



## Global Conference on Cyber Space (GCCS) 2017

*Dr. Chayanika Deka \**

### Introduction

The Global Conference on Cyber Space (GCCS) is an international event focussing on the issue of cyber space with an emphasis on the nature of threats and challenges faced by the larger cyber environment. The countries represented in the GCCS have collectively come together to design globally accepted universal rules in cyber space involving all stakeholders such as government, civil society and industry.

With an aim to ‘**promote an inclusive cyber space** and focus on policies for inclusivity, sustainability, security, freedom, **technology and partnerships** to uphold **digital democracy**, maximise collaboration for **strengthening security and safety** and **advocate dialogue for digital diplomacy**,’<sup>1</sup> the fifth edition of GCCS was held from November 23-24, 2017 in New Delhi. The event was inaugurated by Prime Minister Narendra Modi and attended by Prime Minister of Sri Lanka Ranil Wickremesinghe. There were delegates from 124 countries, including 33 Ministerial Delegates.

During the two-day conference, a total of four plenary sessions and 12 parallel sessions were held premised on the central theme, ‘*Cyber for All: A Secure and Inclusive Cyberspace for Sustainable Development.*’ The sub-themes of the four plenary sessions were (a) cyber for growth, (b) cyber for digital inclusion, (c) cyber for security, and (d) cyber for diplomacy.

Reflecting on India’s vision of digital empowerment, the momentum for the Conference was set by Prime Minister Narendra Modi’s speech that highlighted the inclusive nature of internet as well Indian achievements in the field of cyber space, including the India Government’s

efforts at embracing the human face of technology for making common man's life easy. However, the event was not limited to this aspect. There were several other issues, including use of internet by terrorist groups, diplomacy and international cooperation in cyber space and role of government as an enabler, that were addressed at the meeting.

## Objective

In the context of the fifth edition of the GCCS, this paper will discuss and analyse the major deliberations that took place during the event. The paper is divided into three sections. The **first section** will deal with the historical background of the GCCS that was first held in 2011 in London with 700 international delegates. This came to be known as the “**London Process**,” setting an example in the field of cyberspace.<sup>ii</sup> This was followed by the second conference in 2012 in Budapest with 700 delegates from 60 countries. The third and fourth conferences were held in 2013 (Seoul) and 2015 (Netherlands), respectively. While the third edition had 1600 participants, the fourth had representation from 100 countries with a total of 1800 delegates. All the four editions primarily addressed four main issues: Economic growth and development, social benefits, safe and reliable access, and international security and cyber crime. The fifth edition this year expanded its dimension to include the human face of technology, role of government as an enabler and the utility of cyber diplomacy. The increase in the number of representatives and countries as well as the expansion of the agenda shows that the GCCS has evolved significantly with each conference.

The **second section** will focus on the GCCS 2017, highlighting major developments in the field of cyber security. **Section three** of the paper is the conclusion.

## SECTION I

**Table 1 GCCS Meetings and Agenda**

Themes	2011	2012	2013	2015	2017
	London November 1-2	Budapest October 4-5	Seoul October 17-18	Hague April 16-17	Delhi November 23-24
Role of Government	Realization of countries to deal with cyber abuses with the help of civil society and industry across the world	Government recognition of ICT to accelerate development	Cooperation between government, industry and civil society	Involvement of all stakeholders i.e. government, industry and civil society	Development in the sector of ICT is a multi-stakeholder activity where government, private sector, industrial sector, NGS, technical experts, academia, everyone has a role to play. Involvement of ICT for policy formulation and implementation, addressed ICT as effective device 'for

					<p>realising the goal of Good Governance with Minimum Government'.<sup>iii</sup></p> <p>Called upon government to play a new role i.e. enabler and facilitator rather than be some kind of interference in digital world.</p> <p>The government should play the part of interface point between citizens and economic growth with the help of digital world, requiring modification in policy prescription of governments across the world</p>
Economic growth and development	Broadening of physical infrastructure and training, focus on training of youth in the development of ICT industry, promotion of competitive cyber market	Open and free cyberspace for social and economic progress and promotion of 'Access of broadband, regulatory framework, internet economy, infrastructure background such as role of education, issues of security and privacy, intellectual property rights, rise of social network and mobile communication, connection between security	Internet offers 'free flow of information, research, innovation, entrepreneurship and business transformation, to ensure the protection of personal information in the online environment and to empower consumers and users in online transactions and exchanges' <sup>3</sup>	Acknowledged the role of Internet in transforming the economy. Focus given on education, trust and appropriate policy framework for trade and innovation aiming at 'Internet access for all and cyber capacity building' <sup>vi</sup> .Implementation of open internet standards.	<p>Acknowledged the importance of cyber space in advancing economic growth of nations by offering newer scope for innovation and entrepreneurship.</p> <p>Highlighted evolution brought by Industry 4.0.In the future, growth in robotics, artificial intelligence, IoT, data analytics would alter structures of governance.</p> <p>The conference called for connecting traditional expertise with modern discipline of science and technology in the arena of cyber space to reach</p>

		and development, use of technology to empower marginalised group, endorsement of scientific education as an essential element of ICT infrastructure <sup>iv</sup> along with three priority areas as acknowledged by the World Bank i.e connectivity, innovation and transformation <sup>v</sup>			<p>out common people. Here, the role of governments across the world is commendable. Acknowledged the fact that nowadays governments deliver welfare services to citizens through digital platforms by creating digital infrastructure, digitally empowering masses, engaging m-Governance frameworks and increased participation of citizens. All these cater to the most marginalised communities as it said, “creation of digital points of presence: contact nodes at the last mile, which can deploy sustainable business and service models to engage citizen demand for financial inclusion, healthcare, education and more”<sup>vii</sup></p> <p>The inclusive nature of internet offering equal access and equal prospects directed rise of innovation, dependence of global economy on digital technology</p>
Social and cultural benefits	Internet should play a greater role in reaching out to marginalised sections of the community by improving	Worldwide internet connection promoting social and democratic reform, invitation to private sector to decide rules for cyber security, responsible internet	Protection of freedom of expression online. Recognition of cultural, linguistic, religious and traditional diversities of nations by the Internet.	Promotion of innovation and economic growth with respect to people’s privacy, commitment to protect human rights and security online.	<p>Promotion of freedom in cyber space within certain limits, privacy of users should be respected.</p> <p>Increased engagement of citizens is the heart of GCCS 2017. Free open and inclusive cyber space has provided an equal platform to citizens from</p>

	their access to education and health	providers in managing content, abolishing the debate between open behaviour of internet and state's restriction over internet.			all strata whether have or have not to seek 'knowledge, education and healthcare' <sup>viii</sup> .The world of cyber space offers variety of opportunities to differently-abled civilians to harness their talent and capacity.
Safe and reliable access	Secure and reliable cyber space without censorship, recognition of the role of Internet Corporation for Assigned Names and Numbers (ICANN) Internet Governance Forum, role of private sector and Computer Emergency Response Team(CERT) in maintaining single undivided network <sup>ix</sup>	Need for a comprehensive strategy for cyber space. One rule fits all cannot be initiated in cyber security and promotion of local culture and conditions, strengthening international cooperation and involvement of private sector in dealing with cyber space with sharing of knowledge and information	Development of cyber strategies by governments, industry and individual users in protecting cyber space and critical infrastructures, collaboration among nations to prevent cyber malpractices.	Multi-stakeholder approach for internet governance. Respect to Internet Governance Forum, appreciated the efforts of ICANN to global internet community	Open, free and flexible cyber space with greater representation of vulnerable sections like women and children. Promotion of principles of the charter of United Nations.
International security and cyber crime	International attempts to bridge the gap of digital dividend among nations, more internet connections	Acknowledgement of international laws, integration of developing world to reap benefits of internet. Central role of state along with important role	Recognition of cooperative measures in fighting cyber crimes.Application of international laws especially role of the United Nations especially UN charter and responsible	Focus on international cooperation and sharing of expertise and skills in cyber space, recognition of terrorists using internet, promotion of public-private partnership, capacity building initiatives, cooperation between state, business and NGOs to deal with	Threats posed by cyber space were discussed at GCCS 2017. Increased use of mobile phones and social media has brought newer challenges in the threat landscape of cyber space. Nation alone cannot control surge of cyber crimes in the era of

	<p>to developing nations, adherence of states to both international law and traditional security procedures, measures promoted by United Nations and other regional organisations, recognition of collective approach in tackling cyber crimes, support to the principles adopted at Budapest Convention on cyber crime, involvement of youth in international forum</p>	<p>played by international organisations and private sector. Public-private partnership to strengthen critical infrastructure and safeguard them from cyber threats</p> <p>Establishment of European Cybercrime Centre at the Europol</p>	<p>behaviour of states in addressing cyber challenges</p>	<p>cyber crime. Enactment of the Global Forum on Cyber Expertise (GFCE) strengthening cyber capacity and expertise</p>	<p>digital economy where government and organisations function through digital technology.</p> <p>There is greater focus on sharing of information and coordination between security agencies.<sup>x</sup></p> <p>Deployment of security techniques, inculcating values in cyber world, promotion of legal regime in cyber space, offering cyber expertise to create competent cyber experts</p> <p>The conference called for urgent cooperation among nations to counter ambiguous threats posed by internet. Need for an efficient monitoring apparatus to look after illegal activities in digital world and focus on 'strong cyber governance, trusted secured partnerships, trusted networks and advanced security technologies'<sup>xi</sup></p>
Cyber diplomacy					<p>Emergence of digital technology and digital economy suggested responsible behaviour and transnational cooperation on the part of states. Endorsement of <i>Digital Knowledge Sharing Platform</i><sup>xiii</sup> among nations</p>

The above table shows issues and agendas adopted at the Global Conferences on Cyber Space. GCCS acknowledged that technological advancement brought both opportunities and challenges with more focus on ever-evolving cyber threats. Amidst various types of cyber abuse such as data-encrypting ransomware, password phishing attacks, unpatched software, social media threats, advanced persistent threats, counter efforts by government institutions were not sufficient. Participation by non-state actors like civil society and industry were equally important in mitigating cyber threats which are transnational in nature. The conference strongly pointed out that the establishment of different sets of rules and regulations managed by individual states would lead to anarchy in the open nature of cyber space that thrived on creativity and talents of individual and private industries, therefore cyber space should not be subject to policing of online activity by the state authorities. The conference stressed on the need to build global cyber rules and regulations in internet space which is oceanic in nature and restricted national rights and jurisdiction over cyber space.

The Budapest Conference took a broader agenda in cyber security by discussing 'governance and internet with focus on relationship between internet rights and internet security'<sup>xiii</sup>. The conference attempted to find a proper balance in cyber space i.e. providing a democratic and open space in internet for its users, acknowledging their right to use and express online; and, setting up certain norms to protect internet users from cyber threats and cyber terrorism. Emphasizing international cooperation along with growing importance of civil society's role in internet, the Budapest conference declared that it would create a global centre for capacity building initiatives, improving synchronization and providing security solutions to nations.<sup>xiv</sup>

The third edition of GCCS was held in Seoul, South Korea in 2013, focussing on 'social and cultural benefit, a safe and secure cyber space, cyber crime and international security'<sup>xv</sup> and witnessed the presence of large number of delegates from South Asia. The Seoul conference came out with a comprehensive document on cyber space titled 'Seoul Framework for and Commitment to Open and Secure Cyberspace' that offered a future dialogue to the international community especially developing nations to have easy access to internet in the field of education, economic advancement and other segments of development.

The Hague in the Netherlands organised the fourth GCCS in the year 2015 that centred on the themes of freedom, security and growth. Ninety seven countries participated in the conference "to promote practical cooperation in cyberspace, to enhance cyber capacity building, and to discuss norms for responsible behaviour in cyberspace".<sup>xvi</sup> The conference highlighted privacy as a human right and called upon member-states to develop internet 'as an enabler for development and innovation'<sup>xvii</sup> Key recommendations of the conference were 'development of secure conduct for online business, defence of online freedom of expression alongside fighting against online terrorist and criminal activities and encouragement of international stability in the cyber space'.<sup>xviii</sup>

## Major Issues at the fifth edition of GCCS 2017

With the objectives of **‘promoting inclusivity and human rights in cyber space, preserving an open, interoperable and unregimented cyberspace along with making a political commitment to create capacity building initiatives, addressing and supporting countries to minimise digital divide and recognising the role of private sector and technical experts’<sup>xxix</sup>**, the fifth edition of GCCS presented a global platform in which cyber experts from all over the world could obtain vast knowledge, skills and experiences from each other to protect cyberspace in a technology-driven era. The conference was in sync with its earlier events, but unique in the sense that for the first time a developing nation like India hosted the event. It is noteworthy to mention that previous conferences were mostly held by European countries due to the heavy dependence of their economy on interlinking computer systems, which they wanted to protect as network system internationally without breaching the local legal regimes.<sup>xx</sup> Hence, Global Conferences on Cyberspace provided them an opportunity to discuss benefits and challenges along with identifying international legal norms to behave fairly in cyberspace.

India has emerged as a major cyber power at the heart of the government’s development paradigms such as ‘Digital India, Skill India, Startup India, aiming at strengthening network connectivity, empowering citizens and reducing digital dividends in the country. Promoting **‘digital infrastructure’, ‘digital delivery of services’ and ‘digital literacy’, the present government initiated a digital eco-system in every sector of governance from education to healthcare to banking; all have been linked online so that common people can have a hassle-free living experience.**<sup>xxi</sup> Highlighting opportunities provided by digital space, the government of India has pursued the Aadhaar project, a verifiable digital identity where 1.18 billion out of the total population have been linked with Aadhaar cards. The motive behind all these schemes is to create a digitally inclusive society and breaching the digital divide between digital haves and digital have-nots. In addition, digital economy consisting of IT, communication, e-commerce, digital payment, electronic manufacturing promote the pace of India’s GDP growth. Amidst all these developments, protecting cyberspace is a great concern for the country. The country needs to cope with digital threats which know no boundaries, and **require implementation of a robust legal framework for eliminating digital abuses by terrorists and radical actors.** Although the Indian government has taken various measures to deal with cyber challenges, that is not adequate. There is need for a unified international voice to look into cyber security issues.

The Fifth edition of Global Conference on Cyber Space (GCCS) recognised India’s growing capabilities as major cyber power as acknowledged by the international community. Terming it as a historical event, Shri Ravi Shankar Prasad, Minister for Electronics and IT and Law and Justice observed that “GCCS 2017 will give the world’s cyber community a unique opportunity to learn from global experience and expert insight, and discover more about the technology-led transformation being engineered in India.”<sup>xxii</sup> The following are the major issues discussed at the event:



- ***Increased citizen's participation and changing role of governance***

GCCS 2017 focussed on increased engagement of citizens in a free, open and inclusive cyber space that aimed to provide an equal platform and variety of opportunities to citizens from all strata, harnessing cyber capabilities of differently-abled civilian and greater representation of vulnerable section such as women and children. However, the conference also addressed that freedom in cyber space should be promoted within certain limits; privacy of users should always be respected.

The rapid advancements in the sphere of internet starting from email, personal computers to current opening of social media and mobile phones for data storage and communication has brought about a revolution not only in cyber space but also in the social, political and economic arena.<sup>xxiii</sup> In the economic arena, the evolution of cyber space and technology has brought a foundational change in the nature of economic growth. **GCCS 2017 credited the importance of cyber space in advancing economic growth of nations by offering newer scopes for innovation and entrepreneurship.**

Transformation of global business and economies via the advent of novel technologies such as artificial intelligence (AI), internet of things (IoT), adventures of robotics, data analytics, and 3G technologies has led to the fourth industrial revolution around the world. Digital age has created start up movements across the world with the intention of building a strong and sustainable economic system, offering employment opportunities to larger sections of population. It has made training of human knowledge and skills as important as industrial growth for economic development and offered newer opportunities for growth of start-ups. All these have created a scenario for renewal of governmental structures and become more accommodative to create an open and free cyber space for an increasingly cyber dominated global economy rather than some kind of interference in the digital world. The government should play the part of interface between citizens and economic growth with the help of the digital world, and this calls for modification of policy prescriptions of governments across the world.

The conference called for connecting traditional expertise with the modern discipline of science and technology in the arena of cyber space to reach out common people. Here, the role of governments across the world is commendable. In present times, governments utilise information and communication technology as an efficient mechanism to realise the 'goal of Good Governance with Minimum Government'<sup>xxiv</sup>. Nations around the world have been promoting the human face of technology in digital space creating digital infrastructures along with digital delivery of public services with a view to promote participatory governance among citizens especially disadvantaged groups.

At the Conference, the Indian Prime Minister Narendra Modi added that India has embraced the human face of technology to make life easy for the common people. In the welcome address at GCCS 2017, the Prime Minister talked about inclusive nature of internet and observed, "In India, we give primacy to the human face of technology, and are using it to improve "ease of

living”. Digital India is the world’s largest, technology-led transformative programme which is paving the way for our citizens to avail digital services. We are using mobile power or m-power to empower our citizens”.<sup>xxv</sup> The adoption of digital technology facilitates an easy life for farmers, entrepreneurs, pensioners and women in the IT sector in India, reinforcing democratic values and ideals contributing to participative governance.

The main theme of the conference i.e. cyber4all provided an opportunity to discuss the current digital divide between countries leading to discriminatory behaviour in cyber space where selective gateways controlled the access to internet. One of the key issues highlighted in *Cyber4growth* was the principle of net neutrality. At the inaugural ceremony of the conference, the Prime Minister of Sri Lanka Ranil Wickremesinghe talked about the importance of net neutrality in cyber space. Net neutrality offers all service providers an equal space in internet. The Prime minister said, “Net neutrality lowers the barriers of entry by preserving the internet as a fair playing field and helps more business and entrepreneurs thrive online”.<sup>xxvi</sup> The Sri Lankan Prime Minister’s views came at a time when United States federal communications commission under President Donald Trump’s regime is planning to dismantle net neutrality and provide service providers a freehand to manage information, creating a monopoly for certain telecommunication giants to control internet. This would lead to a real setback for democratic ideals and principles where freedom of speech of everyone is widely acknowledged.

### **Increased use of internet by terrorist groups and cyber security**

Stressing on the human side of technical threats, the discussants at the conference also pointed out the involvement of increased terrorist elements in cyber space. Increased use of mobile phones and social media has brought newer challenges in the threat landscape of cyber space. Terrorists often use social media to influence the youth in their radical agenda and sometimes they gain more popularity than national leaders, utilising Internet for harmful purposes, threatening national security forces. Proliferation of cyber warfare damaged security of the international system given the intricate interconnectivity of computer networks and internet around the world. Therefore, countries across the world should take the responsibility of managing the security services to identify cyber attacks and prevent them. In this process, government also should take into account the need to create a balance between protecting privacy and open behaviour of internet on one hand and safeguarding national security and interests on the other hand. Focus should be given to both rules and regulations at the national and international level.

Like any other nation, India too has become vulnerable to cyber attacks by terrorist groups and organisations and there is an urgent requirement to formulate a global institution to look into cyber defence and offense capacities. At the inaugural session at the GCCS 2017, expressing deep concern over the use of internet by terrorist and radical elements, Prime Minister Narendra Modi believed that only well-trained and competent personnel could deal with cyber attacks and security agencies should exchange information and initiate coordination in dealing with constantly evolving cyber threats.<sup>xxvii</sup> At the ministerial forum of countries participating in

the fifth GCCS 2017 Ajit Doval, National Security Advisor of India also raised concerns over increasing use of internet by terrorist groups. He asked that security organisations across the world should collaborate to fight against cyber threats and cyber warriors. The National Security Advisor stressed the need for joint efforts by both private and government sectors including various stakeholders representing people from different regions.

At the conference, various countries alleged that cyber crimes have been sponsored by state authorities. Andrei Krutskikh, Russian Presidential Envoy for Information and Communication found that the total anarchy in cyber space created a heavenly space for hackers and terrorists who sought to use internet to collect confidential information and meddle in the internal affairs of other countries. In the light of such situations, more than 120 nations had organised drills to combat cyber wars.<sup>xviii</sup> He stated, “Our planet stands on the brink of a new era, as robotics are rapidly evolving, chips are implanted in human bodies, there are unmanned vehicles and blockchain technology.... but all these fields need information security to be ensured, so we all need to make agreements and outline the rules of the game”<sup>xxix</sup>. International humanitarian laws should be applied in a manner that principles of sovereignty and non-interference in cyber space do not get affected. Countries should adhere to UN backed rules and regulation in cyber space without interfering in the internal affairs of states.

Governments across the world are using information and technology in their public services along with reconstructing their economies for growth and innovation. Amidst this increased digitization, safeguarding cyber space in particular protection of data and services is an urgent need. John Suffolk, head of cyber security at Chinese technology giant Huawei, suggested that “The importance of privacy and cyber security increases as an economy relies on digital technology”. Criminals or cyber warriors could illegally use personal data for unlawful purposes. Therefore, governments should begin to support companies that protect personal data of users in a systematic manner while on the other hand punish those who fail to do so.

It is well-known that nations alone cannot control surge of cyber crimes in the era of digital economy where government and organisations function through digital technology. Cooperation among nations is crucial. Security agencies around the world should collaborate with each other and exchange information. Special attention should be placed on newer security techniques, promotion of ethical values in cyber world, creation of legal establishment in cyber space, exchanging cyber aptitude to create cyber-specialist. In addition, the conference called for urgent and efficient monitoring apparatus to look after illegal activities

### **Cyber diplomacy and international cooperation**

Embracing communication and technology in governance came at a price. The dynamic and growing nature of cyber space has brought a new set of challenges. Cyber warriors can operate effectively and destroy networks of any nation due to lack of borders and the anonymity of the actors in cyber space. Therefore, nations across the world should collaborate with each other, reinventing traditional concepts of sovereignty and jurisdiction; and, the presence of large

number of cyber experts at the Global Conference on Cyber space indicated they were doing the same.

Diplomacy in cyber space should be encouraged. There should be sustained efforts on the part of the nations to resolve conflicts in cyber space ensuring an open and accessible cyber space to all states for improving quality of life. The heterogenic nature of cyber threats accelerates a process to build a comprehensive mechanism involving all the stakeholders. However, it is not an easy way especially in the circumstances of lack of a common international law to deal with cyber challenges. Countries should voluntarily come together to implement adequate measures for identifying threats and prevent them. Delegates at the conference agreed on 'global cooperation based on shared values' to fight rising cyber threats.

The External Affairs Minister Mrs. Sushma Swaraj in her keynote address at the valedictory function of GCCS 2017 stressed that security in cyber space can be achieved through using tactics of diplomacy and global cooperation among nations. Focussing on sharing of knowledge and strengthening the universal understanding of challenges in cyber space, the External Affairs Minister asked experts on the subject to create a consensus on cyber governance. Adequate capacity building schemes should be promoted to acquire manpower trained with cyber capabilities.

In this interconnected world, it is the responsibility of every nation to ensure cyber security through global collaboration. As far as India is concerned, various countries at the GCCS2017 agreed to cyber security cooperation. It is quite apparent that the Digital India initiative has contributed to making India as one of the emerging cyber economies through use of digital technologies for development purpose. There has been increasing use of information and technology in areas like health, education, agriculture, poverty alleviation and so forth. All these initiatives for digital inclusion have added to cyber security risk. The country is in rock-bottom with regard to a strong cyber security infrastructure. A report published by NASSCOM in 2017 viewed that India had been one of the top fourth countries which was severely affected by ransomware.<sup>xxx</sup> The representative from Russia at the GCCS 2017 stressed that India and Russia should strengthen cooperation to prevent conflicts with regard to the use of internet rather than resolving conflicts. Lord Tariq Ahmad of Wimbledon, UK's Foreign and Commonwealth Office Minister, held that in an era where digital technology and internet impacts economic, political and social aspects of people's lives, Commonwealth members should work closely and share knowledge and skills enhancing collective capability in cyber security. The minister also elaborated on how the UK has been advancing its cyber capabilities by investing almost \$2 billion over five years for making the country one of the most protected nations of the world for smooth running of online business.<sup>xxxi</sup>All member states of the Commonwealth including India have common interests and should jointly make efforts to secure network enhancing digital technology.

At the conference, all countries agreed that India would launch *Digital Knowledge Sharing Platform*<sup>xxxi</sup> that would consist of government, private sector and civil society to assist in exchanging knowledge and skills among nations to create a secure and global cyber space.

## Conclusion

In recent times, several high level summits, conferences, interactions between the heads of the states discussed the importance and necessity of internet to societal, economic and cultural lives. In similar fashion, a global platform like the *Fifth Global Conference on Cyber Space (GCCS) 2017* promoting comprehensive, open, secure, sustainable and easily accessible internet governance, addressed the key opportunities and challenges of internet in the presence of multiple stakeholders that consisted of governments, civil society, private sector, academia and technical experts.

In this interconnected world, it is the responsibility of every nation to ensure cyber security through global collaboration. In addition, government should also create awareness among the common users about challenges of cyber threats and safe use of digital platform. Technological advancement should create effective tools for citizen participation. The conference called for digital inclusion in all segments of development focussing on 'access programs, digital skill training, community technology spaces and low cost access devices'<sup>xxxiii</sup>. The conference identified various loopholes and issues such as dearth of international cyber coordination and focussed on efforts to bring out a new international legal structure for cyber coordination. It acknowledged the significance of good cyber behaviour on the part of citizens safeguarding critical infrastructures and data of citizens from the attacks of cyber warriors. In this process, there should be a massive restructuring of the education system so that future generations would be well-prepared to deal with the huge cyber challenges offered by the cyber space.

\*\*\*\*

*\*Dr. Chayanika Deka, Research Fellow, Indian Council of World Affairs, New Delhi.  
Disclaimer: The views expressed are that of the Researcher and not of the Council.*

## Endnotes

---

<sup>i</sup> Global Conference on Cyber Space 2017, <https://gccs2017.in/about#goal>, accessed on 1 December 2017

<sup>ii</sup> GCCS Conferences, 2011 London, *GCCS 2017: Global Conference on Cyber space*, <https://gccs2017.in/pastconferences>, accessed on 15 December, 2017

<sup>iii</sup> GCCS2017, Chair statement.

<sup>iv</sup> Chair statement, Budapest Conference on Cyberspace, 4-5 October 2012, <https://www.gccs2015.com/sites/default/files/documents/Chair%27s%20Summary%20Budapest.pdf>, accessed 15 December, 2017

<sup>v</sup> *ibid*

<sup>vi</sup> GLOBAL CONFERENCE ON CYBERSPACE 2015 CHAIR'S STATEMENT, <https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%202017%20April.pdf>, accessed 15 December 2017.

<sup>vii</sup> Global Conference on cyber space, Chair statement,

<sup>viii</sup> *ibid*

<sup>ix</sup> London Conference on Cyber Space, Chair's statement, 2 November 2011, <https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement>, accessed 15 December 2017.

<sup>x</sup> Global Conference on Cyber space 2017, Chair's statement.

<sup>xi</sup> *ibid*

<sup>xii</sup> *ibid*

- 
- <sup>xiii</sup> Budapest Conference on Cyber Space, 4-5 October 2012, <https://www.gccs2015.com/sites/default/files/documents/Chair%27s%20Summary%20Budapest.pdf>, accessed 17 December 2017.
- <sup>xiv</sup> *ibid*
- <sup>xv</sup> Seoul Framework for and Commitment to Open and Secure Cyberspace, <https://www.dsci.in/sites/default/files/Seoul%20Framework.pdf>, accessed 15 December 2017.
- <sup>xvi</sup> Global Conference on Cyber Space 2015, <https://www.gccs2015.com/gccs/all-about-gccs2015>, accessed 16 December 2017
- <sup>xvii</sup> *ibid*
- <sup>xviii</sup> *ibid*
- <sup>xix</sup> Global Conference on Cyberspace 2017, <https://gccs2017.in/about#goal>, accessed on 1 December 2017
- <sup>xx</sup> Governments must not censor internet, says William Hague, The Guardian, 1 November 2011, <https://www.theguardian.com/technology/2011/nov/01/governments-must-not-censor-internet>, accessed on 1 December 2017.
- <sup>xxi</sup> “Digital India – A programme to transform India into digital empowered society and knowledge economy”, PIB, Government of India, <http://pib.nic.in/newsite/PrintRelease.aspx?relid=108926>.
- <sup>xxii</sup> “India to Host Global Conference on Cyber Space 2017 – World’s Largest Conference on Cyber Space”, PIB, Government of India, <http://pib.nic.in/newsite/PrintRelease.aspx?relid=168850>, accessed 1 December 2017
- <sup>xxiii</sup> Full Text of PM Narendra Modi’s speech at GCCS: Stop cyber space from becoming terror playground”, The Financial Express, 23 November 2017, <http://www.financialexpress.com/india-news/full-text-of-pm-narendra-modis-speech-at-gccs-stop-cyber-space-from-becoming-terror-playground/944665/>, accessed 15 December 2017
- <sup>xxiv</sup> Global Conference on Cyber Space 2017, Chair’s statement
- <sup>xxv</sup> “Full Text of PM Narendra Modi’s speech at GCCS: Stop cyber space from becoming terror playground”, The Financial Express, 23 November 2017, <http://www.financialexpress.com/india-news/full-text-of-pm-narendra-modis-speech-at-gccs-stop-cyber-space-from-becoming-terror-playground/944665/>.
- <sup>xxvi</sup> “Sri Lankan PM bats for net neutrality at cyber meet”, *The Times of India*, 24 November 2017, <https://timesofindia.indiatimes.com/india/sri-lankan-pm-bats-for-net-neutrality-at-cyber-meet/articleshow/61778519.cms>
- <sup>xxvii</sup> *ibid*
- <sup>xxviii</sup> “Russia, India call to boost cooperation in information security field — envoy”, Tass, Russian News Agency, 24 November 2017, <http://tass.com/politics/977371>.
- <sup>xxix</sup> *ibid*
- <sup>xxx</sup> “Cyber Security: Are digital doors still open”, NASSCOM, 17 November 2017, <http://www.nasscom.in/natc/images/white-papers/cyber-security.pdf>
- <sup>xxxi</sup> “Commonwealth to prioritise cyber security; cyber capacity building: UK minister”, *business Standard*, 24 November 2017, [http://www.business-standard.com/article/news-ani/commonwealth-to-prioritise-cyber-security-cyber-capacity-building-uk-minister-117112400820\\_1.html](http://www.business-standard.com/article/news-ani/commonwealth-to-prioritise-cyber-security-cyber-capacity-building-uk-minister-117112400820_1.html)
- <sup>xxxii</sup> *ibid*
- <sup>xxxiii</sup> GCCS 2017 – Chair’s Statement- Summary , PIB, GOI, <http://pib.nic.in/newsite/erelease.aspx>, accessed 23 December 2017.