of a multi-stakeholder Conference that was the crescendo of a two-year long effort on the part of the Dutch Government. While India might seek to do a repeat of the previous Conference, given the paucity of time, resources and the current turbulence in world affairs, it might well have to do with a conference of the Seoul variety. For a variation on the theme, there could be closer coordination with the previous host countries who would have acquired a certain amount of heft and credibility by virtue of having hosted the Conference. All these countries could conceivably work together to take the London Process forward by pooling their resources, expertise and points of contact.

Finally, the London Process is, no doubt, an important contributor to the global discussion on cyberspace, and occupies an important niche. Identifying a successor host country well in advance would also alleviate some of the uncertainty that has come to be associated with the Process and put it on firmer ground.

About the Authors

Cherian Samuel is Research Fellow at the Institute for Defence Studies & Analyses, New Delhi.

The Institute for Defence Studies and Analyses (IDSA) is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Disclaimer: Views expressed in IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the IDSA or the Government of India.

Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
contact.idsa@nic.in www.idsa.in
Twitter @IDSAIndia
www.facebook.com/InstituteforDefenceStudiesAnalyses