CyFy 2013

14 – 15 OCTOBER 2013

The Origins of the Conference

A rapid evolution of technology and the near omnipresence of the internet now mean that technical and policy related challenges around the cyber-space are evolving rapidly for both governments and other multistakeholder participants such as private sector, civil society, academia and the youth. Even as this virtual space allows unparalleled connectivity and communication, it is fast becoming contested territory. People and nations are now critically dependent on inherently vulnerable and excessively networked infrastructure. Most militaries, organised crime syndicates, secret services and other actors have realised the underlying strategic potential of these critical vulnerabilities. Militaries can be disabled to alter defence postures. Critical Infrastructures in public and private spaces can be manipulated to destabilize nations. Economies can be weakened through acts of sabotage and espionage. People can be polarised and mobilised by the connectedness of the World Wide Web. None of these postulations are based on future scenarios. Each of these has been proved to be right in recent times. Cyber space and internet, in spite of its life altering advantages, represents increasingly risky discourse and therefore will inevitably be securitised. On the other hand, cyber security can itself become a threat, when abused. Dictatorships already abuse the notion of 'cyber threats' as an excuse to implement strong surveillance and censorship in their countries without appropriate oversight. Freedom and democracy, as we know them today, may increasingly be placed at risk when implementing cyber security strategies. Freedom of expression and privacy is be challenged and altered in many ways. The role for private sector, civil society, academia, technical communities and media is being redefined in a space that has been a traditional preserve of governments.

The time is right to address these challenges and do so comprehensively. New threats from highly skilled, well-resourced multi-spectrum, non-state attackers have to be acknowledged. New response strategies have to be thought out along with a major impetus on capacity building to create the next generation of cyber defense warriors. Traditional policing, prevention techniques and mindsets may be ineffective and counterproductive. Then there are additional sets of problems associated with cyber security encompassing technical, market and policy failures. The cost of implementing a national cyber security plan needs formal recognition in government's budgetary process. These issues need wider deliberations. Global cyber security dialogue began with the London Conference in 2011, Budapest in 2012 and Seoul, Korea in October 2013.

The India Conference on Cyber Security and Cyber Governance: A Turning Point

At a national level, this task is perhaps equally important for emerging countries that are characterised by lower connectivity and relatively lower dependence on IT infrastructure in the immediate future. They have a tendency of underestimating the nature, source and the intensity of cyber attacks in the future. However, they can learn from the experience of high-tech communities to create proactive, robust information societies, more sensitive and sceptical to informationalization and networking. This would enable the creation of new technological and strategic paradigms, which in turn the established information societies might learn from as well. Addressing these questions jointly and cooperatively, including by appropriate engagement of multi stakeholder groups is clearly beneficial. Nations states will have to respond to the challenges of this cyber-age through an unprecedented level of technical and legal collaboration. Trust will be key. Yet some experts see this as a ‘zero-sum-game’ and are creating strategic postures for national security purposes. Reconciling the two agendas for this most dynamic global common will be the central challenge of our times.

The cyber security challenge involves balancing international cooperation with national priorities; protection of free speech and privacy with national security; inter-governmental arrangements with multistakeholder dialogue to sift technical innovations with slow-paced legal and legislative responses; traditional policing and policy makers with digital natives, to counter technically savvy cyber attackers. Mindful of these, the Observer Research Foundation (ORF) and The Federation of Indian Chambers of Commerce and Industry (FICCI) have come together to host ‘**The India Conference on Cyber Security and Cyber Governance**” at The Oberoi, New Delhi, India, on October 14-15, 2013, to discuss these very challenges and more.

CONFERENCE DETAILS

Steering Committee:

Sunjoy Joshi, Director, Observer Research Foundation
Samir Saran, Vice President, Observer Research Foundation
Vivek Lall, President & CEO, Reliance Industries Limited
Mahima Kaul, Fellow, Observer Research Foundation
Virat Bhatia, Chair, Communications & Digital Economy Committee, FICCI
Sarika Gulyani, Joint Director & Head-IT & Telecom Division, FICCI

Co-Chairs:

Samir Saran, Vice President, Observer Research Foundation
Virat Bhatia, Chair, Communications & Digital Economy Committee, FICCI

Coordinators:

Mahima Kaul, Fellow, Observer Research Foundation
Sarika Gulyani, Joint Director & Head-IT & Telecom Division, FICCI
Darshana M. Baruah, Research Assistant, Observer Research Foundation

CyFy 2013

14 – 15 OCTOBER 2013

Confirmed Speakers:

- **Kapil SIBAL**, Minister for Communications and Information Technology, Government of India
- **Shivshankar MENON**, National Security Advisor, Government of India
- **Manish TEWARI**, Minister for Information and Broadcasting, Government of India
- **Nehchal SANDHU**, Deputy National Security Advisor, Government of India

- Jaak AAVIKSOO, Minister of Education and Research, Republic of Estonia
- Sunil ABRAHAM, Executive Director, Centre for Internet and Society, India
- Dirk BRENGELMANN, Commissioner for International Cyber Policy, Federal Foreign Office, Germany
- Ashish CHAUHAN, CEO, Bombay Stock Exchange, India
- Michael CHEETHAM, Director, International Science & Technology Partnership, AAAS, USA
- Jim CLARKE, EU Strategic Liaison Manager, Waterford Institute of Technology, Ireland (Rapporteur)
- Oleg DEMIDOV, The Russian Center for Policy Studies, Russia
- Michael GAUL, Senior Advisor, Emerging Security Challenges Division, NATO
- Peter GRABOSKY, Researcher, Australian National University, Australia
- Brooke GRIFFITH, International Business Development, Raytheon Intelligence and Information Systems, USA
- Arvind GUPTA, Director General, Institute for Defence Studies and Analyses, India
- Sean KANUCK, National Intelligence Officer for Cyber Issues, Office of the Director of National Intelligence, USA
- Anja KOVACS, Internet Democracy Project, India
- Vivek LALL, President & CEO, Reliance Industries Limited, India
- Eric H. LOEB, Vice President, International External Affairs, AT&T, USA
- Vijay MADAN, Chief Mentor, Tata Teleservices Limited, India
- John C. MALLERY, Research Scientist, MIT Computer Science & Artificial Intelligence Laboratory, USA
- Rajan MATHEWS, Director General, Cellular Operators Association of India
- Michael McMAHON, Deputy National Intelligence Officer, Cyber Issues, National Intelligence Council, USA
- C. Raja MOHAN, Distinguished Fellow, ORF, India
- Prakash NAGPAL, Senior Vice President, Product Marketing and Marketing, Narus, India
- Ram NARAIN, Deputy Director General (Security) in the Department of Telecommunication, Government of India.
- M. M. OBEROI, Indian Police Service, Joint commissioner of Police, Delhi Police, Government of India
- Christopher PAINTER, Office of the Coordinator for Cyber Issues, Department of State, USA
- Gabi SIBONI, Director, Cyber Warfare Program, Institute for National Security Studies, Tel Aviv University, Israel
- Joe SULLIVAN, CSO, Facebook, USA

CyFy 2013

14 – 15 OCTOBER 2013

Monday 14th October

Negotiating Cyber Governance

11:00 – 11:30 **Tea**

11.30 – 12:30 **INAUGURAL SESSION**

11.30 Welcome by Sunjoy Joshi, Director, ORF

11.35 Welcome by Virat Bhatia, Chair, Communications & Digital Economy Committee, FICCI

11.40 **Keynote Address** by Shivshankar Menon, National Security Adviser

12.00 **Inaugural Address by Minister** Kapil Sibal, Communications and Information Technology

12:25 **Vote of Thanks by** C. Raja Mohan, Distinguished Fellow, ORF

12:30 – 13.30 **Networking Lunch**

13:30- 15:00 **SOVEREIGNTY, INTERNATIONAL COOPERATION AND CYBER SECURITY: A TREATY DIALOGUE**

Given the global and often borderless nature of cyber security issues, can countries simply take a sovereign approach to the issue? How does India view the Budapest Convention? How can Indian laws and views be coordinated with international norms? What are the challenges to become a signatory? Are there other immediate alternatives?

15:00-15:15 **Tea**

15:15 – 16:30 **THE FIRST LINE OF DEFENCE: THE PRIVATE SECTOR**

The private sector not only owns most network infrastructure around the world, but they are often the most vulnerable to cyber attacks. They are also by default the first respondents. What is the role of the private sector in securing cyber space vis-à-vis the government, within the current market models and regulatory frameworks? How can PPP models be developed and strengthened in the sphere of cyber security? And, how can information sharing or mutual self-defence pacts within the private sector and with the government be made more effective?

16.30 - 17:45 **CYBERSECURITY: STRATEGIES AND RESPONSES**

What are the current national and international approaches to cyber security? What ideas have been put forward by various blocks, and what is India's own thinking? What are the best practices in the mitigation of high profile risks including protecting CII – Critical Information Infrastructure like nuclear facilities? How vulnerable is the cloud and how can it be protected? And, how can we create mechanisms to protect global supply chains and develop global standards for cyber security?

Inaugural Dinner

Venue: The Oberoi, New Delhi

Time: 19:30

"Freedom of Expression in the Internet Age"

by Manish TEWARI, Minister for Information and Broadcasting, Government of India

CyFy 2013

14 – 15 OCTOBER 2013

Tuesday, 15th October

LOOKING AHEAD

09:00– 09:30 Tea

09:30- 9:45 Keynote Address by Minister Jaak Aaviksoo

09:45- 10:00 Q+A

10:00 – 11:30 **IMPLEMENTING NATIONAL CYBER SECURITY POLICIES**

Where are the threats to the global internet commons really coming from? What are the different approaches when looking at cyber crime and cyber warfare? What are the policy failures, contradictions, market conditions and technical vulnerabilities that have led to the growth of cybercrime? How can supply chains be protected? What role can communications networks and infrastructure play in responding to cyber threats?

11:30 – 11:45 Tea

11:45 – 13:15 **INTERNATIONAL PUBLIC PRIVATE PARTNERSHIP IN CYBER GOVERNANCE**

How feasible is international cooperation and centres for excellence where countries can share expertise? How can countries work together amongst themselves and with the Private sector to combat cyber crime and cyber warfare? What are the possibilities of developing acceptable standards and norms without technology and commercial biases favouring corporations and countries? How can governments coordinate effectively when cyber governance is still dispersed within nations among ministries and departments?

13:15-14:15 **Lunch**

14:15 – 16:00 **PRIVACY and NATIONAL SECURITY**

Securitising the internet often puts freedom of expression at risk – What are the pros, cons and practical challenges in managing security and freedom of expression? Where does security begin and privacy end? Can surveillance and privacy co-exist? How to deal with big data collection and what are the implication of the emanating vulnerabilities?

16:00 – 16:15 Tea

16:15 – 17:45 **MULTISTAKEHOLDERISM: Avoiding the PRISM Paradigm**

Following the Tunis Agenda 2005, the civil society and academia was expected to play a stronger role in internet governance and by extension, in cyber security. However, along the way it seems, that multi-stakeholder groups and citizens have been disenfranchised from the security and governance agenda of states and institutions. Increasingly, the securitized and corporatized cyber space is reshaping notions around privacy, property and sovereignty. Private citizens, who constitute much of the virtual world have minimal voice and impact on governance agendas and discourse. How do we bridge this cleavage? What should be the language, platforms and format of communication between the citizen and state? This session seeks to understand the modalities of the new multistakeholder dialogue that must begin between citizens, private sector and governments across the world on for creating a safe and free cybersphere.

17:45-18:00 **READ OUT by Dr C. Raja Mohan,** Distinguished Fellow, Observer Research Foundation

18:00-18:15 **VALEDICTORY ADDRESS by Nehchal Sandhu, Deputy National Security Advisor, Government of India**

18:15-18:20 **VOTE OF THANKS by Samir Saran**, Vice President, Observer Research Foundation