

Global Conference on Cyberspace 2015: Opportunity for India

 claws.in/1389/global-conference-on-cyberspace-2015-opportunity-for-india-surya-kiran-sharma.html

Cyber security has emerged as the primary focus area for defense and national security. As national resources and critical infrastructure are digitised using computers and information technology, cyberspace is the next big battlefield. Keeping in view the strategic importance of cyberspace, the Global Conference on Cyberspace (GCCS) 2015 was organised in The Hague, the Netherlands on 16 and 17 April 2015. The conference brought together representatives from various national governments, private sector and civil society organisations to discuss potential for cooperation, capacity building, and to find possible solutions for the threats emerging in cyberspace. The themes for the conference were:

- **Freedom** – There is a need to ensure freedom of speech and expression, and the right to privacy online, as is available to all individuals offline. The conference discussed the issues related to privacy protection and the role each stakeholder must play in this regard[i].
- **Growth** – Considering the growth in Internet and the challenges it poses for security and privacy, the conference sought to focus on the importance of preconditions for Internet driven economic growth and social development[ii].
- **Security** – With the increased dependence on information and communication technology, the security of cyberspace is paramount. Key issues in this regard include cyber security, cyber-crime, ethical hacking and capacity building[iii].

The outcome statement for the conference highlights the commitments made over the two days by various stakeholders. However, it fails to give out a concrete plan for achieving the targets and goals as set by the conference[iv]:

- Support practical cooperation in cyberspace
- Promote capacity building and knowledge exchange in cyberspace
- Discuss norms for responsible behavior in cyberspace

Deputy National Security Adviser, Dr Arvind Gupta, represented India at the conference and spoke in the session dedicated to international peace and security in cyberspace. India currently boasts of the third largest population of Internet users across the world, behind only China and the United States. As per data available for 2014, close to 20% of India's population uses the Internet[v]. India has thus far failed to take the initiative and incorporate the global efforts in cyber security into its domestic policies, reflected in how far we lag behind China in cyber domain.

Global Forum on Cyber Expertise

The GCCS 2015 marked the launch of the Global Forum on Cyber Expertise (GFCE), an expansive initiative to give political momentum to global cyber security efforts and capacity building. The Hague Declaration on the GFCE points that the forum “will be consistent with, complement and reinforce existing bilateral, multilateral, multi-party, regional and international efforts to build cyber capacity and expertise and avoid duplication and overlap. The efforts undertaken within the framework of the GFCE will be consistent with international law, in particular the Charter of the United Nations, and respect the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the UN Guiding Principles on Business and Human Rights, where appropriate.”[vi]

The GFCE aims to “provide a dedicated, informal platform for policymakers, practitioners and experts from different countries and regions.”[vii] India is amongst the 42 founding members of the GFCE, which includes governments, intergovernmental organizations and companies.[viii] It provides a grand opportunity for India to learn from the global experiences in cyber security, capacity building and developing strategic partnerships with other nations in cyberspace. Though the GFCE is voluntary and not legally binding, it provides a platform for India to learn the best practices in cyber domain around the world and to pick up its own cyber efforts from the present nascent stage.

Multi-stakeholder approach

The GCCS also discussed the multi-stakeholder model of Internet governance. The Internet Assigned Numbers Authority (IANA), operated by the Internet Corporation for Assigned Names and Numbers (ICANN), allocates and maintains unique codes and numbering systems that are used in the technical standards (“protocols”) that drive the Internet. It oversees the global use of domain names, number resources, and protocol assignments.[ix]

IANA functions as a non-profit American corporation governed by US laws and contracted to the United States Department of Commerce. However, the contract is set to expire in September 2015 with the US Department of Commerce declaring its intention to give up control over IANA and handing over the duties to an international multi-stakeholder group.[x] The GCCS recommended future mechanisms to recognise the respective roles of all stakeholders without giving out a path to follow. The various stakeholders involved are the civil society, technical community, businesses and governments across the world. India should take up an active role in the establishment of such a multi stakeholder forum to ensure adequate representation for the developing world, lest majority control is handed over to developed countries of Europe and the United States. A proactive stand on Internet issues is necessary to ensure a free, open and safe web without government intervention and regulation on content, as is found in Russia and China.

International peace and security

The conference also discussed the applicability of international law in cyberspace, particularly in light of the recent episodes of cyber-crime and cyber-attacks. The cyber-attack by North Korea on US company Sony Pictures highlighted the lack of international memorandum on the issue and the applicability of *jus in bello* and *jus ad bellum* in cyberspace. There is a greater need to define the principle of State sovereignty in cyberspace and developing norms to be followed during peacetime while preventing conflicts. The Tallinn Manual on the International Law Applicable to Cyber Warfare is a non-binding document launched in 2013 by the NATO Cooperative Cyber Defense Centre of Excellence, based in Tallinn, Estonia. The manual studies how international law applies to cyber conflicts and cyber warfare. The need of the hour is to create a binding framework to promote international cooperation, peace and security.

As the focus now shifts to the recommendations that the GCCS 2015 will come up with, cyberspace appears to have received inadequate attention in terms of capacity building, clarity of international law, applicability to State sovereignty, and a lack of a multi-stakeholder forum.
