CYFY 2014: OUTCOME STATEMENT

'Cyfy 2014: The India Conference on Cyber Security and Cyber Governance' was held in New Delhi, from 15-17 October, 2014. It was attended by 350 participants, with speakers from over 12 countries representing government, business, academia and international organisations. Now in its second year, this conference has emerged as India's biggest international cyber policy platform to date. Cyfy's success highlighted two indisputable facts: the growing Indian interest and thought-leadership on internet governance and the increasing attention of the global community to cyber debates in India, as was apparent by the high-level participation at Cyfy.

The Indian Minister for Communications and Information Technology Ravi Shankar Prasad inaugurated the conference. He discussed the ambitious 'Digital India' programme, the breadth and scope of which surpasses any similar endeavour across the globe. In order to bridge the digital divide, the Minister enumerated a number of projects that will serve the citizens, including e-government applications and financial inclusion programmes that will leverage the power of mobile technologies. He also mentioned the launch of innovative platforms to help solve pressing social issues.

In his valedictory address, India's Deputy National Security Advisor Arvind Gupta addressed the security challenges posed by a fast-growing internet ecosystem. He pointed out that India already has a billion mobile phones active on the ground. These, and others joining the network, need to be connected to the internet through effective and secure digital information infrastructure. Calling it a big focus area for the Indian government, the Deputy NSA remarked that India is at an advanced stage of implementing a comprehensive cyber security architecture.

The discussions at Cyfy confirmed that the Indian government is not the only stakeholder grappling with the central question: Can, should and how will the internet be regulated, governed and managed? This crucial question, running as a common thread through the 14 sessions at Cyfy 2014, found resonance in the themes of jurisdiction, security, privacy, use of social media, critical infrastructure, global governance platforms and the rules of the global cyber market.

While a detailed report of the conference will follow, below are a set of important initial impressions:

* The role of states in the internet age was discussed in detail. Some experts framed the debate around the internet being a global commons, thereby arriving at a set of conclusions about its governance structure. This included the idea of a UN-led internet governance structure, and the application of an international legal regime. The commons would mean equal governance access for sovereign governments. However, another school of thought argued that the internet is a collection of interconnected public and private networks that exhibit the characteristics of a global commons, but fall short of being one. They reached a different set of conclusions. Multiple institutions comprising of multiple stakeholders, as they do today, are capable of governing different aspects of internet governance: from technical to social issues. There was a feeling that talk of global governance arrangements may be moving away from the "ideal" to realpolitik.

* However, on the topic of developing cyber norms, the sentiment of the house was that there can be no single grand design that will produce, in one instance, a set of principles or guidelines on organising the cyber world. It was argued that a sectoral approach might have more success.

CYFY

* It was also noted that 'internet multilateralism' was at an interesting juncture. Will the rules of the medium be decided by dialogue between major powers like the US, China and Russia? The possibility of a 'Digital 20' was flagged: Nations with similar interests could band together to sign a digital treaty, compelling the rest to either opt in or opt out. The experience of the Arms Control debate of the 20th century, it was held, offers an interesting perspective.

* On the topic of internet governance, ICANN reform was discussed in some detail. The organisation is facing a question of legitimacy over the issue of 'space capturing' by some players. An alternative   possibly moving ICANN functions to the ITU (or other fora) faces concerns regarding efficiency. Many felt that the multilateral ITU will not serve as an appropriate platform for a fast-moving medium like the internet. Others suggested the ITU be reformed to enable it to absorb these functions. However, it was noted that even proponents of multistakeholderism are trying to nuance their positions, since the 'characteristic' of an institution being 'multistakeholder' seems to be taken as the solution itself. It must be determined if the resultant multistakeholder structure(s) is interventionist in nature, and if the presumed *universalised* values underlying debates at these forums are helpful to the particular challenges of developing countries. ICANN, it emerged, was keen to discuss 'all issues,' including its internationalisation and matters of jurisdiction, as it undertakes the IANA transition.

* The future of internet governance, it was clear, is not going to be a straightforward division of emerging powers vs. major powers. The multipolar nature of the world and the tension between values and interests are likely to have a significant impact on future arrangements within this medium.

* Participants raised key questions on the quality of interconnectivity and appropriate mechanisms for securing critical infrastructure. While everyone wants system security, some difficult questions need to be addressed: What are the costs and how will they be shared? Who will be the interlocutor for defining what constitutes the definable objectives? On the question of international security, it was held that traditional notions of deterrence do extend to the cyber domain. The challenge will be to adapt to this particular medium and generate better understanding of concepts of offence, defence, deterrence, pre-emption and prevention in cyberspace.

* Terror networks flourishing over the internet were flagged as a common cause of concern by most individuals present. This moved the conversation towards solutions by way of real-time information sharing and closer cooperation between countries, despite varying interests. There is also a need for the 'state' to find the right balance between surveillance and privacy in order to secure its citizens without infringing their rights. Accountability of agencies of the 'state' involved in surveillance activities was also identified as a key area of concern.

* Freedom of speech was discussed extensively, along with the reality that there is no global consensus on normative value of free expression. Does simply being connected by an open internet mean universalisation of these values? As for social media, while it gives rise to the same contradictions as older communication technologies, there is today integration and fragmentation at the same time. Polarisation in some cases is contrasted by greater unity in others. Social media is far broader in scope, reach and impact, and thus more powerful   or dangerous. Regulation of content is also a very contentious issue. Who should be regulated? Those who generate the information, those who transmit it or those who use it   and in which proportion and order? Countries like India who believe in 'reasonable restrictions' need to find the golden mean between needing to preserve free speech and maintaining law and order.

* The conversation noted the importance of finding the balance between anonymity and connectivity, between privacy and security, as also   as increasingly apparent today   between innovation and regulation.

* The discussion highlighted the slow move towards private censorship as intermediaries are given more powers by technology, governments and citizens to be arbitrators of speech.

* The debate on the global cyber market   the engine fuelling the growth of the internet   hinted that harmonisation of laws across the world could be an effective way to solve many of the jurisdictional issues that arise because of international data flows and transactions. This includes data protection laws. Further, while the development of government-to-business relationship in cyberspace is important, the problem is that 'business' is not a united actor. The state will still need to mediate between competing capital and sector interests.

CYFY

* The idea of data localisation was brought up several times. Whether or not sovereignty over data translates into economic progress and security was a matter of intense debate. The tension between dispersion and centralisation of power was highlighted. The question of localisation of internet infrastructure was also raised. Those who wanted centralised power argued for data localisation to ensure data security. Others, however, argued that dispersion is needed to provide security and efficiency, and that data nationalisation is no guarantee of security.

What the high-level and complex debates at Cyfy 2014 revealed was, as C. Raja Mohan, Distinguished Fellow at the Observer Research Foundation, captured in his closing comments "the age of innocence is over…., the widely held beliefs that cyberspace will be a libertarian utopia for individuals and a technological cornucopia for corporations now look utterly unrealistic….. the experiment in constructing a cyber world beyond states has come to an end." Cyberspace needs common rules so that all stakeholders can use it legitimately, legally and safely. India has taken a strong position to preserve the democratic nature of the internet. At the same time, India's Minister of Communication and Information Technology expressed his willingness to "take that extra step as far as the evolution and stabilisation of these frameworks" is concerned. These frameworks must be inclusive and democratic. Cyfy 2014 was an important step in bringing Indian ideas and debates to the world. Indian audiences were also exposed to some key global conversations. We are looking forward to continuing these efforts in the years to come.

Samir Saran
Chair
Cyfy 2014

CYFY