CYFY 15-17 OCT 2014

THE INDIA CONFERENCE ON CYBER SECURITY AND CYBER GOVERNANCE

THE OBEROI HOTEL, NEW DELHI

Report

CYFY 15-17 OCT 2014

THE INDIA CONFERENCE ON CYBER SECURITY AND CYBER GOVERNANCE

THE OBEROI HOTEL, NEW DELHI

OBSERVER RESEARCH FOUNDATION
NEW DELHI

Contents

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 follows in the pages ahead, 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 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.

- 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, the Internet Corporation for Assigned Names and Numbers (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 International Telecommunications Union (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 upon 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 which 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 relationships 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.

- 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 that "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

Introduction

The internet seems to be an increasingly preferred medium of communication for large sections of the country's population – a testimony to the comfortable relationship that Indians now enjoy with technology. Today, anywhere between 300 to 400 million Indians are connected to the internet and, according to studies on internet penetration in India, up to 100 million more people in the country will go online in the next year alone.

India will soon be adding 10 million users every month and this large number of new users will shape the digital world in multiple ways. This phenomenon is not unique to India. It is clear that in the current decade, the internet is witnessing a rapid geographical shift – from its user base concentrated around the Atlantic Ocean to the fast-growing economies in Asia and Africa. A digital pivot to Asia – and more specifically to India – is undeniably underway.

Cyfy 2014

The India Conference on Cyber Security and Internet Governance sought to address this shift in digital consumption and influence. One of the key issues that has emerged with the coming of "Digital Asia" is whether netizens will be engaged with, and cognizant of, the role of institutions and the governance architecture that will impact their ability to use, benefit from and leverage this medium. Will they be included in key global debates on cyber security and internet governance? Will they have access to institutions where they must participate and be heard? CyFy 2014 provided a platform to bring key global debates to India and enabled Indian stakeholders to share their opinions with the global community. In many ways it sought to make a modest yet meaningful contribution to India's engagement with the global community on cyber security and internet governance.

In its second year, CyFy attracted speakers from government, industry and academia from India and over a dozen countries; over 350 delegates attended 14 sessions during the three-day conference organised by the Observer Research Foundation (ORF) and the Federation of Indian Chambers of Commerce (FICCI) from October 15 – 17 in New Delhi.

Compared to its first avatar, CyFy 2014 was larger in both scope and scale and expanded its original mandate by engaging in a wider set of issues.

The conference witnessed quality conversations on matters concerning both the developing and developed worlds. Its central objective was not to seek universalisation of positions and perspectives but rather to present differences and diversity and thereafter discover common ground in an uncommon digital terrain.

The discussions at CyFy 2014 were particularly engaged with the challenges specific to developing countries, which are today establishing their digital domains. First among these challenges is the core question of access. Internet penetration in India is relatively low, with even the most generous estimates placing it well below 25 percent. This is far lower than India's partners in the BRICS grouping, for instance. There are other economies in South Asia and Africa with similar figures. Access is a major hurdle that must be overcome by any government seeking to provide services, governance and opportunities through digital means. The government alone cannot provide this access. A healthy participation from private enterprise and civil society is needed. The idea of a global village, connected by a network of networks, is predicated on access that allows participation by all. The creation of not just a global cyber market, but more broadly a common digital market, where services and ideas can move seamlessly across borders, is an ideal many stakeholders are striving for. That a fisherman on the coast of Kerala, using the internet, can instantly share photos and sell produce to customers halfway across the world squares the circle of the previous decade of that same fisherman connecting to local markets through a mobile phone.

It is this fisherman – and countless others like him straddling the last mile – that one must keep in mind when discussing the growth and potential benefits of the internet. What would make the internet attractive to them? To be able to access the internet in the language they know, to have keypads which allow them to use their native scripts and to have freely available content in the dialect they use are some of the key drivers in bridging the proverbial digital divide. Technical prowess needs to meet imagination and innovation, to offer the bottom-of-pyramid customers content to suit varied levels of digital and real literacy. Developing countries offer an expanding customer base of differentiated literacy and capacity, those who may struggle to read and write but would still be competent using keypads and voice stimulated applications. This new reality of users and the demand created from their aspirations is caveated by supply. The benefits of access can only be realised by allowing stakeholder engagement on terms that are contextual, inclusive and foster participation. It is indigenous content that will help increase adoption of internet and technologies, consequently driving up investments in internet infrastructure due to such local demand. It is certainly true of the internet that the global is linked to the local, and it is from the local that the new spurt of global growth will be derived.

This provision of access is also very sensitive to prices. Access to devices, to the network and content is also a result of the right pricing for the right demography. After all, the internet is finally giving communities choice and control over what and how they consume, unlike the one-way broadcast media of the previous generations. The Indian experience has certainly been an example of how to innovate for the customer. Right from a burgeoning luxury market, where the most expensive products find a home in India as easily as they would in the most developed markets of the world, there is also simultaneously demand for the world's cheapest tablet computer, geared for

students hungry for the benefits of technology. From monthly 3G (and soon to be 4G) plans offered to Indian consumers to solutions which offer internet services for INR 1 a day (less than two cents per day), the pricing market in India has responded to the fluid and dynamic demands of this aspirational class. It is this same adaptability and responsiveness of the internet as a whole, the regulatory regimes and pricing arrangements, and the governance that underwrites its free and open character which will ultimately shape the larger information society.

And this digital society needs to be built on a solid foundation of trust. Devices with backdoors, service providers with monitoring facilities, content companies with the keys to personal data, governments with surveillance capabilities, lawmakers and a judicial system with inadequate expertise, and cyber criminals with a growing arsenal of tools are only some of the challenges facing the average internet user. The prism through which societies look at these issues will shape its response to them, and ultimately, decide whether these technologies will liberate or constrain the digital citizen. What are the principles that a society would like to imbibe into its digital culture? Is security more important than privacy? Will a twentieth century approach to law and order trump freedom of expression? Will the net remain a neutral medium, or was it never one? All of these are increasingly important questions for the next and the new billion connecting to the digital world.

There is also the question of stability of the ecosystem. Data is a valuable form of currency, and its repositories have grown. Criminals, states and non-state actors have all demonstrated their willingness to exploit this medium. And they are not just looking at data. Infrastructure – computers, modems, fibre optic cables, wireless networks and devices – and critical sectors, including government services, defence, health, energy, information and telecommunications, and banking and finance, are immediately at risk. The private sector and the government are working together in many countries to inculcate an environment of risk assessment and information sharing to create frameworks in order to protect the medium. But nothing can exist in silos in the online world. The nature of the internet demands that countries and relevant authorities and institutions work together to battle these new threats, and together define norms of state behaviour in cyberspace.

And no conversation about the internet is complete without looking at the vast opportunities it offers. That it impacts economic growth, job creation and prosperity is visible. In 2014, global business-to-consumer e-commerce generated $1.5 trillion, and is set to increase by nearly 20 percent annually. But the real power of these technologies comes through in the huge transformations it has brought to societies and to individuals. Those left out of the education system can today use mobile and online solutions and participate in virtual classrooms where top academics in the world engage with them.

Artisans in rural areas can sell their products to customers without giving away a slice of revenue to the middleman. Talented – and not so talented – young people can become celebrities overnight, based on the number of likes and downloads they attract from the court of public opinion and not the filter of a critic. Patients in rural areas can consult city doctors through video calls, and professionals around the world too can use those same video calls to collaborate on projects. A

plumber can find his next job through the click of an app, and a student can make some pocket change by renting out her/his room over the weekend through the internet. These, and a billion other stories, only reinforce what we know to be the best qualities of the internet – open, inclusive and collaborative – and this is the reason why it is so important to discuss the many competing factors that continue to shape its development.

Cyfy 2014 and its succeeding editions strive to build a global platform located out of India to debate all of this and much more.

Cyfy 2014 was organised by the Observer Research Foundation (ORF) and the Federation of Indian Chambers of Commerce (FICCI), and took place from 15 – 17 October 2014 at the Oberoi Hotel, New Delhi, India.

Agenda

Session I - Cyber Lawfare: The Contest over Territory and Jurisdiction

The network of networks might be considered a global commons by many nations, but the infrastructure that runs it certainly has roots in specific countries. Therefore, the question confronting the smooth functioning of the internet is: Whose jurisdiction does digital data come under? Is it the origin of the data, the point where the server is located, or the final destination of the data? How will application of law be determined in a multi-geographical transaction? And, more pertinently, what jurisdiction, if any, is applicable to the entire internet itself?

Chair

C. Raja Mohan, Head, Strategic Studies, Observer Research Foundation, India

Panellists

Sean Kanuck, National Intelligence Officer for Cyber Issues, United States of America

Jamie Williamson, Head of Unit, Relations with Arms Carriers, International Committee of the Red Cross

James Lewis, Senior Fellow and Director of the Strategic Technologies Program, Center for Strategic and International Studies, USA

Session II - The Digital Nation: Is Social Media Disruptive or Democratic?

Although individuals, corporates and governments have embraced social media, it is increasingly the first casualty when there is a law and order problem. Countries are being blamed for 'scapegoating' social media. But is the hard truth that social media needs regulation? And what does this mean for freedom of expression in the digital age?

Chair

Ashok Malik, Australia India Institute - ORF Chair for Indo-Pacific Studies, Observer Research Foundation, India

Panellists

Raheel Khursheed, Head of News, Politics and Government, Twitter, India

Wajahat Habibullah, Former Chief Information Commissioner, India

Barkha Dutt, Group Editor, NDTV, India
Karuna Nundy, Advocate, Supreme Court of India, India

Session III - Counterterrorism in Cyberspace

The evolving nexus between terrorism and information and communication technologies (ICTs), in particular the internet, is undermining the global commons and is cause for global concern. This issue is of increasing importance in India as well, most recently flagged by Prime Minister Modi at the United Nations General Assembly in 2014. An honest assessment of ICT resources as tools for terrorism activities, such as incitement, recruitment, training, planning, collection of information, communication and financing, and as targets of terrorist activities, in particular critical infrastructures, needs to take place domestically as well as through international cooperation.

Chair
Marc Porret, Legal Officer, Counter Terrorism Committee Executive Directorate, the United Nations

Panellists
MM Oberoi, Director of Cyber Innovation & Outreach Directorate, Global Complex for Innovation, Interpol
Jan Neutze, Director, Cybersecurity Policy, Microsoft, USA
Deepak Maheshwari, Head, Government Affairs, Symantec, India
Rajan Luthra, Chairman's Office, Corporate Security Expert Services, Reliance Industries Limited, India

Session IV - Rethinking the Global Cyber Market

The growth of commerce over the internet has been, to a large extent, due to the free trade zone the internet has provided so far. But this seems to be changing. Is the value of the internet moving away from North America and Europe to Asia? Already 45 percent of the nearly three billion internet users, and four out of 10 of the internet's biggest companies are based in Asia. Some of these countries do not share the 'open' values the West prescribes. Many are engaged in bitter battles of cyber espionage with each other. Others want data localisation. Can the 'global cyber market' survive this?

Chair
Richard Ponzio, Head of Global Governance, the Hague Institute for Global Justice, Kingdom of the Netherlands

Panellists

Aaron Kleiner, Senior Strategist, Cybersecurity Policy, Microsoft, USA
Vijay Madan, Chairman, FICCI Subcommittee on Cyber Security and Chief Mentor, Tata Teleservices, India
Jonah Force Hill, Technology Policy Consultant, Monitor 360, USA
Kamlesh Bajaj, CEO, Data Security Council of India

Session V - ICANN or ICAN'T?

The IANA transition and the restructuring of ICANN to ensure broader participation still leaves open very important questions on the evolution of current internet governance. ICANN's attempt to attract broader participation and legitimacy is undermined by the reality that it is still located and has to respond to the jurisdiction of one nation. Will large emerging economies and other developing countries allow their interests and investments to be determined by local jurisdiction? Is the transition truly representative and will it make internet governance international? Will the control of the 'root' of the internet be democratised? Or will ideas, such as India's suggestion to move ICANN functions to the ITU, pave the way forward?

Chair

Samir Saran, Vice President, Observer Research Foundation

Panellists

Latha Reddy, Commissioner, Global Commission on Internet Governance; former Deputy NSA, India
Yu-Chuang Kuek, Vice President and Managing Director, Asia Pacific, ICANN
Dr. Govind, CEO, National Internet Exchange of India

Session VI - Deconstructing Multistakeholderism

Recent debates, internationally and also within Indian civil society, show that agreement on the appropriate process, form and format for multistakeholder governance of the internet still eludes us. It is important to recognise the differing perceptions on this issue and to discuss threadbare the difference in approaches and concepts around "multistakeholderism" and the dynamics that are shaping the motivations of government, businesses and civil society actors on this subject.

Chair

Suhasini Haidar, Diplomatic Editor, *the Hindu*, India

Panellists

Christopher Painter, Coordinator for Cyber Issues, US Department of State
Parminder Jeet Singh, Executive Director, IT for Change, India

Wouter Jurgens, Head, Cyber Security Department, Ministry of Foreign Affairs, Kingdom of the Netherlands

Alan Marcus, Senior Director, Head of Information Technology and Telecommunications Industries, World Economic Forum

Session VII - Protecting CIIs

There has been a steady increase in global cyber attacks, and recent sophisticated malware attacks like Stuxnex and Duqu have demonstrated the vulnerability of critical resources from power grids to nuclear facilities. India was the third most affected country, after Iran and Indonesia, by Stuxnet, infecting computers at electricity boards and an oil rig. The Indian Prime Minister flagged cyber security as a "major concern" at the BRICS summit in July 2014. The Government of India released a National Cyber Security Policy in 2013, but questions of policy and preparedness still remain. Are Indian CIIs – Critical Information Infrastructures – still in fire-fighting mode, and how do they transition to anticipating attacks? Are sectoral Computer Emergency Response Teams the right answer? Does India need a cyber crisis management plan? Is mandatory regulation the answer? How does cyber law need to evolve? Can public-private partnership projects be the answer to assess internal capability and the way forward? And what can be learned from the experiences of other countries?

Chair

Tobias Feakin, Director, Australian Strategic Policy Institute, Australia

Panellists

Gulshan Rai, Director General, Computer Emergency Response Team, India

Yoko Nitta, Principal Researcher, Japan Safe and Security Crisis Management, Japan

Andy Cheadle, Chief Engineer, Communications Solutions Division, BAE Systems Applied Intelligence

Sherif Hashem, Vice President, Cyber Security, National Telecommunication Regulatory Authority, Egypt

Session VIII - Privacy Is Dead?

The debate around surveillance, privacy and big data is binary. On the one hand, with data collection and analysis capacities increasing the world over, human rights are routinely abused under the garb of national security and better governance. On the other hand, there is belief in the power of big data to do good by solving many of the world's problems, such as public service delivery and policing and security. The questions that must be asked are: Is the right to privacy fundamentally threatened in the digital age? Can we harness big data without infringing on rights of individuals? How are different societies responding to this new-age duality?

Chair

Mahima Kaul, Head, Cyber and Media Initiative, Observer Research Foundation

Panellists

Sunil Abraham, Executive Director Centre for Internet and Society, India
Siddarth Verma, Managing Director, Corazon Systems, Australia
Karsten Geier, Head International Cyber Policy Coordination Unit, Germany
Gerrit Jan Zwenne, Professor, eLaw@Leiden, University of Leiden, Kingdom of the Netherlands

Session IX - Norms Of Cyberspace

With the number of incidents of international cyber crimes and attacks on the rise, a need to talk about norms of behaviour in cyberspace has been felt globally. Many efforts are underway to determine the contours of state responsibility, which would include taking action against non-state actors operating from their countries. This session will explore the 'norms' that have been suggested by the global community.

Chair

C Raja Mohan, Head, Strategic Studies, Observer Research Foundation

Panellists

James Lewis, Senior Fellow and Director of the Strategic Technologies Program, Center for Strategic and International Studies, USA
Alok Prasad, Former Deputy National Security Adviser, India
Patryk Pawlak, Senior Analyst, EU Institute for Security Studies, France
Joris Larik, Senior Researcher, Global Governance Program, the Hague Institute for Global Justice, Kingdom of the Netherlands

Session X - Preparing for Cyber Conflict: Is It Inevitable

With many countries agreeing that the laws of armed conflict apply to the cyberspace, the question becomes one of extending these agreements to a specific cyber context. Should the response to a cyber attack depend on the effect it has on a country instead of the weapon used? Can the principle of state responsibility be extended to cyber attacks, or will smaller states feel threatened by the bigger powers? What are the rules in a situation just short of war?

Chair

Sean Kanuck, National Intelligence Officer for Cyber Issues, USA

Panellists

Gabi Siboni, Senior Research Fellow and Director, Military and Strategic Affairs and Cyber Warfare Program, Institute for National Security Studies, Israel
Suleyman Anil, Head, Cyber Defence, Emerging Security Challenges Division, NATO
John C Mallery, Research Scientist, MIT, USA
Ian Wallace, Visiting Fellow, Cyber Security, Center for 21st Century Security and Intelligence, Foreign Policy Program, The Brookings Institution, USA

Session XI - Emerging Powers & Internet Governance: Looking Towards 2020

With over 600 million internet connections expected in the next six years, how does India see the development of this digital space? The Chinese and the Russians have created their own critical infrastructure – indigenous root systems – and are capable of protecting their digital space. Should the emerging powers also seek to create a degree of internet independence? Or, must India seek to find a pole position in the international order? How will India respond to the debate on data protection – is localisation the optimal question?

Chair

Samir Saran, Vice President, Observer Research Foundation

Panellists

Rajan Mathews, Director General, Cellular Operators Association of India
Uri Rosenthal, Special Envoy, Global Conference on Cyberspace, Netherlands 2015, and former Foreign Minister, Kingdom of the Netherlands
Fernanda Crespo, Intelligence Analyst, Fundação Getúlio Vargas, Brazil
James Lewis, Senior Fellow and Director, Strategic Technologies Program, Center for Strategic and International Studies, USA
Christopher Painter, Coordinator for Cyber Issues, US Department of State

Inaugural Address by

Mr. Ravi Shankar Prasad

Hon'ble Minister from the UK, Mr. Sajid Javid, Mr. Sunjoy Joshi, my good friend Samir, eminent journalist Ashok Malik, ladies and gentlemen, excellencies. I know of the great work ORF is doing in India, promoting a positive image of the country. Last year I met Samir and I asked him what projects ORF is involved in. He mentioned this whole cyber event they organised last year, and it was very enlightening to know the results of the conclave. But I never thought, not in my wildest dreams, that I, as the Communications Minister, would get the privilege of inaugurating the next session of the same cyber conference. Good luck, Samir. Sunjoy, I am not going to begin with Shakespeare or any such thing because I think it is important to recognise the in-house creativity of the digital world, which is by itself too enormous.

I had the privilege and honour of being a minister in the previous NDA government headed by the legendary Shri Atal Bihari Vajpayee, where I handled the law, information and broadcasting and

coalmines portfolios. When I became the Minister for IT and Communications, I made two comments. I said that if Mr. Vajpayee's government was known for the highway programme - the entire national highway programme commenced in that regime and was a great success - Mr. Narendra Modi's government will be known for the information highway. The phrase clicked and was picked up. The second thing I said is that India is sitting at the cusp of a big digital revolution and we have to make it happen. When I became the Minister I asked how many mobiles we have and I was told the number is more than 900 million. The internet users: 325 million. In the rural areas, internet users numbering 72 million have risen to 85 million as of June 2014. Our IT sector accounts for 38 percent of India's services exports. Indians have become highly newsy people. When I was the I&B Minister I promoted, as Samir rightly pointed out, the opening up of the television sector. We have about 600 to 1,000 channels in the Indian sky. We have 245 24x7 news channels in different languages, which keep on blaring sense, and at times nonsense, but which we have to tolerate in a democracy. I had the privilege of initiating the liberalisation of radio - the FM channel revolution - and today we have 275 FM channels in India besides the All India Radio, whose reach is nearly 99 percent of India. Then there's the internet - India's Google, Facebook, and the fact that smartphone consumption outside USA is perhaps the highest in India.

This being the scenario, the foundation was already ready for a digital revolution. Samir, you mentioned my involvement in the Vajpayee government in opening up mobile telephony; here is one particular image of how, if you provide the platform, Indians learn to use it - and at times overuse it, short of abuse. I had gone to Chennai, and I saw a photograph in a newspaper where a fisherman had gone fishing with his vessel and was using his mobile phone to know the rates of the fish in the market. Those priced well, he was keeping in his vessel, and those which were not, he was throwing back in the sea. Here was one power of technology he was using. A second instance is all the more interesting. We have a news channel, India News, whose anchor Mr. Rajat Sharma is very popular, and he told me a very interesting story.

Whenever he used to return to his home in Greater Kailash from his studio at night along with his wife, he would find one of his staff sitting on a motorcycle in front of a particular house and playing with a smartphone. On the third day, he asked why. His wife said, "Very simple, the Wi-Fi connection before that house is the best one available and he uses that to see Brazil's football world cup." This is India.

Indians are very adept at incorporating technology. Narendra Modi, our prime minister, himself being very tech savvy - in fact, he went digital in a modest way in the 1990s itself, and he is one of the most followed political leaders of the world today as you all know - he has started certain programmes, and I am looking forward to seeing how governance challenges are tackled. What exciting times we are in! We launched the portal MyGov, where we sought suggestions from the people of India on issues like infanticide, child rights, Ganga cleaning, environmental issues, etc., asking for concrete suggestions as to what they would do. Within a short span of a fortnight, we received 200,000 suggestions along with many videos. There is a dedicated team of the Prime Minister's Office interacting with them and also disseminating messages to various departments. 15th August is the Independence Day of India. I asked the citizens on MyGov to design e-greetings

from the Prime Minister of India; in a week, there were 3,000 suggestions. We picked out three and the Prime Minister ended up sending four million e-greetings to the people of India.

We talk of financial inclusion, so we decided to launch the programme Jan Dhan Yojana. The name of the programme was also suggested by people. On 27th September we held 77,000 small and big functions in India and we ended up opening 14 million accounts in one day, and those with mobile phones got 5,000 rupees overdraft facility and 100,000 rupees insurance cover. Further, in a week's time, new bank accounts being opened for people below the poverty line went up to 40 million. When we involved the people, and they realised the Prime Minister was doing something for them, they collectively deposited 20 million in a short span of a month. These cases clearly showcase how we can leverage technology.

In the quest of governance, there is one more issue we are following up on. While we have an India which is an aspiring India, a rich India, a middle class India, we also have a poor India, where children are lost. We thought about how to leverage technology to locate lost children. We are going to very soon launch a portal whereby information will be available on lost children as well as their photographs; with the application of technology, we can help parents locate their lost children.

Hardly a week ago the legendary Mark Zuckerberg came to meet me. I had a wonderful meeting with him. I asked him, "What is your age?" He replied, "30." "When did you found Facebook?" He said, "19." I put my meeting with him on my Facebook page with a comment, 'Friends, let me share on my Facebook page my meeting with the legendary Mark, the founder of Facebook,' and within a short span of three hours I had 700,000 likes on my Facebook. This is a different India. This is a different world.

This Digital India programme emerged from there, to bridge the divide between rural India and digital India. The Prime Minister's mandate is very clear: We have to reach every nook and corner of India through broadband and through the best technology possible in the field of IT. The Prime Minister has coined the phrase 'IT + IT = IT': India's talent plus information technology is India tomorrow. That is the message he has given for which we have to work towards. The second formula is the 3Ds of democracy, demography and demand: We have to leverage this 1.25 billion plus capacity of Indians in an open space of democracy with the power of demography – 65 percent of India is 35 and below; 50 percent is 25 and below - the question is how we can leverage this power. The third formula is the 3Ss - speed, scale and skill. How can we use all three? With this larger architecture in mind, the Digital India programme has been conceived and the idea is to have digital infrastructure available for all the citizens of India, government services available on demand and digital empowerment of Indians. We have got 140 percent penetration of mobile phone in urban areas while in rural areas it is only 44 percent; we have to bridge this divide. We have to also ensure proper e-governance, and we have to ensure electronic manufacturing in India, which we are lacking.

In India, our understanding is very clear. If Indians are given the platform, they have a great knack to use it. Young people love new gadgets, but for me, the best trophy of empowered IT India is

when an 80+ granny understands the meaning of a missed call. She may not be literate, but she knows she has to respond. That is the power of India. We wish to reach all the gram panchayats in India, the clusters of villages which will reach over 250,000 in number in the coming three years. Then we wish to take it further, with a government user network, and we also want to involve private players in detailing, etc. I see great potential for e-education, e-health and above all, e-commerce. Aspirations in both rural and urban India include having access to affordable, reasonably good things available; surely, Digital India is also a platform for this.

Our Prime Minister has given us a mandate: 'I want to see the government available on mobile phones.' It is a very simple sentence but carries a lot of meaning. Today, we can book our trains on our mobiles, check the weather forecast on the mobile and access a lot of other information through various applications, which are being used to empower India and Indians. Let me given another example, again from rural India. One of my juniors, when I used to practise law, was from the state of Madhya Pradesh and she had a taste for the wheat, rice and other pulses from her own state. She used to buy them from a small grocery shop owner in a rural area in Madhya Pradesh. One day she told me about a very exciting happening. She saw on her mobile phone, in WhatsApp, the receipt of the grains which that small shopkeeper had booked in a goods train. There was the number of the train, the bogey number, the station in Delhi at which it was going to reach, when it would be likely to reach, the receipt for the goods delivered and his bank account details for money to be electronically transferred.

Now, kindly see, a simple shopkeeper in a rural area is now using the power of technology for commerce. There was no training. What we need to do is to 'polish' this process. Digital India is basically designed to improve the technological potential of Indians, and in that I see immense potential for expansion of the entire IT architecture in India - enormous jobs, potential for commerce, potential for appliances and potential for local and world players to enter India. When the Prime Minister says 'Make in India,' even outsiders can make in India, supply in India and also export outside. Use the finest talent available here. The Prime Minister is every keen on this, and we are pursuing it. I am very happy that lots of improvement is going on. The governance, the certificates, the information, public delivery - all should be available online. People are using these tools in farming and local education. This enormous potential is going to be properly channelised in the umbrella programme of Digital India, in which we propose to invest $21 billion. That is indeed a game changer. With this kind of architecture, ladies and gentlemen, surely security becomes important.

This is a world which is virtually without boundary. It is a world which is also about living anonymously. Anyone can reach anywhere. Terrorism is indeed a very serious issue. When we talk of cyber security-related issues, in the year 2004 we had only 23 incidents. Last year we had 72,000 incidents. We hear reports as to how cyber attacks are done to completely immobilise the financial infrastructure, immobilise the other information infrastructure. These are challenges we have to face. I wish to share something very sensitive with you. Last year, in my own state of Bihar, the Prime Minister, then as Chief Minister of Gujarat, was holding a rally. Nearly a million people had come. Some terrorists decided to disrupt it. 80 people were injured and about eight died. We were

sitting on the dais. We could see the bombs being exploded. We tried to contain the crowd. One of the suicide bombers, who had larger designs, was caught while strapping on the explosive; it exploded and he died. His pen drive was confiscated by the police. The security people in my department showed it to me, it was in an encrypted form, they decrypted it, and I was amazed to find how many photographs of what they wanted to target had been stored in the pen drive, including four photographs of me. I never knew I was so important. But that is the hard fact. Today, how I see it Mr. Minister, the internet, mobile phones, the new media is one of the finest inventions of the human mind. It is indeed a game changer. Why should a few be allowed to abuse it to destroy humanity? I see it in larger context and larger perspective and therefore cyber security by itself becomes of critical importance. How do we see it? Are we ready for it? Are we prepared for it? Are we committed to ensure a proper regime? I would like to highlight some of the issues which are very important to be flagged: Do we have the technical and legal architecture available to identify the perpetrators and the sources of attack? Do we have any international mechanism for sharing of information, and determined action against perpetrators? This unhindered growth of networks of infected computers across the world - how do we propose to address this problem in the absence of global cyberspace norms to regulate and guide responsible behaviour in cyberspace?

There are many issues. I am only flagging the few which must concern us as policymakers. We in India are very clear that we need a proper framework for internet governance, which must be inclusive, which must be democratic. I am happy, Mr. Minister, to hear you say that the exchange on the internet should not have only one particular mind-set. It cannot be. Global can never become meaningful unless it is linked to the local. That is how I see it. The internet may have been invented by a particular country, but is today the property of the world. It is the heritage of humanity powered by diverse innovations from every part of the world. All should be welcomed, all should be made a stakeholder. That is the approach of Government of India as far as the issue of ecosystem is concerned. Now, if the internet is owned by the global community, is it not important that we must make collective effort to ensure it is not manipulated or misused? And this is not only about terrorism. I remember, at one point in time, rushing to an airport to catch a flight and finding out, to my dismay, that the flight system had failed and everything had come to a stop. There was some problem.

Suppose some extremist or terrorist tries to manipulate the system and ensures that the entire information system of the world itself comes to a grinding halt - what will be the consequences? Therefore, there is a great need to have a proper ecosystem and proper framework whereby there is meaningful cooperation followed by prompt action under defined norms against those who seek to manipulate the system. It is very important that information is properly shared and it is equally important that there is a mechanism of accountability in place with respect to crimes committed in cyberspace, so that the internet remains a free space for universal well-being. These are some of the larger issues I would like to flag. Yes, we remain committed. As a Minister of the Government of India, let me assure this international gathering today that India is willing to take the extra step as far as the evolution and stabilisation of these frameworks are concerned.

There is one last issue I would like to flag. If the internet is the property of the world shared by the human race, if the global has to have a strong linkage with the local, it is equally important that local cultures be reflected on the internet. I told people in my department to ensure that various Indian languages are equally reflected online, especially simple languages like Hindi, English, Tamil, Telugu and Malayalam. In a similar way, the new media, the social media, which has become a powerful tool - this powerful mechanism, one of the finest inventions of the human mind, must also give respectful platform to various cultures of the world, be it Asia, Latin America, be it Africa, and not only Europe and America. That is how I see it. If that happens, then this whole mechanism, which I say is a game changer, will be really serving the needs of the people of the world and every country.

The last take I have is that there is something we owe to the posterity of the world - a safe internet which is always useful for people and geared towards growth in a constructive way.

These are some of the larger views. Samir, thank you for giving me the platform so I could share my views with all of you. Namaste.

Keynote Address by

Mr. Sajid Javid

Thank you very much and good morning,everyone. Sunjoy, thank you very much for your remarks as well, your very thoughtful remarks. You've made me remember that when I was appointed the Culture Secretary in Britain, the media started to report that I was a Star Trek fan and they were wondering whether I enjoyed Star Trek more than Shakespeare. So, I think Sunjoy understands the importance of Star Trek, but in any case it is a real pleasure to be here in India, a country that, as the Communications Minister Ravi Shankar Prasad has recently observed, is at the cusp of an IT revolution. India is a proud nation, a very great nation and it is a nation that stands to become even greater still, thanks to the incredible power of the internet. The World Wide Web is without doubt the greatest technological success story of the modern world. Just as Britain's inventors powered the world wide industrial revolution, so it was that the British genius Sir Tim Berners-Lee ushered in the global digital age. The ability to get online has completely transformed the way billions of people live, work and learn. It allows us to build communities across borders,

trade with customers in distant lands, and to instantly share ideas with friends and strangers around the world. These benefits have been felt already by hundreds of millions of Indians. Only China boasts more internet users than India. Prime Minister Modi had used the social media to revolutionise the way politicians in the country communicate with a vast electorate. And the Digital India plan is set to change both the face and the profile of India for years to come. Yet around 80 percent of Indians are not regular users of the internet. Worldwide, more than 60 percent of people have never ever been online, not even once. That is four billion people who are missing out on the opportunities of the Web, four billion potential customers missing out, for example, on what Indian businesses have to offer.

But as we have heard, the situation is already rapidly improving. Internet penetration is growing at a phenomenal rate. The web is becoming even more open to different languages and non-Latin scripts. Every year the number of users increases by 10 percent and by an incredible 40 percent in India. In the past decade alone, almost two billion people worldwide have gained access to internet for the very first time. Earlier this month McKinsey predicted that an extra 900 million people will be online by 2017. But that will only happen if the previous explosive rate of growth continues. That, in turn, will only happen if the internet retains its freedom to grow and evolve across national boundaries - and that is why continued collaborative internet governance is so important.

Before going any further I think I should make it clear what I mean by internet governance. It is one of those phrases that journalists and politicians have been throwing around a lot recently. It is good, I think, to be exactly clear on what is meant. When I talk about internet governance and when the UK government talks about internet governance, I mean the definition that was agreed at the World Summit on the Information Society. Let me just quote that definition: "the development and applications by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." The way that should be put into practice, I think, is best expressed by the principles that were agreed in Brazil earlier this year at the global multistakeholder meeting on the future of internet governance, NETMundial. These principles were not put together by politicians, they weren't drawn up by the bureaucrats at the United Nations or the ITU, they weren't imposed by civil servants in London or in Washington or in Delhi, but were created in the open by the community that supports and curates the internet - the people without whom 'online' would simply not have been possible, the people who have the best possible grasp of both the challenges facing the internet and the means required to tackle them.

The principles agreed upon are as robust as they are simple. Internet governance should be built on a fully inclusive, multistakeholder process, one that ensures the meaningful and accountable participation of everyone involved. Decisions should be made in a bottom-up, open, consensus-driven way. There should be a suitable level of accountability with mechanisms for checks and balances as well as for review and redress. Anyone affected by an internet governance process should be able to participate in that process. I am proud to say that the UK government wholeheartedly supports the NETMundial principles as a basis for the global internet governance frameworks and I would urge our Indian friends to do the same. After all, what is the alternative:

Top-down, centralised decision-making, a bureaucratic World Wide Web full of red tape, cyberspace divided by firewalls and virtual fences, and the internet being run not out in the open by the people who make it work but behind closed doors by horse-trading politicians?

Just imagine: An internet relying on governments agreeing on things. Internet governance has to match the rapid change experienced by the internet itself, but let's face it - rapid action and inter-governmental agreement are not concepts that generally go together, and a fragmented locally managed internet would be bad for business too. India is already a global technology hub with outstanding skills and a base in IT and communications. Companies such as TCS, Wipro, Infosys are world leaders in their fields. These firms and many others besides rely upon free, unfettered access to a global internet market place to thrive and to trade internationally. If we were to restrict the online world by moving to a model of governance based solely on discussions between governments, we could quickly find ourselves with an internet that is broken up into regional blocks and an internet that is no longer truly global. If that happens, the financial implications for some of the most dynamic and most successful companies would be very damaging.

But I don't want you to think that national governments have no role to play in internet governance. Of course we do. We are one of the multistakeholders, after all. We have to ensure that the internet does not become an online version of the Wild West, a dangerous place where honest people cannot feel safe and secure. The law must apply online just as it does offline. Governments cannot deliver that by simply throwing up barriers and fragmenting the internet; working together, however, we can take a lead in the promotion and delivery of effective cyber security. As the global internet economy grows, so do the risks posed by cyber criminals. In the UK we rank computer-based attacks alongside international terrorism as one of the biggest threats to our national security. It is a problem that must be tackled. If the world is going to fully realise the benefits of the online age, the internet needs to be open, yet secure. We need to know that we can communicate and transact safely. That is why in 2011, the UK government published its first cyber security strategy. It supports economic prosperity, protects our national security and safeguards the public way of life by building a more trusted and resilient digital environment. The strategy is being delivered with almost one billion pounds of government money and is another example of the multistakeholder approach in action.

Here is another example, our Cyber Essentials scheme. Developed by government, industry and academia, Cyber Essentials lets any organisation, large or small, British or overseas, demonstrate that they have the key technical controls in place needed to counter the most common online threats. It is a great opportunity for companies around the world to demonstrate to their customers that they take cyber security seriously. With 70 years of experience in information assurance and worldwide reputation for excellence in its field, it is no surprise that the UK's cyber security sector is going from strength to strength. It expanded by 22 percent last year, including 80 million pounds of exports to India. That is the highest growth rate in the global list of 53 economies and it means we are on track to hit two billion pounds of cyber security exports by 2016. Now, once again, this is down to the multistakeholder approach, which brings together government, industry and academia so they can work together in cooperation rather than in competition. We are more than happy to

share with the world so that other countries can join the multilateral fight against cyber crime. That is why the UK government was delighted to co-fund this event, giving stakeholders from both of our countries a chance to discuss solutions to the challenges we all face.

But you must not be lulled into thinking that cyber crime is just about hacking or online fraud. From terrorists to stalkers, an insecure internet is a rich resource for those who seek to harm others. Later this year our Prime Minister David Cameron will be hosting an international summit on tackling the online sexual exploitation of children. It is a great opportunity for world leaders to come together and confront these criminals, and I look forward to India taking part. We must ensure the internet is safe, secure and successful, but we cannot allow that to be an excuse for further government control of cyberspace. The multistakeholder model, both for governance and security, is the single best solution to this challenge. It will allow the internet to survive and to thrive, providing unlimited benefits to countless individuals and businesses. India is uniquely placed to show the world just how well this approach can work. It is the world's largest democracy, the third largest economy in Asia, home to a rapidly expanding digital community that has a phenomenal potential for future growth. With a new government, a booming private sector and a vibrant civil society, there has never been a better time for India to embrace the multistakeholder approach that already serves the internet so well. ICANN's Fadi Chehadé has called the internet, and I quote, "the greatest public gift." He is absolutely right. It does not belong to anyone; it is not controlled by anyone. The internet itself has endured and expanded precisely because it is bigger than any one country, and there should be no barriers in cyberspace. Thank you.

Cyber Lawfare: The contest over Territory and Jurisdiction

Chair

C. Raja Mohan, Head, Strategic Studies, Observer Research Foundation, India

Panellists

- **Sean Kanuck**, National Intelligence Officer for Cyber Issues, USA
- **Jamie Williamson**, Head of Unit, Relations with Arms Carriers, International Committee of the Red Cross
- **James Lewis**, Senior Fellow and Director of the Strategic Technologies Program, Center for Strategic and International Studies, USA

The internet, the network of networks, might be considered a global commons by many nations, but the infrastructure that runs it certainly has roots in specific countries. The first issue is the tension between the notion of sovereignty and the fluidity of cyberspace. There was a notion that

was once in vogue that the internet would usher in an era where states did not matter and individuals could operate freely. In a sense, that was a libertarian, utopian vision.

That sense of the cyber domain is now in the past.

Cyberspace has a huge physical infrastructure of servers and cables and satellites, not all publicly owned. The internet has significant economic benefits and disproportionate effects in the physical world. Capital has interests, and capital will defend those interests.

The state has struck back on a number of issues such as protecting intellectual property rights, national cyber defence against foreign threats, content regulation and cyber crime. The state also plays a large role in managing the physical infrastructure of the net. All this is complicated by disagreements not just between states but also within states. Much of this has to do with how people view notions like privacy, and also the nature of the relationship between the government and its people.

The Snowden revelations have had a varied impact on the nature of this debate. They highlighted many of the issues of cyber snooping and privacy and made people realise their individual stake in these debates. Individual freedoms had been challenged. The revelations also gave an impetus to a more general discussion on issues like data localisation, privacy and internet governance. That said, the Snowden affair merely gave more exposure to debates that had already existed. The question of how to design a new, contextualised system still remains.

India has made attempts to overcome jurisdictional issues in cyberspace, for example through provisions in the Information Technology Act of 2000 which extend to offences committed outside India by people of any nationality, if an Indian computer network is at all involved.

In 2013, India's Minister for Communications and Information Technology at the time, Kapil Sibal, said that if the effects of a cyber crime were felt in India, or if it dealt with Indian subject matter, then India should have jurisdiction over the case.

India's courts have followed the effects-based approach to determining jurisdiction between states in India, in the Banyan Tree Holdings case, which could be applied to international transactions as well...

At one point of time there was talk of an international treaty on lawful access to communications, because of the assumption that every country snoops on communications. However the fundamental nature of espionage makes it resistant to regulation. The idea of a treaty was dropped also because it was too difficult to reconcile countries' differing views of jurisdiction and internet sovereignty.

This time, however, it cannot be dropped so quickly because the economic stakes of the internet are so huge.

Spying on one's own people is a completely different ballgame in democracies which value freedom of speech and privacy. Questions are asked about the gathering, storage, usage and security of information – and whether or not due process is being followed. The reason for this concern is that

...Banyan Tree clarified the legal position, holding that "Insofar as the position in this country is concerned, there is no 'long arm' statute as such which deals with jurisdiction as regards non-resident defendants. Thus, it would have to be seen whether the defendant's activities have a sufficient connection with the forum state (India); whether the cause of action arises out of the defendant's activities within the forum and whether the exercise of jurisdiction would be reasonable." (Banyan Tree Holdings Limited v. M. Murali Krishna Reddy and Anr, CS(OS) 894/2008 (High Court of Delhi, 23rd November 2009), para 9).

The Delhi High Court ruled in World Wrestling Entertainment, Inc v M/S Reshma Collection that trademark and copyright-related e-commerce cases would have jurisdiction based upon the location of the buyer.

human rights are universal values – even though some countries pretend they have no international obligations on this score. That said, the 'control' argument must not be dismissed as totalitarian overreach. The fact today is that there is a crying need for identification and attribution in cyber crime, which necessitates control of some kind – especially with regard to identification measures.

Consequently, notions of sovereignty move very naturally into cyberspace. States whose prime responsibility is the safety, security, and prosperity of their citizens obviously must extend that responsibility to cyberspace. National networks are subject to domestic laws. What is less obvious is how to deal with the extra-territorial application of domestic law to a global internet and the balancing of international commitments.

One of the biggest dilemmas that the internet poses is between political stability, dependent in some cases on firewalls, and economic opportunity – which requires freedom of cyber movement. The reality is that no country will cut itself off from economic opportunity and so no country – except possibly North Korea – can afford to island itself. Self-interest may very well be the key to the preservation of interconnectivity.

Cyberspace cannot be classified as a 'commons' under the traditional definitions of either international law or political economy. Cyberspace and its parts were invented and they carry intellectual and other private ownership rights, unlike, say, outer space.

A two-speed approach could emerge, where civil agreements take longer, but security-related issues see pockets of convergent opinions translate into more rapid action.

One issue here is that differences in notions of things like states' rights and privacy have much to do with the Westphalian notion of sovereignty, which western nations moved away from after the Second World War. This has led to a strange situation where human rights trump sovereign rights – which not all countries agree with.

How do countries benefit from the economics of the internet but manage its political fallout? The Danube model is germane in this context. The river crosses many countries and for the mutual benefit of everyone, the river system is governed by an agreement between all the riparian states, while their sovereign laws apply on land.

Since common sets of rules have been established for trade and finance, it should be possible to create one for the internet. However, common rules are premised on the basic idea of a level playing field for everyone – domestic or international.

The rising prominence and sophistication of non-state actors adds complexity to the equation. They have grown from thugs with guns to actors with expert knowledge of cyber vulnerabilities and a flair for propaganda.

Does the responsibility to protect people from these actors lie at the point of origin or at the terminal point of attacks? This is further complicated by the existence of sub-state actors which are used by states specifically to benefit from the disruptive actions of these players, while disavowing responsibility. A standardised set of norms and rules is needed.

Some of these conundrums may in fact be unsolvable. The rapidity of technological progress means that laws, which are fundamentally reactive, will not be able to keep pace with it. However, the speed of innovation now means we have to give up notions of regulation and control, and instead focus on making the internet as safe and fair as possible. This will become more difficult as serious synergies, such as those between information technology and biotechnology, progress.

The Director of the Central Bureau of Investigation identified multi-jurisdictional cyber crimes as one of the "biggest global challenges confronting all…nations".

In order to retain full control over government communications data and to increase security, all Indian government offices can only use official emails provided by the National Informatics Centre, as per the Government of India's Email Policy.

Cyber forensics, which is critical for attributing cyber attacks, is a growing field in India, through government efforts at the Centre for Development of Advanced Computing and private efforts like EY's Cyber Forensics and eDiscovery Centres.

One solution then could be a principles-based approach as opposed to a rules-based approach. A successful example in the field of weaponry is Article 36 of the first Additional Protocol to the Geneva Convention. It requires that new weapons conform to the principles of international law, and places the responsibility of ensuring this on the state developing the weapon.

However one must keep in mind that even principles-based agreements can have limitations—as the issue of data shows. While data by itself may be the property of one sovereign state, its effects may have extraterritorial implications. This is where another country will claim the right to regulate such extraterritorial data. As a result, while principles-based systems may work in some cases, increasing jurisdictional disputes seem inevitable. A likely result will be several agreements between various collective action groups based on their respective interests and where they lie on the political stability-economic prosperity dilemma, rather than one agreement.

The Digital Nation: Is Social Media Disruptive or Democratic?

Chair

Ashok Malik, Australia India Institute - ORF Chair for Indo-Pacific Studies
Observer Research Foundation, India

Panellists

- **Raheel Khursheed**, Head of News, Politics and Government, Twitter, India
- **Wajahat Habibullah**, Former Chief Information Commissioner, India
- **Barkha Dutt**, Group Editor, NDTV, India
- **Karuna Nundy**, Advocate, Supreme Court of India, India

Although individuals, corporate houses and governments have embraced social media, it is increasingly the first casualty when there is a law and order problem. Countries are being blamed for 'scapegoating' social media. But is it the hard truth that social media needs regulation? And what does this mean for freedom of expression in the digital age? In India, opinion on the role of social media varies. The role of the government has been questioned and a dichotomy among opinions

has emerged. Many hold the view that government structures are indeed extremely uncomfortable with social media and freedom of media/expression. However, others are of the opinion that the government does indeed support social media, and that government participation is vital to social media, and vice versa, for democracy. During Prime Minister Modi's election campaigns, many highlighted that the emphasis was on inclusion, and that there was a greater acceptance of social media as a mode of communication in governance. It is also believed that the current government understands that rather than regulating social media, it can be included in governance.

Furthermore, the objective of the law is to promote public participation in government and make democracy a truly participative one. In order to achieve this, there can be no clash between democracy and social media. The introduction of the Right to Information Act has given the citizen the power to question.

The objective of this law is a form of governance which seeks to promote transparency and accountability in such a manner that it becomes inclusive and citizens become participants in governance. The RTI also seeks to correct discrepancies created due to bureaucratic caveats. Situations have, and can, arise where civil servants refuse to part with information. Various government ministries may also release differing reports because some departments are willing to part with information, and others, not so much. The RTI, by lending transparency to the system, seeks to rectify the issues at hand. In such a situation it can be understood that social media is by no means in conflict with transparency in the government.

On issues related to social media, the role Twitter has played is extensive. Many are of the opinion that Twitter's purpose is to provoke individuals to fight with others. Yet it is evident that Twitter can also provide a platform for direct engagement between people of this country and the government. By bringing government mechanisms and citizens on the same platform, it gives people access to important conversations on policymaking, as well as provides them information on detailed activities of the government.

This has led to global empowerment of citizens in conjunction with two trends – the information hierarchy being broken down, and information being democratised. A few years ago people would not have had access to this information, but conversation is now two-way. Additionally, Twitter also serves as a platform for data collection as well as information exchange during national disasters, such as during the Jammu and Kashmir floods or the Andhra Pradesh cyclone. As evident from these recent examples, it has also become an important tool in the collection of relief aid.

India is one of the world's largest social media markets, with well over 100 million active users of social media platforms; India is Facebook's second largest user base after the USA.

India's Prime Minister, Narendra Modi, is an active tweeter and is one of the most popular personalities on Twitter, with 10.8 million followers for his personal account and 5.3 million followers on the account of his office.

Social media was widely credited with playing a large role in the election which brought PM Modi to power – in the five months leading up to polling more than 58 million tweets on the election were exchanged.

Government officials have embraced social media as a way to deliver news and updates to their constituents. At the time of the Modi government's formation, nearly 90% of its members were on social networking platforms.

In late 2014, a series of floods hit the Indian state of Jammu & Kashmir, crippling phone networks. Social media quickly became active, with the hashtag #KashmirFloods centralizing information and providing vital lines of contact.

The Indian army based many of its rescue efforts on information obtained through platforms like Whatsapp, Facebook and Twitter.

Another contentious issue is whether social media is, can be held responsible, for triggering violent protests and riots.Kashmir in the 1990s was plagued by insurgencies that were spread by lack of communication and violent rumours. In recent years, riots have actually been sparked off by the internet – there have been such cases in Bangalore and Pune against citizens of India's Northeast. In such cases, understanding if channelling the role of social media would have alleviated the situation is a difficult task: It is not easy to say whether social media would have promoted peace or exacerbated terror. However, what is clear is that in such situations social media would have made it much easier to mitigate doubts and complaints.

Journalists address the issue of social media from a different angle. They can crowdsource ideas from social media. Has social media helped or hindered their work? The answer is both yes and no. Social media is beneficial for journalism due to the fact that sometimes, what can be learned from browsing Twitter for half an hour cannot be got from reading 10 newspapers. Consumption has become curated. More ideas can be brought forth, many of them new, and young voices can be discovered and heard more easily. Also, social media enables more people to air their opinions and concerns, which is a welcome challenge for journalists, as it ensures they do not get jaded or too predictable. Success in the media also tends to be measured by the number of online hits an article gets.

In India there is also a tendency for political discourse on social media to get personalised. This happens because Indian political debate is getting more and more polarised. Social media in India reflects an amplified version of Indian society. For women, social media can be both a threat and an opportunity. Misogyny exists everywhere, and women are easy targets on social media as well. They are scrutinised and teased on social media, just the way they are in daily life. Also, the sort of attention and aggression that social media allows can be quite problematic, since this aggression sometimes takes the form of physical threats. (There have been cases of rape threats online.)

However, with women becoming more visible and proactive at workplaces, and internet penetration increasing significantly over the years, both women and men need to be online. Also, women from traditionally more conservative societies that restrict their presence in public spaces – Egypt, Iran and Libya – view social media as a means to express themselves, and gain a voice.

One issue remains unresolved. Is social media important enough to be treated like other media? Should it be subject to the same measures of gate-keeping as other forms of media? Section 66A of the IT Act is a provision that criminalises and renders liable for prosecution speech that is annoying or inconvenient. However, what exactly is annoying or inconvenient has remained undefined.

Given the speed of the internet and the slowness of Indian courts, a completely unregulated internet is also problematic (for instance, cases of child pornography). The sheer speed of the internet makes it difficult for the law to keep up. Technology moves and innovates extremely fast. In courts, judges are struggling with this problem and are finding it difficult to get into the complexities of the situation.

Similar efforts have been made both in advance of and in the aftermath of natural disasters, like Cyclone Hudhud which struck the state of Andhra Pradesh.

The speed of social networking has had negative effects as well in India, such as in Bangalore in 2012 when social media rumours of imminent attacks on people from the country's northeast forced thousands to flee the city.

Social media in India has been regulated by the Information Technology Act, 2000, particularly section 66A, which punishes the electronic sending of offensive messages.

Section 66A is being challenged in the Indian courts amidst claims that it violates the fundamental right to free speech and expression.

Section 66A was challenged in the Indian courts amidst claims that it violates the fundamental right to free speech and expression. India's Supreme Court struck down the Section in March 2015, calling it "unconstitutional".

Counterterrorism in Cyberspace

Chair

Marc Porret, Legal Officer, Counterterrorism Committee Executive Directorate (CTED), the United Nations

Panellists

- **M.M. Oberoi**, Director of Cyber Innovation & Outreach Directorate, Global Complex for Innovation, Interpol
- **Jan Neutze**, Director, Cybersecurity Policy, Microsoft, USA
- **Deepak Maheshwari**, Head, Government Affairs, Symantec, India
- **Rajan Luthra**, Chairman's Office, Corporate Security Expert Services, Reliance Industries Limited, India

In 2001, there were approximately 50 million internet users in the world. Today the number has increased to over 2.7 billion. Studies have predicted an exponential rise in the number of users to around 50 billion within the next 10 years. The rise of digital technologies has undoubtedly

provided enormous economic opportunities, but it also poses a huge security challenge – first and foremost being a massively expanded ambit for attack. Everyday gadgets like computer-controlled lights, watches, refrigerators, even cars – anything utilising a poorly encrypted IP address – is a potential target for attack. The interconnectivity of cyberspace is both its boon and its bane.

Enforcement agencies around the world are facing a multitude of challenges in countering cyber terrorism: From anonymity of the perpetrators and ease of access for terror groups to the gigantic underbelly of cyberspace known as the deep web which is entirely unregulated and highly encrypted. Both domestic and international agencies frequently face challenges of identification, attribution and obfuscation in such domains.

In recent years, social media has emerged as a blessing for terror organisations. Their propaganda machines use it as a tool for external as well as internal communication. These outfits have mastered the use of social media, belligerently utilising it not only for spreading propaganda but for recruiting, training, coordinating and even financing purposes. The recent example in India of the Indian Mujahedeen's use of social media to spread rumours and incite violence against the state highlights the highly successful use of cyberspace by terror agencies. The ease with which social media has been hijacked by unruly elements in society has given rise to a growing sense of defeat within the global community.

In the face of growing social media use in India, law enforcement officials have faced difficulty in tracking those using the internet for illegal purposes.

Digital means have been used to aid terrorists, as in the case of the 26/11 attacks on Mumbai, when the technology chief of Lashkar-e-Taiba, Zarrar Shah, reportedly used Google Earth to show militants the routes to their targets.

Social networking platforms are also used by terrorist organisations like the Indian Mujahideen to communicate and coordinate attacks.

Indians have also used social media to aid international terror outfits; a young Indian man was responsible for running “Shami Witness”, described as one of the most influential Twitter accounts of the Islamic State before his arrest.

However, enforcement agencies have repeatedly emphasised the potential of social media as a force for doing good. An effective way of countering terror propaganda on social media is for the larger society to be more active, and for it to spread facts to counter such propaganda. Simultaneously, enforcement agencies need to enhance their technical enforcement capabilities and react rapidly to such situations. Due to the vast resources at their disposal, government and enforcement agencies could ideally make maximum use of social media as it has the potential to monitor and observe events in real time.

Counterterrorism challenges in the cyber world are further exacerbated by the complexities inherent in a multijurisdictional sphere. While responding to these challenges, enforcement agencies have to maintain a balance between legitimate internet counterterrorism (ICT) and preservation of basic human rights like freedom of expression. They also have to consider the notions of proportionality and collateral damage.

Recruitment over the internet has also been highlighted as a key counter-terrorism concern for India, following reports of young Indians going abroad to fight.

Nevertheless, specialised anonymising software does not appear to be popular – fewer than 10 out of every 100,000 internet users in India uses Tor.

The Government of India is exploring ways in which to use social media to counter terrorism, through de-radicalisation programmes and by partnering with private organisations Prime Minister Narendra Modi discussed such initiatives with Facebook CEO Mark Zuckerberg when the latter visited India.

There is growing demand for the use of the public-private partnership model to counter the growing menace of cyber terrorism, as most of the skills, technologies and information lie outside the domain of law enforcement agencies. There of course exist differences in mechanisms and practices between the private and the public sector, but governments are fast realising the significant capacity deficit within their ranks. Given the current circumstances, governments understand that their ICT goals cannot be achieved without academic inputs and private sector cooperation. Cyber counter terrorism challenges are too broad for any one government to have the blanket interdisciplinary expertise necessary to tackle underlying social and infrastructural issues. Moreover, there exists a strong common will between private players and public agencies to combat these issues through joint efforts.

However, there is currently a trust deficit between governments and private players due to the alleged overreach of governments in seeking private information which goes against the fabric of private businesses. The private sector considers the government to have three basic functions in cyberspace:

1. Governments are end-users of cyberspace
2. Governments have a duty to protect cyberspace and enforce laws
3. Governments have a mission to collect data in cyberspace for security purposes

But due to the heavy handed response of certain governments, private players have added a fourth dimension, which is at the crux of the contention:

4. Governments have become exploiters of cyberspace

Private players have demanded defined processes, warrants and regulation in cyberspace before they provide private consumer information. To circumvent the perceived illegal overreach by governments, private players are increasingly encrypting their data in transit and in between servers to better protect customers' private information from prying eyes. Such encrypted data has made it even more cumbersome for law enforcement agencies as far greater time is being spent in deciphering information, which unfavourably affects their response time.

A major point of contention between civil society and the government has been the issue of attribution and whether it necessarily constitutes an invasion of privacy. Policy experts believe it is in fact the lack of legal safeguards, definitions and processes that has made attribution a direct threat to privacy.

It is widely accepted that the most challenging issue in countering terrorism in cyberspace is dealing with the multijurisdictional nature of the internet. There is an immediate and urgent need for international policies which can make law enforcement easier and more effective. Governments have to strive for greater capacity building in law enforcement and multijurisdictional capabilities to counter global cyber crimes. The emphasis should be on promoting security by design, i.e. designing digital technologies keeping in mind the perceived security concern. The key aspect in reducing friction between private and public agencies is to legally define privacy and develop essential oversight mechanisms to safeguard private data.

In light of the cross-border nature of cyber terrorism, India has made several terrorism-specific cyber agreements with international partners including Israel and the USA.

India extended its support in tackling cyber terrorism to the Shanghai Cooperation Organization, where it has observer status, during a meeting of the organisation's Regional Anti-Terrorism Structure in 2013.

India has also been involved in counter terrorism and cyber security dialogues with the Association of South East Asian Nations (ASEAN), which Indian External Affairs Minister Sushma Swaraj stressed was part of India's Act East Policy.

Rethinking the Global Cyber Market

Chair

Richard Ponzio, Head of Global Governance, the Hague Institute for Global Justice, Kingdom of the Netherlands

Panellists

- **Aaron Kleiner**, Senior Strategist, Cybersecurity Policy, Microsoft, USA
- **Vijay Madan**, Chairman, FICCI Subcommittee on Cyber Security and Chief Mentor, Tata Teleservices, India
- **Jonah Force Hill**, Technology Policy Consultant, Monitor 360, USA
- **Kamlesh Bajaj**, CEO, Data Security Council of India

The internet has revolutionised the way we conduct business today. According to a recent McKinsey report, the increase in real per capita GDP that took 50 years during the Industrial Revolution takes place in a fraction of that time in today's digital world. There is more cross-border trade today than at any other time in history. The global cyber market has established itself as one

of the foremost economic multipliers in the world in a very short span of time. However, the central question is how the economic utility of the internet can be maximised amidst security, privacy and other challenges.

The global cyber market (namely hardware, software and services) has seen a demographic shift to Asia and a subsequent modification of policies. Cyberspace was predominantly a western phenomenon but the rise of the middle class in Asia has resulted in enormous growth in the number of internet users. Countries in Asia have different cultures and thus different internet philosophies – some of which threaten the western 'open values' of the internet.

There are many different levels of internet users, from governments to small and medium enterprises to individuals. The global cyber market needs to constantly cater to all such groups while continuing to remain relevant for all of them at the same time. It is essential for the cyber market to balance various social, economic, legal and security aspects which differ from state to state, making it a necessity for technology and cyber policy to develop simultaneously. There is an urgent need to depoliticise issues of security, privacy and other cyber norms to the greatest extent possible. Glaring privacy concerns and policy gaps in the global cyber market are yet to be addressed,

In 2013, the internet contributed 2.7% of India's GDP, for a value of around $60 billion, outstripping the contributions of the military and healthcare sectors which contribute 2.5%.

By 2020 it is forecast that the internet economy could triple in value to around $200 billion, amounting to 4% of India's total GDP, which is in line with the contribution in more developed economies.

"India is the third country in the world to have over five companies valued at over $1 million," according to Google India Managing Director Rajan Anandan.

E-commerce will form a significant part of the internet's value to India, as it is expected to be worth at least $100 billion by 2020, up from $17 billion today.

The internet is also changing how smaller and medium enterprises (SMEs) do business in India - out of a projected 13 million SMEs in the next 3 to 5 years, 8 million of them will be e-commerce companies.

The internet has the potential to create up to 2 million jobs by 2018. Offline growth is being driven by online growth in India, with initiatives like the government's 'Make In India' project running in tandem with the 'Digital India' programme, providing hardware and other support to online businesses.

resulting in increased disputes between various stakeholders and users.

However, policy creation cannot remain limited to governments because the nature of the cyber market is too multidimensional for governments alone to regulate. It is crucial to involve private players, academics and other stakeholders in developing behavioural norms and policies for cyberspace. The need to balance regulation and business connectivity highlights the importance of public-private partnerships. But this model cannot be restricted to stakeholders of an 'elite' group of countries. It is imperative to include all regions of the world while framing these policies. There is therefore concern regarding the serious economic implications of internet monopolies. Market consolidation is taking place, with smaller companies being subsumed at an alarming rate. These monopolies are disrupting the equilibrium of the cyber market, and could push Asian countries out of the debate. There is apprehension amongst the Asian countries of total domination by American companies resulting in the latter getting seats at the governance table at the expense of others.

Both businesses and governments have identified cyber security as a top priority. Going forward, the development of cyber policies has to include the principle of security within all aspects of the framework. However, the current models of security and surveillance have cast a shadow over the free-flowing nature of the internet. Surveillance is affecting global supply chains – for example,

mass surveillance means that personal as well as economic data is collected, which can then be used to swing trade negotiations in a particular country's favour, thereby disrupting the global supply and demand equilibrium. There is a growing view that such interference – using surveillance to influence global arrangements – should be included within the ambit of direct cyber espionage. Additionally, data sharing is critical to combating global cyber crime syndicates. Current mechanisms, including the mutual legal assistance treaties, are not working, as the processes often take months or even years for information to be shared, stalling criminal prosecutions. In the information age, where data changes easily and rapidly, access has to be quick – and yet it takes up to three years to get information from some countries.

The growth of India's digital markets is also fueling an increase in cyber attacks on those businesses - in 2014, nearly half of all Indian companies had faced a cyber attack of some kind.

The Indian government has increased awareness of both digital opportunities and risks, through the Digital India programme and plans to increase its cyber security budget.

Indian businesses are following their government's lead: 74% of chief information officers (CIOs) recently surveyed said they expected their IT budgets to increase to cover new security risks.

Following the Snowden revelations, there was an unprecedented uproar about surveillance and how countries and individuals should deal with this challenge. One of the most controversial, but natural government responses was to push for data localisation. Governments rely on the policies they are familiar with, which is why they have a tendency to turn inwards. But there is often confusion when it comes to data localisation. 'Fragmentation' is a term used without precision to mean something bad is happening to the internet, whereas localisation is what people are actually thinking about when they say 'fragmentation.' Rather than turning towards data localisation, policies should address the issues which are leading to the demands for localisation to begin with. One of the more widely accepted notions is that content belongs to the user who created it and not to companies or governments. Scholars argue that data localisation does not make data safer due to the globally interconnected nature of the internet, but it does make it more accessible to local law enforcement agencies. Even if localisation does take place, there will be a need for innovative joint ventures, as local companies are not yet equipped to deal with everything that is currently being handled by international companies. Partnerships with those who already have the knowhow and the capacity will thus be useful.

ICANN or ICAN'T?

Chair

Samir Saran, Vice President, Observer Research Foundation

Panellists

- **Latha Reddy**, Commissioner, Global Commission on Internet Governance; former Deputy National Security Adviser, India
- **Yu-Chuang Kuek**, Vice President and Managing Director, Asia Pacific, ICANN
- **Dr. Govind**, CEO, National Internet Exchange of India

The Internet Assigned Numbers Authority (IANA) transition and the restructuring of the Internet Corporation for Assigned Names and Numbers (ICANN) to ensure broader participation has raised very important questions on the evolution of current internet governance. ICANN's attempts to attract broader participation and legitimacy have been undermined by the reality that it

is still located in, and has to respond to the jurisdiction of, one nation, the US. The nature of this transition has raised several concerns. Will large emerging economies and other developing countries allow their interests and investments to be determined by local jurisdiction? Is the transition truly representative and will it make internet governance international? Will the control of the 'root' of the internet be democratised? Will radical ideas, such as India's suggestion to move ICANN functions to the International Telecommunications Union, pave the way forward?

Before focusing on the debate, it is important to understand the exact role and functions of ICANN. It has often been reiterated that ICANN is not an institution that governs all. Indeed, the main responsibility of ICANN is to manage domain names, and update the domain name system in order to keep the internet stable, secure, resilient and interoperable. On technical issues the ICANN has a very narrow function, and its role is one that is clearly distinguished from that of the role of internet governance.

In 2014, ICANN, which has regional offices in Turkey and Singapore, appointed its first representative in India.

The 31st International Public Meeting of ICANN was held in New Delhi, in 2008.

In the run up to the September 2015 ICANN transition deadline, India has taken steps to harmonise its internet governance policy, with joint policy meetings of the Ministry of External Affairs, the Department of Telecommunications and the Department of Electronics and Information Technology.

Within its ambit, ICANN works as a multistakeholder process – it is advised by 40 governments as well as representatives of civil society. It functions with the support of various other agencies such as the Internet Engineering Task Force, the Regional internet Registries, and the Address Supporting Organisations. To underline that the ICANN model is one of the easiest platforms that

The ICANN transition process provides India with a chance to influence internet governance, moving away from the traditional stance of favouring the UN as the preferred platform for internet governance.

Since 2012, the Indian government has sought "far stronger representation of the developing world on the four ICANN Advisory committees"; a representative from India has been on the At-Large Advisory Committee (ALAC), and India currently has representation on the critical Governmental Advisory Committee (GAC).

The Indian government's Centre for Development of Advanced Computing (CDAC) and ICANN announced the coordination of a Centre of Excellence to look at the issue of Domain Name System Security in India in 2013.

enables voices from across the globe to be heard, the organisation has spread its offices, which are now present in Los Angeles, Istanbul and Singapore.

With regard to policymaking, ICANN again maintains that it promotes a multistakeholder approach. It hosts three meetings a year to discuss policy formulation, and the meetings are set up in a way that there is open policy discussion, which enables larger and more diverse participation. Also, the transcripts of these meetings are publicly available.

The ICANN staff is not responsible for creating policies related to the Domain Name System. This policy process is overseen by various players who have a seat at the table. Also present are committees such as the Government Advisory Committees that play a role in critiquing elements related to policy. Further, the venues of these meetings move across continents to different cities – London, Los Angeles, Singapore, and Buenos Aires. Fellowships are also provided to encourage participation from various countries.

Despite this, questions regarding the extent of ICANN's democratic nature arise, primarily for three reasons. First, ICANN is a US corporation; second, it is registered in the US; and third, it is subject to US laws. These reasons underscore the need for ICANN to enhance its democratisation process.

Future user countries, developing economies such as India, and those in the developing South time and again stress the need for ICANN to be more inclusive. On many occasions they have also expressed the need to increase its participation. Engaging with only a few successful economies will hinder the process of successful democratisation. To win the trust and support of the world, and to continue to maintain its credibility, ICANN must ensure that its reform process continues.

Another issue of primary importance is cultural specificity. This issue affects many nations where English is not the first and most common language. Countries such as India have a large number of languages and dialects, and crossing this language divide can be extremely difficult. How should ICANN address this problem? Finally, even though the internet is no longer a North-centric model, the distances over which countries such as India need to engage are extremely long, given that a majority of these conferences are held in LA, Buenos Aires etc.

For fast developing countries such as India, there are a number of options to engage better with ICANN. Two parallel paths should be followed. One: India should remain a part of the World Wide Web, and the larger internet community. Two: India has a large population, with many successful IT professionals. Thus, developing India's own domestic capabilities is very important. If theft of intellectual property from companies is carefully considered, one will realise the importance of building systems that are Indian, and also accommodating language capacities.

Finally it can be grasped that in internet governance there are no holy cows. Every part of multistakeholderism is debatable, and in such a situation weighing the pros and cons of this approach is wise. Emerging economies such as India need to further involve themselves in the IANA transition, as it is crucial for their progress in this space.

India is one of the few countries in the world to have its own National Internet Registry—managed by the National Internet Exchange of India (NIXI)—a result of negotiations with the Asia Pacific Network Information Centre, which is a regional registry under ICANN.

In 2014, India registered the '.bharat' domain name, allowing the naming of websites in the Devanagari script - opening up 8 Indian languages including Hindi and Marathi.

Around 125 million people in India speak English, the most common language on the internet; the government is trying to increase the online content available in other languages to reach the other billion who speak other languages.

Deconstructing Multistakeholderism

Chair
Suhasini Haidar, Diplomatic Editor, The Hindu, India

Panellists

- **Christopher Painter**, Coordinator for Cyber Issues, US Department of State, USA
- **Parminder Jeet Singh**, Executive Director, IT for Change, India
- **Wouter Jurgens**, Head, Cyber Security Department, Ministry of Foreign Affairs, Kingdom of the Netherlands
- **Alan Marcus**, Senior Director, Head of Information Technology and Telecommunications Industries, World Economic Forum

Recent debates, in India and internationally, show that agreement on the appropriate process, form and format for multistakeholder governance of the internet remains elusive. It is important to recognise the differing perceptions on this issue and to discuss thoroughly the difference in

approaches to and concepts around "multistakeholderism." Also key are the dynamics that are shaping the motivations of government, businesses and civil society actors on this subject – who owns the internet? Who runs the internet? Is the internet a public good, a resource, a utility or something else entirely?

In the "State of the Debate," a survey conducted by the Observer Research Foundation for CYFY 2014, a whopping 20 percent of the participants did not know what multistakeholderism was. This is unsurprising, given that the very essence of the word has been strongly debated globally, with some decrying the term as being overly vague. On many occasions people are also not certain of what they are debating and expressing, and indeed regularly end up talking past one another.

What needs to be understood is that the debate surrounding this issue goes a lot deeper than just the simple multistakeholderism vs. multilateralism conversation. A good debate requires innovation, ideas and imagination.

Many feel the internet is an engine for economic growth and social development, which strengthens the way we use technology. The internet has the power to define how future social systems will function. It also has the power to define the kind of state that can be achieved, illustrated by the internet's role in shaping important sectors like healthcare and education.

In 2011, India at the U.N. General Assembly sought to create a U.N. Committee on Internet-Related Policies (CIRP) in order to democratise global internet governance which is currently U.S.-controlled.

At the Internet Governance Forum 2012 held in Baku, Azerbaijan, India was represented by the Minister of State for Telecom, who signalled that India was open to working with ICANN.

At the Internet Governance Forum 2013 held in Bali, Indonesia, India did not send any ministerial representation.

India has been part of the UN Group of Government Experts meetings, which have examined the existing and potential threats from the cyber-sphere and possible cooperative measures to address them.

India has observer status at the Shanghai Cooperation Organizations (SCO), a Eurasian political, economic and military organisation which was founded in 2001 in Shanghai by the leaders of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan. The group also discusses norms of state behavior in cyberspace.

The Indian governments submission to the NETmundial meeting in April 2014 stated that, "Internet Governance should be multilateral, transparent, democratic, and representative, with the participation of governments, private sector, civil society, and international organisations, in their respective roles. This should be one of the foundational principles of Internet Governance." India also registered frustration at not having these principles included in the draft outcome statement and suggested that the outcome paper should be treated as a discussion paper instead.

At the same time, people have the tendency to take the internet for granted – expressing a carefree attitude towards it, forgetting that there are multiple layers which must come together for it to work. They may not even care about who owns or runs the internet, as long as it works for them. However, caring is essential. Questions of governance and infrastructure will impact the future; one should understand and appreciate both the complex technical layers underlying the internet and its jargon-filled governance system.

Widening the range of participants in the processes and engaging more people in the debates is one way to improve levels of understanding and effectiveness. NETmundial is a good example of a forum that allowed diverse sectors to be heard, including civil society, academics, NGOs and government.

Diversification enables the production of much stronger outcomes. It does not render the government role-less. Indeed, governments are still important players in this space, even though they do not necessarily have the final word. Depending on what is at the forefront of discussion, the role of government will vary. States are not the only stakeholders invested in key policies related to the internet. In areas like cyber crime and issues related to cyber security, states must effectively communicate with their civil society, their private sector, and even form partnerships with them to tackle such issues.

There are a large number of cyber conferences and internet governance forums, and these are always attended by the same people. That is, the 'internet community.' However, if other stakeholders – labour unions, religious groups, people from the arts, etc – are involved, new opportunities to tackle serious challenges and anticipate problems arise.

The test of multistakeholderism stems from whether or not it is a participatory democracy: Is it increasing or decreasing the participation of individuals and organisations? Decisions are taken based upon who is present in the room, and yet they affect many people who are not given a voice in that room.

Also, another issue surrounding the multistakeholderism concept is the issue of time and making decisions in a timely manner. In this regard the Netherlands has proved to be a good working example of a country based on consensus building, without discussions stalling. However, in final policy decisions there are zero-sum games, and one side must lose out.

Presently the regulatory space is occupied by several different bodies with differing specialisations. There are seven billion individuals in the world, and thus ideally, there should be seven billion voices in any internet governance process. While theoretically sound, in practice the question that arises is how to hear seven billion voices. How decisions are made and how these decisions are informed is a big part of the debate on multistakeholderism.

A grouping like the International Telecommunication Union (ITU) is not the final answer. The ITU, as an example, deals with traditional telecommunications, and is not participatory in nature. It is a very valuable and specialised platform, yet the expertise within the ITU is limited to mostly communications or regulations. It does not have the capability to deal with other important issues in this space, such as human rights abuse or national security.

Internet governance should not be a 'one ring to rule them all' space. As a relatively new and extremely complex space, it would be more beneficial to involve more stakeholders, enabling distributive solutions and providing greater flexibility. Another point of concern is that not all nations are democratic in nature. In this context, there are a number of countries that have a completely different view on cyberspace. Due to the fact that these nations view multistakeholderism as a threat to their stability, they tend to focus more intensively on information security rather than network security.

However, the Snowden affair proved to be a reality check for many nations. Realisations included the fact that every country conducts some amount of surveillance, on its own citizens and others. The surveillance may be in order to protect citizens, and therefore principles like the rule of law, transparency and judicial oversight are critical. Yet surveillance can also be used as a way to silence dissenting views. A lot is said about attribution being vital to cyber security efforts, but perfect attribution may lead to human rights abuses, for example in the case of whistleblowers.

At the ITU Plenipotentiary in Korea, November 2014, India proposed that the ITU has a role to play in Internet governance: first, because the Internet cannot be separated from telecommunications; and, second, because countries have legitimate security and access issues that are best addressed through multilateral institutions. The proposition was not accepted at the meeting.

During the 2014 July BRICS summit in Brazil, Indian Prime Minister Narendra Modi pointed at cyber issues being a global commons and the need for BRICS to look at this medium and its efficient management.

The Indian Minister for Communications and Information Technology stated in January 2015, “India will decide on its Internet governance model which will be consistent with the role private players play in spread of Internet and pre-eminent role played by government in public welfare.”

Protecting CIIs

Chair
Tobias Feakin, Director, Australian Strategic Policy Institute (ASPI), Australia

Panellists

- **Gulshan Rai**, Director General, Indian Computer Emergency Response Team, India
- **Yoko Nitta**, Principal Researcher, Japan Safe and Security Crisis Management, Japan
- **Andy Cheadle**, Chief Engineer, Communications Solutions Division, BAE Systems Applied Intelligence
- **Sherif Hashem**, Vice President, Cyber Security, National Telecommunication Regulatory Authority, Egypt

In a relatively short span of time, cyberspace has become an indispensable tool in our technologically driven societies. Be it in industry, security, education or even spheres such as politics, cyberspace is fast becoming a driving force. Critical Information Infrastructures (CIIs)

form the backbone of the cyber world, connecting various spheres by linking them internally as well as externally through cyberspace. Basic facilities such as electricity and public utilities, in addition to strategic sectors such as missile defence, nuclear power, air and maritime surveillance all rely on CIIs and cyberspace to varying degrees. Naturally, the uphill task of protecting CIIs is of the utmost importance to governments across the globe.

CIIs are highly interdependent not just amongst themselves but also on networks that may lie outside their realm and which do not often enjoy the same degree of protection. Some CIIs are at times controlled through vulnerable networks which leaves them open to potential cyber risks. As CIIs cannot work in isolation, the challenge of protecting them can be complex. These complexities are often exacerbated, as most of the processes in place to manage these infrastructures are hard coded and act as a hurdle in effectively dealing with fast-changing threats. Due to the existence of multiple ever-evolving technologies, CIIs are typically slow in implementing upgrades, resulting in periods of high vulnerabilities that can be exploited by rogue actors to devastating effect.

There are some glaring inadequacies inherent within CIIs, such as systems not being kept up to date with current security threats, most systems not being designed with security threats

The IT Act, 2000, section 70(1) defines critical information infrastructure as, 'the computer resource, the incapacitation or destruction of which, shall have deliberating impact on national security, economy, public health or safety'.

The Indian government has the authority under the act to prescribe security practices for all 'protected systems' as defined in section 70, meaning it can regulate security procedures of privately-owned critical infrastructure.

Critical infrastructure was emphasised as being in need of cyber protection in India's 2013 National Cyber Security Policy (NCSP), with the responsibility delegated to the National Critical Information Infrastructure Protection Centre (NCIIPC).

Protecting critical systems and networks remains a priority for the Department of Electronics and Information Technology, as part of its overall cyber security strategy.

At the height of the Stuxnet attacks in 2011, the National Technical Research Organisation (NTRO) estimated that out of 10,000 infected computers in India, around 15 were located in critical infrastructure zones including state electricity boards and oil rigs.

In 2013, a major hack breached servers of the National Informatics Centre, exposing hundreds of government email accounts and leading to information leaks including details of troop deployments along India's borders.

in mind, and the existence of a limited number of suppliers of CIIs as compared to general-purpose information technologies. There has been a paradigm shift in the security challenges faced by today's digital societies. Governments today have significantly less data information, as most data rests with the private sector, which, based on its customers' privacy preferences, is hesitant in sharing the information with governments due to fear of customer reprisal.

An aspect of CII protection often overlooked is the importance of physical security as part of the broader purview of cyber security, especially in light of the Fukushima disaster in Japan. There is an urgent need for network security and national cyber security policies aimed at creating crisis management plans. These plans should work towards building proactive security posture assessments and forensically-enabled information infrastructure, while mandating security audits of CIIs on a regular basis. Emphasis should also be laid on other measures intended to safeguard CIIs, such as sectoral computer emergency response teams, drills for cyber risk scenarios and crisis management plans. There is also a growing belief that by deploying multiple servers in different locations and countries, governments can minimise loss of critical cyber data even in the event of disasters.

Japan is specifically focusing on strengthening public-private partnerships for better management of CIIs, including developing more global partnerships as well as investment in research and

development. The aim is to revolutionise the next generation of technology aimed at enhancing security features by creating test-bed centres for various aspects of CIIs and their protection. It is imperative for countries to implement cyber policies to safeguard their CIIs. Governments should recognise specific business players and infrastructure to be part of CIIs, and partner with network operators to further strengthen cooperation between all significant players in the field and enhance shared network capabilities.

Challenges specific to private players include operational integration, mid-space exploitation (use of data from communication devices and platforms), threat intelligence and predicting potential threats, incidence response, and most importantly the need to promote the development of people, their skills and knowledge to maintain capacity. Stuxnet (the computer worm used against Iran) was an event that proved countries can no longer live in isolation believing they are safe from cyber attacks simply because they have limited exposure to the internet.

Security in cyberspace is about managing risks and expectations. It involves a comprehensive setup working out contingencies for all scenarios, but it also has to educate people and make them understand the limitations of the precautions set in place. Security frameworks are focused on protecting only the most critical infrastructures and not individuals. It is up to individuals and private players to safeguard their own cyber assets. Not all sectors understand the need for security and most usually brush it off as an economic luxury. Organisations are hesitant in taking cyber security seriously. Unless the effect is immediate and direct, most private companies regard it as a waste of financial resources. Governments themselves do not fare any better. Countries are either in a state of denial or a state of panic, with very few prepared for – or preparing for – such attacks. Countries should not wait for major incidents to bring cyber security to the forefront of national security policies.

Shortly after the NCSP launch, the NTRO formulated restricted guidelines for the protection of national critical information infrastructure, covering 8 industry sectors including energy, finance and aviation.

The Nuclear Power Corporation of India is a constant target for hackers, facing up to 10 attacks a day.

Individual sectors have taken measures to protect CII themselves - a notable example was the Reserve Bank of India mandating that all Indian banks have in place a steering committee on information security and a chief information officer.

Proposals have been made for sector-specific computer emergency response teams (CERTs), to complement the national team (CERT-IN)
The NCIIPC aims to recruit at least 500 cyber experts for its ranks by 2018.

Privacy Is Dead?

Chair

Mahima Kaul, Head, Cyber and Media Initiative, Observer Research Foundation

Panellists

- **Sunil Abraham**, Executive Director, Centre for Internet and Society, India
- **Siddharth Verma**, Managing Director, Corazon Systems, Australia
- **Karsten Geier**, Head International Cyber Policy Coordination Unit, Germany
- **Gerrit Jan Zwenne**, Professor, eLaw@Leiden, University of Leiden, Kingdom of Netherlands

The debate around surveillance, privacy and big data is binary. On the one hand, with data collection and analysis capacities increasing the world over, human rights are routinely abused under the garb of national security and better governance. On the other, there is belief in the power

of big data to do good by solving many of the world's problems such as public service delivery and policing and security.

The Edward Snowden affair elicited strong reactions from many countries. At the forefront of expressing their anger towards the US were Brazil, New Zealand and Germany. The Snowden revelations highlighted the question that many dreaded – is privacy dead?

In the past and even now, many have looked to Europe to set a gold standard for what privacy standards should be. However, privacy is a universal issue, not a European one; the United Nations General Assembly adopted a consensus resolution that strongly backed the right to privacy. Also, several non-European countries such as Brazil take issues related to privacy very seriously.

Currently India has no dedicated privacy law, though a draft law is said to be under consideration.

In India, privacy rights have been 'read in' to other rights, including the constitutional right to life and personal liberty (Article 21).

India has taken steps have been taken to protect electronic data under the 2000 IT Act, through sections 43A (liability of corporations negligently handling sensitive data resulting in wrongful loss/gain) and 72A (disclosure of information without consent).

Whether or not a global consensus on privacy is possible is debatable. ORF's "State of the Debate" survey highlighted the fact that India was ready to part with a certain amount of privacy. Yet it was also highlighted that it is important for India to have a privacy and data protection law that is in compliance with global norms.

In the field of healthcare, however, the challenges faced with regard to privacy differ. In this industry, privacy is key – for both patients and organisations. Here, the challenges faced are twofold – while practitioners understand the importance of protecting the privacy of patients, they also

The Indian government is also proposing a Data Protection Authority (DPA) to investigate and respond to data security breaches.

The Unique Identification Authority of India (UIDAI) launched the Aadhaar number programme to ensure more efficient service delivery by serving as address and ID proof. Aadhaar centralises demographic information about citizens (including their name, gender, age and address) and links it to biometric data - as such concerns have been raised about whether this data is being adequately safeguarded.

realise the importance of the information available being used for innovation in this area, and also for the greater good overall.

On the ground, the relationship between data protection and innovation differs among countries. Unlike the US, which is much more liberal in terms of privacy rules, the EU has a rigid privacy structure. And while many companies may be dissatisfied, and feel disadvantaged with the decision to maintain a less flexible framework, it is in place for a reason. The data protection law was created to support the internal market and provide more business to it. Certain EU countries (like Germany) had much more advanced data protection laws than other EU countries. Thus, the EU as a whole – in an attempt to harmonise the internal market – came up with what we now call the Gold Standard.

Despite this, the EU does not lead the way. The internet is, at the end of the day, powered by commerce, and companies deal with data. Data is therefore an essential part of commerce and the internet. Data must not be over-regulated as this will kill innovation. But at the same time, it must not be under-regulated as this will kill privacy. There needs to be a happy mean.

In India it was understood that the private sector must self-mitigate through innovations and development with regard to privacy. It would be beneficial to achieve a co-regulatory approach between the private sector and the Privacy Commissioner – an office to be set up once the Privacy

Protection Bill, still in the draft stage, is passed. Also, the Privacy Commissioner should play a more reactive role and take decisions based on certain principles.

Regarding data ownership and data control, questions arise as to who the owner should be – the user who owns the data or the companies which provide it? Data protection comes at a price – it means losing a certain degree of convenience. Owning data can prove to be extremely difficult, but controlling data is a realistic and viable option. Ultimately this debate filters down to the fact that consumers prefer to have some control over data.

The Indian experience regarding data ownership works on the premise that transparency should be directly proportional to power, while privacy should be inversely proportional to power. This can be accomplished by knowing what 'public interest' is. Users, who also put out a large amount of data on the internet, feel the need to have it regulated. A data protection authority could effectively deal with this issue.

India conducts surveillance on its citizens through mechanisms like the Central Monitoring System (CMS), launched in 2013. The CMS allows security agencies access to the entirety of India's telecommunications network to collect call records and other types of data.

In 2012, a Group of Experts on Privacy constituted by the Planning Commission, presented its findings, including an analysis of relevant legislations/Bills from a privacy perspective. The group also suggested recommendations for the government to consider when proposing a privacy framework for the country.

Many hold the belief that privacy is not dead, but that "privacy is hiring." University courses, jobs and organisations are being created to better tackle and understand this concern. The argument essentially is that if privacy is dead, then security too should be dead, as they go hand in hand. But some experts believe that perceptions have changed – the idea of privacy is no longer what it was a few years ago.

Norms of Cyberspace

Chair

C Raja Mohan, Head, Strategic Studies, Observer Research Foundation

Panellists

- **James Lewis**, Senior Fellow and Director of the Strategic Technologies Program, Centre for Strategic and International Studies, USA
- **Alok Prasad**, Former Deputy National Security Adviser, India
- **Patryk Pawlak**, Senior Analyst, EU Institute for Security Studies, France
- **Joris Larik**, Senior Researcher, Global Governance Program, the Hague Institute for Global Justice, Kingdom of the Netherlands

The explosive growth of cyberspace has made it an effective force as well as an economic multiplier. Its mass appeal and cross-border penetration has fundamentally changed the way individuals, private players and governments interact with one another. The idea of international

behavioural norms of cyberspace to govern interactions in areas such as privacy, cyber crime and e-commerce is fast gaining momentum. But the diversity which is responsible for the success of the internet is also the biggest challenge when it comes to reaching an agreement on norms between diverse stakeholders. Due to varying cultures and societies, different states have different ideas and definitions of the many aspects of cyberspace. The traditional roles of international bodies and structures of global governance may not hold when it comes to the internet. Although the internet was a highly Western tool to begin with, over the years it has shifted its demographic to Asia, which currently has the highest number of internet users in the world.

India – as well as other developing countries – is increasingly looking at cyberspace as a tool of empowerment, better governance, financial stability and delivery of services in an inclusive manner. Most public policy issues in the country arise from these expectations. The government of any state has a responsibility to protect information infrastructures, especially critical information infrastructures. The government also has a duty to protect the data of its citizens from prying foreign or private actors. Despite repeated efforts, developing countries have fallen short of these objectives; however, there exists room for creative thinking even though the policy issues are not entirely generous. There is a need for the focus to shift from mere domestic policies to international public-private partnerships to better prepare governments to face cyber challenges.

India is not a signatory to the Budapest Convention but participates in international cyber crime cooperation through Mutual Legal Assistance Treaties (MLATs) with other countries, and through its INTERPOL membership.

India has individual cyber bilateral agreements with USA, the UK, the Netherlands, Korea, Japan and Israel, among other countries.

India participated in meetings on cyber security of the Group of Governmental Experts (GGE) at the UN, contributing to discussions about principles for behaviour in cyber space and how international law could play a role in cyber space.

The 2013 GGE report acknowledged that information and communication technologies play a large role in international security and stability. It suggested that existing international law principles could be developed to form the basis for future cyber norms.

India has observer status at the Shanghai Cooperation Corporation (SCO), a Eurasian political, economic and military organisation which was founded in 2001 in Shanghai by the leaders of China, , Kyrgyzstan, Russia, Tajikistan, and Uzbekistan, which also looks at developing norms of behavior in cyberspace.

One of the most crucial needs is to translate these norms into concrete actions. There is a need for not one norm but a market of norms. There is also the question of trust; new cyber norms are impossible to create if we do not have trust in the existing norms. Both governments and international groups, with the help of their respective enforcement mechanisms, should work towards applying the existing norms. A point of stability has to be reached before new norms can be created. Rather than debating cyber norms in abstract terms, we need to focus on how to enforce the existing ones, while maintaining a balance with respect to online freedoms.

The trust of end-users in regulatory institutions is another crucial factor for successfully implementing norms in the cyber world. Countries should initiate confidence building measures like the UK, which has implemented special projects aimed at building trust within its citizenry vis-à-vis its cyber policies through massive outreach programmes. The crux is that there are no better or worse norms, as it all boils down to mechanisms in place to implement norms and whether they are successful, in which case the norms are considered good. Capacity building is a key tool for developing norms in cyberspace.

The Budapest Convention is hailed as a milestone in developing international norms. Some have maintained that the Budapest Convention is a great example of flexibility in international agreements, as it provides options to countries to opt out of or terminate particular aspects of the

agreement. But there are also others who consider the Budapest Convention model ineffective and compare it to a rental agreement that is easy to get out of without severe penalties. However, there is growing consensus among global policymakers on the need for stability in cyberspace. The Budapest Convention may not be a good model but it is a model that currently exists and can be made effective with the use of the right enforcement mechanisms. The global community can use the model as a platform to develop wider norms that are so essential in cyberspace today.

Global norms are not going to be created in one attempt. There will be contestation but there is room for pragmatism. The important thing is to keep making efforts towards reaching global consensus on low-hanging fruits such as sectoral norms. To continue moving wherever there is consensus instead of constructing abstract designs for the entirety of cyberspace is the approach to follow. Functional cooperation is the need of the hour to further promote goodwill between various stakeholders. There is acknowledgment within the global community that even if norms are created, enforcing them is not going to be easy due to the multijurisdictional nature of the topic and the ever-increasing number of players involved. There is a possibility of rogue states maintaining double standards and actively defying the norms, but if there is an understanding between the major powers, progress is possible. Pragmatism is the key to achieving global cyber norms.

India is a part of the BRICS (Brazil, Russia, India, China, South Africa) economic and political grouping, which in its 2013 Durban Declaration stated that it was "important to contribute to and participate in a peaceful, secure, and open cyberspace."

The Indian government has in the past floated the idea of introducing mandatory disclosure norms, whereby companies would have to report any system breaches they experienced to the government.

India is an 'authorising nation' under the Common Criteria Recognition Arrangement, which aims to evaluate information technology products to make sure common technical and security standards are maintained.

Preparing for Cyber Conflict: Is It Inevitable

Chair

Sean Kanuck, National Intelligence Officer for Cyber Issues, USA

Panellists

- **Gabi Siboni**, Senior Research Fellow and Director, Military and Strategic Affairs and Cyber Warfare Program, Institute for National Security Studies, Israel
- **Suleyman Anil**, Head, Cyber Defence, Emerging Security Challenges Division, NATO
- **John C Mallery**, Research Scientist, MIT, USA
- **Ian Wallace**, Visiting Fellow, Cyber Security, Center for 21st Century Security and Intelligence, Foreign Policy Program, the Brookings Institution, USA

In the complex framework of cyber governance, cyber security is fast emerging as one of the biggest challenges. Within cyber security, the phenomenon of cyber conflict is potentially the biggest cause of concern for states as well as private corporations. Cyber conflict can be defined as

mirroring conflicts in the physical world with added complexities due to the multijurisdictional nature of the cyber sphere. The nature of the cyber domain means that the use of cyberspace is potentially more useful for certain actors than others. The low cost of cyber warfare allows a level playing field for not just small states but also for fringe groups. The actors in the cyber world are the same as the actors playing a crucial role in the global sphere. The cyber world is essentially a mere extension of the physical world.

The present day global cyber threat environment is extremely alarming and volatile, and can be expected to last until there is necessary international consensus on cyber challenges. The numbers of threat actors have increased, with increased spending on cyber offensive capabilities; the attack surface has exponentially grown due to the digitally reliant nature of societies with more and more interconnected cyber gadgets; and the current global political environment incentivises cyber conflicts due to the relatively lower costs involved as compared with traditional conflicts. It also allows multidimensional responses in conflicts, which makes the idea of proportionality even more complex vis-à-vis cyber conflicts. The rise of cyber conflicts has also given rise to 'hacktivists,' who have taken the place of traditional mercenaries with a greater potential to cause damage based on their capabilities to launch attacks on different fronts simultaneously. Most of these hacktivists are manipulated by states or non-state actors with an agenda. There

India's 2013 National Cyber Security Policy (NCSP) set out explicitly to counter cyber threats including full-blown cyber warfare.

The NCSP also seeks to build cyber security capacity, through the creation of a workforce of at least half a million trained cyber security professionals. To this end, the University Grants Commission indicated that cyber and information security should be added to the curricula of technical institutions in India.

Non-state actors from India and Pakistan regularly trade hacks by tampering with government and other websites in the other country. In 2014 over a period of two days more than a dozen websites were hacked on both sides of the border after the Press Club of India website went down and hackers claiming to be Pakistani claimed responsibility.

The cyber security arm of the Government of India, the Computer Emergency Response Team, (CERT-In) reported 62,189 cyber security incidents in the first five months of 2014; many of those cyber attacks were linked to IP addresses located in China, though it was unclear if they originated from there.

High-profile hacks like the breach of the Indian navy's computer systems in 2012 have also been linked to China. One of the main targets of the 2012 hack was the Eastern Naval Command, which supervises naval activities in the South China Sea.

is a growing cyber arms race in most parts of the world. Different actors have different motives for building their capabilities.

The Russian cyber conflict doctrine is based on redundancy. Historically, the Russian intelligentsia has been very attentive to psychological methods of destabilising their leadership and they view cyberspace in the same light. Their quest essentially is for several layers of redundancy in the face of overwhelming Western technological superiority. In recent years, China has emerged as another significant player within the realm of cyber conflict. The Chinese policy essentially seeks to target said Western technologies to reduce the gap and ensure disproportionate effects, given how dependent Western weapons are on intelligence, surveillance and reconnaissance systems. There is a global belief that both Russia and China actively engage in industrial espionage to offset the technological superiority of their Western counterparts.

All conflicts in today's day and age have a cyber component. No conflict in the global world is being fought in complete isolation from the cyber world. To counter this growing menace of cyber security and cyber conflict, states around the world have initiated programmes aimed at improving their cyber capabilities and capacities. The foremost challenge in building capabilities is the lack of information or knowledge about the capabilities of adversaries. Due to the non-physical nature of cyber conflict, developing defensive capabilities without understanding the intent or the offensive capabilities of opponents can be an uphill task. There is

an urgent need to integrate cyber aspects into existing security postures, crisis management procedures and capacity building measures. However, due to the dynamics of the cyber sphere, questions remain on the best approach towards capacity building within society.

There is a growing section which believes that capacity building in cyberspace should predominantly be in the private realm. Unlike the non-cyber world where governments have the most sophisticated intelligence capabilities, in the cyber world, private players have the most data and governments need to access this data through private distribution networks. In our evolving world, capacity building must be done in private corporations as well as individually. There needs to be an emphasis on development of people's skills and their knowledge for a quicker response time. Civil society groups have increasingly been advocating for civilian capacity building to take precedence over military capacity building, emphasising an asymmetric capacity building approach where multiple dimensions can be safeguarded.

In 2011 India's Naresh Chandra task force identified the need for a cyber command. This concept has been doing the rounds; in 2014 it was suggested that the 3 chiefs (army, navy, airforce) institute a Tri-Service Command called the "Tri-service Special Operation Command" which would include cyber.

In March 2015, the Indian government appointed a 'Cyber Security Chief' under the Prime Minister's office. The new chief, Dr Gulshan Rai, previously headed CERT-In at the Department of Electronics and Information Technology (DeitY), in the Ministry of Communications and Information Technology.

Different kinds of attacks focus on different dimensions which need to be simultaneously built up. Military attacks are about attenuating capability, while espionage is about gaining information and economic or financially motivated attacks are about causing disruption or gaining an advantage. Thus, proportionality is a major challenge in the sphere of cyber conflicts. Due to their mass civilian reach, cyber conflicts can have wider effects on the populace than a traditional conflict. In response to the issue of proportionality, countries are gradually implementing laws related to cyber conflicts and cyberspace in general. They are increasingly assessing the implications of cyber conflict before initiating such laws and considering necessity, collateral damage and proportionality to avoid legal penalties in the face of the growing global outcry that accompanies most such conflicts. The UN Group of Governmental Experts has agreed that norms of war such as proportionality, distinction, necessity and avoiding collateral damage apply to cyber war as well, but has yet to work out how to apply them.

Within the global community, there is ongoing debate on whether cyber conflicts should be treated differently from conventional conflicts. There is widespread support for looking at cyber conflicts in the same light as traditional ones, as the aspects involved in the latter resonate in cyberspace as well. Enforcement of laws is relatively easy in traditional conflicts due to the tangible nature of the acts as well as the limitation of location. Enforcement in the cyber world is a more complex task. In the absence of international governing laws, the multijurisdictional nature of cyberspace severely limits enforcement mechanisms.

Emerging Powers & Internet Governance: Looking Towards 2020

Chair

Samir Saran, Vice President, Observer Research Foundation

Panellists

- Rajan Mathews, Director General, Cellular Operators Association of India
- Uri Rosenthal, Special Envoy, Global Conference on Cyberspace, Netherlands, 2015; former Foreign Minister, Kingdom of the Netherlands
- Fernanda Crespo, Intelligence Analyst, Fundação Getúlio Vargas, Brazil
- James Lewis, Senior Fellow and Director of the Strategic Technologies Program, Centre for Strategic and International Studies, USA
- Christopher Painter, Coordinator for Cyber Issues, US Department of State

With over 600 million new internet connections expected in the next six years, the debate on the potential challenges and opportunities in cyberspace is gaining ground and momentum. Several nations have created vast infrastructures to reinforce their independence in the interconnected global cyber sphere, while many in the developing world such as India have recently focused their attention on the development of critical information infrastructures. The question, however, remains whether countries should strive towards a global system of cyber governance based on mutual understanding and cooperation or follow the Russian and Chinese model of domestic capacity building, paying little heed to larger international norms.

China's role on the global stage has frequently come under the scanner. With aspirations of being a major global power, China is careful to avoid actions that can be perceived as espionage. It is reconsidering some of its positions in the face of adverse global opinion; however, domestic political stability continues to remain the primary goal of Chinese cyber policy and it is unlikely to change in coming years. Cyberspace is a tool of state power for China and all trends indicate that it will continue to use this aggressively in achieving its objectives.

As observed by many experts, the NETmundial conference held in April 2014 was Brazil's response to the growing issue of

The Government of India was one of 12 governments which attended the NETMundial Global Multistakeholder Meeting on the Future of Internet Governance; along with Russia and Cuba, India did not sign the outcome statement of the meeting due to concerns that it didn't sufficiently address issues including surveillance, the role of states, and net neutrality.

The Indian government has reiterated its commitment to an open internet, including principles like net neutrality, with the telecom minister saying that the internet must promote both the local and the global.

India wants the internet to be an 'equinet' of values – a free and global, level playing field where governments still have a role to play.

Prime Minister Narendra Modi stated that "BRICS countries should take the lead in preserving cyber space as a common global good"; on the sidelines of the 68th UN General Assembly session the foreign ministers of the BRICS nations issued a joint statement expressing their concern about "the reported practices of unauthorized interception of communications and data from citizens, businesses and members of governments, compromising national sovereignty and individual rights." It also emphasised that "security in the use of information and communications technologies (ICTs) through univesrally accepted norms, standards and practices is of paramount importance."

cyber security and the broader cyber conversation in the face of the Snowden revelations. There is an aggressive campaign for data localisation within the country. The Brazilian government, in the face of growing domestic demand, is moving towards keeping all information, including cyber data, within the country by transferring data to domestic servers. As an upcoming global player, Brazil is working towards developing the public-private partnership model to promote cyber infrastructure domestically. Brazil has also strengthened its domestic cyber laws: Internet providers in the country are now required to retain data for a year whereas application service providers are required to do so for a minimum of six months for greater transparency and accountability. Brazil has also implemented the right to be forgotten, where citizens can request removal of any personal data from the web.

As the leading cyber power in the world, the US is at the forefront of the global cyber debate, and is often criticised for the inherent contradictions within its cyber policy – as highlighted by the Snowden affair. US policy experts argue that their domestic cyber policy is a result of the US deliberately debating cyberspace and its governance mechanisms comprehensively before forming a national cyber policy. There is an understanding among policymakers in Washington of the interdependence of cyber policy with other aspects of governance and society. Meanwhile, one of the fiercest vocal advocates of preserving the free nature of the internet, the Netherlands has adopted an inclusive domestic cyber policy. The cyber discussion in the Netherlands is left at the technical level to industry experts and

academics, but strategic policies for cyberspace are discussed at the political level. The main objective is to promote and ingrain online freedom in society. The consensual nature of Dutch society is reflected in cyber policies as well, where there is a healthy discussion between government agencies and private players.

On the other hand, India's recent focus on cyber development, although commendable, is ambiguous at best. India is still working towards developing a national cyber policy which can represent its global and domestic aspirations. India's current cyber initiatives lack a coherent, comprehensive view of how it perceives cyberspace. The Indian government has been extremely slow in incorporating cyberspace in its core governance policies and has allowed private players to soar ahead in infrastructure capabilities. Due to the dominance of the private sector in owning data and cyber infrastructure within the country, the current Indian government is formulating a national policy which will address private concerns while ensuring access to its billion-plus population. While there is widespread agreement with respect to the merits of an open internet as the best policy for economic growth for all stakeholders involved, there is a need to treat internet governance as a matter of substance which will have far greater consequences on governance in the coming years. Domestic laws can be domestically viewed, but in the longer run, there is a need for a unified approach to the internet considering its scale and interdependence across boundaries. Globally, cyber laws need to be as inclusive as possible, all the while continuing to maintain the internet's global, open nature. The question of how to apply international law to cyber law and security is integral to the broader cyber debate. However, there is an emerging school of thought that argues that even though open, global markets are indeed a sensible economic solution, the world is quickly moving towards a multipolar environment. Why then can the internet not exist as a multipolar environment, with different sets of rules and norms guiding different regions or groups?

India and its government have linked the internet to development through the Digital India programme, which in addition to widening connectivity in India acts as a national e-governance plan.

India and China have the two largest populations of internet users in the world, a combined total of nearly 1 billion people; according to the ITU, two-thirds of all internet users will come from the developing world.

The world of cyberspace has grown exponentially in the past decade and it is crucial for India to overcome its historical inferiority complex about the "advanced world" in order to be a leading voice in the field. Vast differences within the cyber context exist globally between countries, not only from an economic point of view but culturally, locally and historically. There is scepticism within the global community about whether concrete measures can indeed be established within such a heterogeneous group. There have been several initiatives but none have been able to lead the way. The Brazil-Russia-India-China-South Africa (BRICS) grouping was created in response to a specific economic need rather than with the intent of leading the cyber debate. Based on their different views and internal differences, BRICS does not seem likely to become a unified voice in the cyber debate. India is in the unique position of becoming a beacon in the area of cyberspace governance in the emerging world, but it will have to get its domestic cyber policy in order before it can assume such a crucial role.

Keynote Address by

Dr. Uri Rosenthal

Thank you so much, Mahima, and thanks to ORF for inviting me here. It is a great pleasure after the sessions we had in May this year, when you were in full swing with your election process, and it was clear then as it is now how democracy here in India is kicking and alive. Let me say that I am very pleased and honoured to support the ORF in organising the CyFy conference and it is clear that we are here on solid ground. When we talk about cyberspace, cyber security, there are an incredible number of internet users in India: India is a really key player in the global debate on the future of cyberspace. No wonder that CyFy has drawn such a large audience this year. I heard that the audience grew yesterday throughout the day; who knows how things will look in the late afternoon today!

Let me say that it is also good to see that the conference is actually involving all stakeholders. It is, in that sense, a perfect avenue to engage on the matters of cyberspace. The key points to be addressed

include the shared interests of democratic, market-based countries in cyberspace, implementing state sovereignty in cyberspace and its effect. The Netherlands is hosting a global cyberspace conference in April 2015 in The Hague and we would like our Dutch delegation here to address the opportunities that this conference will offer in terms of promoting a free, open and secure internet. Talking about shared interests of both the Netherlands and India in cyberspace, it creates grand opportunities. But it also presents new threats and challenges to continue benefiting socially and economically from the cyber realm as a global public good while at the same time finding ways to protect national interests, guarantee rights of citizens and find responsible ways to exercise sovereignty in cyberspace. Being here in India, I take particularly notice of the fact that the internet has become a vital factor in exercising democracy and, indeed, free speech, which is so important as we all know. Given that throughout the world, censorship and surveillance are on the rise, it is good to remind ourselves that the political and civil rights that are protected offline must also be protected online.

Seeing how important cyberspace has become to our societies, it is of no surprise that the way the internet is governed has become an increasingly contentious, if not controversial, topic. The Netherlands and India, I am happy to say, share many of the same concerns, and for our part, the Netherlands supports the NETMundial principles and the roadmap for internet governance reform based on a multistakeholder approach. I do see some sort of a common ground emerging.

Within these parameters, when we talk about multistakeholderism, it is an approach; we should not be dogmatic. We must involve all stakeholders in their respective roles, but we should be very clear that effective decision-making is also part of the story and we must, for that matter, strengthen the role of governments in those areas in which governments have a legitimate public policy concern. On a similar note, regarding the transition of the IANA contract, the way it is exercised should be made more accountable to the global community, in which the global South plays an increasingly important role. However, IANA and ICANN functions must remain with independent private organisations as part of a distributed polycentric ecosystem of internet governance. While states must be able to influence the overall direction and parameters of internet governance, they should not be involved in the running of the day-to-day operations, which should be the domain of technical experts. When strengthening the role of governments in the governance of cyberspace, we must ensure that this does not lead to the sort of multilateral paralysis that we have seen in so many other areas thus far. The topic is simply too important for that to occur. Obstacles in reaching agreement on solutions should not prevent solutions from being developed in the first place, and the global community should find middle ground to develop a workable and responsible proposal for globalising the IANA function before the deadline in late 2015. Such proposals are necessary to get, for example, permission-less innovation that is the fundamental source of socio-economic benefits of cyberspace. We cannot allow a lack of compromise to be used as a reason for maintaining the status quo, because involvement of a truly global community is a moral imperative.

It is clear, ladies and gentlemen, that cyberspace presents challenges to the national security of societies and states. Citizens expect their governments to take responsibility for their security in cyberspace as long as they do so to protect privacy. It is logical, therefore, that state sovereignty also

play its part in cyberspace. The Netherlands has just as much interest in this as any other country. Our vital infrastructures are targeted on a daily basis. We have suffered serious and severe attacks aiming at undermining the basic functions of society and the state. However, if sovereignty plays its part in cyberspace, it also means the existing system for regulating international relations between sovereign states is applicable in cyberspace: The system I am talking about is international law, and it offers far more opportunities than is sometimes assumed. The Netherlands believes that international law already offers useful instruments that can contribute to greater security and stability amongst states even though its application must be clarified.

Important work is being done by the UN Group of Governmental Experts on clarifying how international law, including international humanitarian law, governs behaviour of states in situations of armed conflict in cyberspace. However, equally important is to look at situations below that threshold. Fields of law like the laws of state responsibility, trade law, international human rights law and parallels - I would like to emphasise this - parallels from the laws of the sea and outer space could offer guidelines for responsible state behaviour. It would be more effective to see how these already agreed upon instruments work in cyberspace instead of entering into contentious negotiations on new ones. We should be positive and we should be constructive. Work is being done already in academia, and discussions as here in the CyFy conference can indeed contribute to generating ideas and developing consensus. By supporting a series of regional meetings and seminars on these topics the Netherlands is actively contributing to this process, and the results of these meetings will serve as an input for our discussions in the global conference in April 2015.

Ladies and gentlemen, increasing confidence and trust is key to increased stability and predictability in cyberspace. Norms of responsible state behaviour, as also important confidence building measures, can pave the way for wider clarification and application of international law. Some norms could even go beyond the protection arrangements included in international law. For example, when we talk about identification and protection of certain neutral objects, the neutral zone and cyberspace-enabling information and communications technologies, these could be declared off limits to any action that undermines their stable and secure operation in both war and peace time. Our global conference on cyberspace will offer a platform to clarify and also specify what this would look like in practice so as to facilitate consensus and agreement in other processes.

Now, ladies and gentlemen, we should not encourage what is sometimes called a sort of 'cyber Westphalia agreement.' International political agreements are important in working out how state sovereignty can be responsibly implemented in cyberspace. This should be done very carefully because a full Westphalian interstate system for cyberspace is simply untenable. States will never be able to fully regulate against inherent risks of cyberspace, because in many cases these are also its greatest strengths. State sovereignty in cyberspace should and inevitably will focus on state-specific responsibilities, not the least because states are not the only stakeholders controlling the domain. I would even like to say that states and state authorities must learn to accept these realities; nothing less will do.

Ladies and gentlemen, as I have already mentioned, the Netherlands is hosting the fourth Global Conference on Cyberspace in April next year. It will discuss and deal with similar issues being debated here at the CyFy conference. The global conference in The Hague is not the determinative process that will deliver an international agreement, but is rather a platform for high-level international discussions that can generate ideas and move them a step further in order to move the international debate forward. It will take place at a very, let me say, interesting moment. I should warn you that tulips will not be flourishing at that moment. But it will be exactly one year after NETMundial, which means it will be the right time for mid-term review of its findings, of its roadmap. It will be right in the middle of the discussions of the BILT Commission on Internet Governance. It will be halfway into the mandate of the current UN Group of Government Experts and it will be few months before the current IANA contract expires. A continuing Dutch innovative approach to this type of high-level conference will be an interactive simulation session of several cyberspace dilemmas. All participants will be asked to discuss and contribute possible solutions. This innovative approach has been tried out at the Nuclear Security Summit with government leaders from all over the world at the beginning of this year.

The desired end of the conference in The Hague is a negotiated chair statement that includes three outcomes. First, support for practical implementation and international cooperation where we can jointly develop practical, worldwide responses to urgent challenges. For example, cooperating in investigation and prosecution of cyber crime, improving, for instance, CERT cooperation. Second, support the emerging consensus on norms and international stability. As already discussed, we should focus on clarifying the role of international law as a real and sincere source of stability in relations among states and we should support the emergence of consensus on certain norms of responsible state behaviour. Third, and by far most importantly, we would like to promote capacity building and the exchange of knowledge. Indeed, what you call the Digital India programme is a truly fantastic example of the kind of capacity building that will lead to economic growth and moreover, social development. By exchanging expertise on capacity building, more countries will be able to harness those benefits. Increasing capacity building in a structural and significant way is not only crucial for bridging the global digital divide, it is also crucial as a confidence building measure in itself for international relations. At the conference, the Netherlands will launch a global forum on cyber expertise, where all parties can share their cyber strengths and capabilities. Partners from both sides of the digital divide will work together to launch joint initiatives on capacity building and within those capacity building efforts, best practices in the fields of tackling cyber crime and data protection. We should increase political dialogue on capacity building and build solid support and funding for such activities.

Ladies and gentlemen, to conclude, and turning back to CyFy, it is important to have these kinds of conferences where different perspectives are exchanged among a global audience from all parts of the world. They are valuable for finding and supporting emerging consensus on international agreements. Of course, we must keep in mind that only by working together can we unlock the huge potential gains in wealth and welfare that cyberspace offers. We hope on our part to greet our Indian friends and also friends from other parts of the world in The Hague. Thank you, ladies and gentlemen.

Special Address by

Ms. Angela McKay

Good evening everyone and thank you for the kind introduction, Samir. CyFy is a really important forum for us to be able to discuss cyber security and cyber governance, and Microsoft is very proud and very honoured to be able to sponsor this particular dialogue. I would like to go ahead and take a few moments to thank our organisers ORF, and in particular Samir, Mahima (who is somewhere in the room) and the team for running a great conference and bringing this all together. I would also like to thank the other organisers and all of you in the room, the attendees here. The conversation has been vibrant and we have had some really interesting discussions that help drive the dialogue forward, and that does not happen in every single conference. So, thank you for that.

I am very fortunate; this is my sixth time visiting India and I love coming to this country. My friends, colleagues and family know that, but when I get asked why I love coming to India, there are three

things that come to mind. I thought I would raise these before I get into my closing comments. First of all, India is very hospitable. I always feel very welcome in this environment, whether I am meeting with a Microsoft subsidiary, talking with government officials, or even going out and shopping (because I do like to do some shopping while I am here!). Second of all, I have noticed that the people of India have such great intellectual curiosity and you don't see that everywhere. What is really interesting is that it is not just intellectual curiosity to help advance themselves as individuals, but it is intellectual curiosity to help advance the country and society – and that is a unique characteristic that I think we need to acknowledge. Last, but certainly not least, I am a long-term vegetarian who loves Indian food, so why not come where it is going to be the best. So, thank you very much.

In my closing comments, I am going to talk about four types of changes that have been talked about throughout the course of the conference, the outcomes of these changes and three concepts that I think will help all of us manage these changes and actually help improve cyber security. The first change that has been brought up consistently are the demographic changes that are going on around the world. These came up particularly in the inaugural session and by Minister Prasad. Whether you want to talk about what the world is going to look like in 2015, 2020 or 2025, what we know is that the world is changing dramatically. When we think about many of the Western European countries and the United States, these environments are going to be saturated. Internet usage – everyone is already online. But what is interesting in those environments is the device diversity. If even I think about how many different devices I have brought here with me on the trip, it is probably at least seven. So, it is going to be a device-rich but internet-saturated global north. At the same time you are going to have a user-rich global South, where users will be younger and will be coming online with mobility. What is really interesting is that these environments are still going to be plugging in users even past 2025. As policymakers and as part of the industry, we have to think now about preparing for this kind of future. What that really results in is this globally interconnected society that we have all talked about.

The second kind of change that has been talked about are the geopolitical and geo-economic changes we are seeing. We have already moved from a unipolar to a multipolar world. But as was well highlighted in the pre-conference session, the Snowden revelations not only brought forth a conversation that needed to be occurring in the public domain about surveillance issues, but it also catalysed and reinvigorated some of those geopolitical changes. What that means is that there has been breaks in trust. We have heard a lot about breaks in trust between governments, but there has also been a break in trust between users and ICT providers around the world. So, what does this really mean? IT means that developing policy in this environment is much more difficult. We are not only dealing with the issues themselves and the existing overlay of politics but also a new overlay of politics and a more emotionally charged environment that makes policy formulation much more difficult.

The third change that has been talked about a lot are the changes in the cyber marketplace. I could name all the various technological innovations – cloud, mobility, internet of things, app development, e-commerce – but some of the other changes that are going on in the cyber

marketplace include the diversity of players that are now involved. In this conference I heard quite a bit about multinational organisations. But I want to highlight that the ICT industry is flourishing not just with multinational organisations but with innovation around the world; what is also interesting is that innovation is occurring in other sectors which are adopting ICT to advance their businesses. An interesting conversation that occurred the first night was about what is going on in the healthcare industry. This greater diversity of players also involves civil society, who is making sure that the interests of the people get represented.

The third thing in the cyber marketplace is that the government model is in flux. I thought Ambassador Reddy did a particularly nice job in the ICANN-ICAN'T debate (which is still my favourite session name from the overall event) of really highlighting what India needed to do to be influential in this conversation. But Ambassador Reddy's comments are relevant for every single organisation and country that is represented in this room. To influence internet governance, you are going to have to be engaged and resourced. These changes in the marketplace in this environment result in a degree of complexity, uncertainty and rapidity in innovation that is creating a gap and greater delta between policy development and what is going on in technological innovation.

The last change I want to talk about are the changes that Microsoft is actually making recently. When we look at this globally interconnected society, we recognise the degradation of trust and we see the uncertainty and complexity. We have to think about how to build greater trust with our customers and how to better protect our customers. This is something Microsoft has been doing for many years. We have had a longstanding commitment to security, privacy and reliability, but I do want to highlight five things we are doing more recently when we see all these changes in the global ecosystem.

The first is that we have been working in the technological layer. We are doing a lot of encryption. I would like to consider encryption at scale, encryption in data at rest, encryption in data in motion. Second, we are thinking about architectural changes, in terms of where we are going to build the data centres to serve our customers. The situation is changing – we have to think a lot not just about business continuity, making sure that you can have ready-time backup that is provided and global elasticity account services, but we also have to be thinking about how to address concerns of sovereignty and data localisation. Just to be very clear, we cannot build a data centre in every single country in the world, it breaks the model of the cloud. But fortunately, at least here in India you are going to be getting your own data centre. Our CEO Satya Nadella was here a few weeks ago and actually announced that. But we are thinking really carefully about what to do in the architectural layer.

Third is our work in transparency. We were already doing transparency reports before the Snowden revelations, but since then we have upped the ante. We actually sued the US government so that we can provide additional information in our transparency reports on the number and character of law enforcement and intelligence requests for our customer data. Fourth, in the legal domain, in addition to our suit against the US government, we have started to challenge the extra-jurisdictional

reach of the government. This particular case is still making its way to the judicial system but will set a precedent for the world on how jurisdictional reach is managed and how to protect customer data no matter where it sits in the world.

The last thing we are continuing to advance is a broad series of activities in the policy space. I happen to personally be close to these activities. There is a bunch of legislative stuff we are doing in the US regarding surveillance, and around the globe we are working on a wide variety of issues like critical infrastructure protection, information sharing, incident reporting and supply chain risk management, again working to ensure that we can build trust with our customers and better protect them.

Now, thinking about all these different changes, there are three concepts that I think are really important for us all to think about in managing these changes and have been brought up consistently through the conversation here at CyFy. The first one is who should be involved as we work to advance security. Well, fortunately or unfortunately it has got to be a multistakeholder process. But this is an operational reality. As I spoke earlier about changing market dynamics, I highlighted the diversity of players. All these diverse players have a role in this ecosystem. But as was noted in the panel on multistakeholderism, the model does not have to be uniform. Who is involved, the level of engagement that they provide and who can actually help effectuate change depends on the problem-set or the topic that is being addressed.

The second concept is how we are going to work together on these problems. I would certainly advocate for something that was brought up earlier – and which is consistent with how I work – pragmatism. We are not only going to have to think about what we can do or what we should do, but about what we must do. We are also going to have to think about where specifically progress can be driven.

That brings me to the third concept. There is going to need to be some prioritisation, although I can't tell you what your priorities should be. Every single organisation and individual is going to have to think about what they consider to be priorities. Here, I will share a few where Microsoft thinks we can make progress, and this is all informed by the pragmatism I spoke of a second ago. We definitely believe that there is considerable progress that can be made in countering cyber crime. While there may not be uniform agreement on what cyber crime is, there is generally broad agreement on many of the aspects of cybercrime. This is an area where progress can be made – and demonstrable progress is really quite important. This is because when you engage on a topic and you see progress, it provides return on investment and it enables you to come back and work on other problems. This is very important to continue to bring people into the process.

The second area where we really think a lot of progress can be made is on advancing the security of critical infrastructures. I recognise that there are varying models of ownership in different geographies and different verticals around sectors, but a lot of the basic cyber hygiene issues and risks facing critical infrastructures around the world are quite similar. There are models being advanced in different regions of the world that have some commonality. In the US there is the cyber

security framework that resulted from the executive order; in Europe we are seeing progress on the Network and Information Security Directive that has some key concepts; and even in China you have the multilevel protection scheme. From a Microsoft point of view, we like to think about this as risk-based. We need to be focused on outcomes pointing to international standards and have as much mutual recognition and harmonisation as possible so that the industry and our customers can benefit from the innovations that exist.

The last of the areas of priorities I am going to outline is actually a little different from the first two. We really think there is plenty of opportunity and need to drive progress in international security and stability. As highlighted by Dr. Rosenthal, international law and cyber security norms are going to be important tools in this space. We see this as a particular priority, because we have seen activity that has resulted in unintended consequences which need to be mitigated, and concerns about escalatory actions that are unintended as well. So, in this space there is a great deal of opportunity below the threshold of armed conflict. There has been considerable work on confidence building measures at the OSCE and important work that has gone on in the Group of Governmental Experts. But there is still space below the law of armed conflict where we need to make progress. Something interesting is that in the absence of agreement on the acceptable and unacceptable behavior in cyberspace, implicit norms are being developed by action instead of by deliberation. That is concerning. Microsoft is working on a paper right now about some concrete norms to contribute to the conversation and help drive dialogue in this space. We look forward to sharing that with you in the near future.

In closing, this event, CyFy, and others like it bring together expertise from around the world and raise an important series of issues. We look forward to continued dialogue with you and others, and we certainly look forward to seeing the combination and aggregation of these issues at the Hague conference in 2015. Thank you so much and have a great evening.

Valedictory Address by

Mr. Arvind Gupta

Thank you, Samir, for that kind introduction. Just a small correction - it was not the semiconductor industry that I was involved in. At that time, I was involved in large-scale integration research and that was way back in 1974. I had hoped that we would bring out the first chip in 1980, because we had set up a semiconductor complex that year. But somehow, things did not move the way they should have and India is not producing chips today. This is perhaps one of those missed opportunities. I think India has missed several opportunities over the last 30-40 years, but I must not become too frank because I realise I am now back in the government.

So, thank you very much for asking me to give this valedictory address. I am quite conscious of how difficult it is to speak as the very last speaker of a conference which you have not attended. So, what do I do? You already have in this conference a number of speakers who have spoken, some top

experts, and I think you would come out with a report. So I start the easiest way by thanking the organisers for actually bringing this forum together - and this is the second one, if I am not mistaken, I attended the last one also. Sustaining this forum is very important, and as it goes forward, the quality will only increase and there will be more intense discussions. I may not have anything startling new to say in my remarks because already some rich discussion has taken place in this conference. I am also conscious of the fact that I speak in front of Latha Reddy, who was my predecessor three years ago and she has played a very important role in evolving the cyber security framework in India, which I will briefly mention. But if you have any questions, please address them to her.

Raja Mohan's summary was superb and I am going to take a copy from him. We will try and put it in our government notes and say that India is thinking about cyberspace, that these are the ideas which have actually been generated in this forum. You have considered some excellent themes like cyber crime, cyber terrorism, nature of social media, protection of critical information infrastructure, online privacy, norms in cyberspace and some issues of internet governance - this, I think, is a synonym for that M-word, multistakeholderism.

Let me begin by saying that as a major user of cyberspace, India has a substantive presence as both a consumer and a provider of content. I think that is a very important facet of India's dealing with cyber security issues. You may have heard this, I think it was mentioned in one of your briefs, that the number of mobile phones in India is now touching about a billion, which is a huge number; 300 million people are already using the internet, which is of course a low density but in absolute numbers is still quite huge. More people are now beginning to access the internet through mobile phones and desktop computers, and these trends are likely to grow in the future and at quite a rapid pace. The potential of cyberspace for developing countries like India is unbounded. I think the opportunities are just opening up and we have seen that the new government has taken up some ambitious governance schemes which will rely on information technology and IT-enabled services.

Under the Digital India programme, miles of connectivity will be ensured. E-governance initiatives will multiply and our villages, probably 250,000 villages out of about 500,000 village panchayats, will have services delivered online. The internet will be widely used in improving governance for efficient delivery of services in education, health, medicine, transportation, energy, infrastructure and financial sectors. The digital connectivity and physical connectivity, the two priorities of the government, will go hand-in-hand. I was mentioning to Dr. Rosenthal, whom I met this afternoon, that the scale of the problem in India is huge. So what the Netherlands can do very quickly, we may take much longer simply because of the scale involved. So, while information technology will be used to bring about economic growth and social connectivity, there are serious challenges which need to be addressed.

The cyberspace has a dark side to it, which you would have discussed. Cyber security becomes an extremely important area for those who are designing and implementing digital information infrastructure in India. It is a challenge how to incorporate cyber security right from the beginning when these schemes are being conceptualised, and cyber security is a must, ironically, for free flow

of information. Threats in cyberspace are difficult to deal with due to the borderless nature of the medium, rapid changes in technology, the difficulty in attribution and the lightning speed at which vast amounts of information move through cables across the borders and with massive consequences.

Social media, which was mentioned, is another area of growth and is also a cause of concern. In India more than a 100 million people are already on Facebook, 33 million people on Twitter and 26 million on LinkedIn, and these numbers are growing exponentially. Even as social media creates tremendous connectivity and becomes a powerful catalyst for growth, it brings with it its own challenges: It can be misused for accentuating ethnic and social discord, for example, and this I speak from India's experience. So, we have experienced both positive and negative impacts of social media. Cyberspace has grown as a free medium and is almost akin to a global commons, if not one already. Billions of people worldwide are using the internet freely, but we have seen in recent months - and this conference also discussed this - a sharp but inconclusive debate on multistakeholderism versus multilateralism in the context of internet governance. What I could gather from Raja Mohan's summary, he did not use the word "contradictions" but "antinomies", which is a play on words. Whether it is antinomies or contradictions, we will have to see because it is a new area, and the debate essentially boils down to the question of whether the internet should be regulated, can be regulated, and how we do it if we have to do it.

Several models have been talked about but no consensus has yet emerged, and I have a feeling it is going to be a long time before such a consensus emerges, although I think we can reach that point. Whether you take the arms control issues, nuclear issues, chemical weapons, the Law of the Sea, or any number of other regimes, it took decades before we could come to any conclusions. But even today, the Law of the Sea has problems, the space regime and many other regimes have problems. So, cyber is going to experience, I suspect, a similar situation, where we will be discussing these issues for a very, very long time to come. But the need for balance was pointed out by Raja Mohan. A balance needs to be brought about among these various poles of contradictions or antinomies. What has emerged, in the recent past, is the increasing assertion by states that state sovereignty should be respected in cyberspace as well and that the state is an important and legitimate stakeholder in cyberspace. I think that cannot be doubted because you have so many stakeholders - this point was very well brought out in the summary Dr. Raja Mohan gave us. However, the precise role of states in the regulation of internet is not yet determined and there is no unanimity on this question as yet.

Here, a word about cyber conflict, which was also mentioned. It is a very delicate situation when you realise that in the entire spectrum of conflict, starting from low-intensity conflicts to the highest, i.e. nuclear, now cyberspace is also fitting in somewhere, and there is a link, and I think these are the issues which need to be discussed; they are being discussed, but again, there is as of yet no consensus. So, issues of cyber warfare, information security, cyber terrorism, cyber crime, etc., can trigger a conflict. How the conflict will be triggered, what will be the nature of conflict, how will you contain it - these are some big issues that are being discussed.

On the issue of internet governance, again, the positions are evolving. The Indian position, which was articulated at NETMundial in April 2014, emphasised the need for making the internet governance regime representative and democratic in the spirit of the Tunis Agenda of WSIS 2005, i.e. the World Summit on the Information Security. This is the basic position, but I think it needs to be fleshed out as discussions proceed.

In recent years the question of norms of state behaviour in cyberspace has assumed urgency. Recognising that information and communication technologies have reshaped international security environment, the June 2013 report of the third UN Group of Governmental Experts, of which India was a member, had recommended that norms derived from existing international laws are relevant to the use of ICTs and are essential to reduce the risk to international peace and security and stability. The fourth GGE has already held one meeting and these issues will be taken up further.

Unfortunately, this time India is not a member of the UNGGE, but some of the gentlemen who are here that I have met said that they will remain in touch. The Indian position on these issues will continue to evolve and we will be happy to keep these conversations flowing. The June 2013 report also stated that international law, in particular the Charter of the United Nations, is applicable and essential in promoting an open, secure, peaceful and accessible ICT environment. However, the debate on norms is still inconclusive. What these norms should be and how this should be implemented is yet to be determined.

As I was mentioning to some of my friends here, I think UNGGE is a useful forum, but it should be made more representative. Perhaps it should also be considered whether its remit could be expanded to take into account some of these issues we've highlighted in this closing session. Raja Mohan also raised the issue of legitimacy. Whatever we do in cyberspace should be legitimate. So, I think some UN forum needs to be devised where these issues can be discussed in a legitimate fashion.

For the forthcoming ITU Plenipotentiary Conference in Busan, South Korea, which is being held in October-November, India has submitted a paper on Internet Related Public Policy. It emphasises that the policy framework of an internet governance system at the international level must involve the governments of various nations through mutual consultations and negotiations. In the same sense, governments also need to involve all the stakeholders in the consultation process before they come out with their positions.

India is dealing with the challenges of cyber security in multiple ways. One of the most important steps taken has been the formulation of National Cyber Security Policy in May 2013 and the conceptualisation of a cyber security architecture (where Ambassador Latha Reddy has played a major role) under which critical cyber security institutions will be constructed. I will read out the salient aspects of this: Operationalisation of National Critical Information Infrastructure Protection Centre; establishment of the National Cyber Coordination Centre for threat management and information sharing in real time; establishment of cyber security assurance and

certification bodies for testing, evaluation and cyber security audits; creation of a research and development fund for setting priorities for research; indigenisation and human resource development. A very important part of this architecture is the public-private partnership on cyber security. We have a joint working group, which has met several times, and we have been discussing some of the issues of market, etc., and how the government and the industry can have a dialogue and consult each other and be equal partners. I think this dialogue will go forward. Another extremely important issue is capacity building. That is a very big term. It will be the focus of our efforts in future, which also include the creation of nearly 500,000 cyber security professionals. How to do it, what infrastructure to make, what ecosystem to make - here, too, the private sector will be involved. India is now engaged in implementing some of the policy initiatives and these are in advanced stages of implementation. We are hopeful that sooner rather than later, India will have a cyber security architecture in place.

International cooperation is a very important part of India's cyber security policy. We already have a number of cyber security dialogues. We have a very involved dialogue with the US and we have, I think, four or five other countries with which we have a major conversation going on. I think we can further expand our reach. A number of technical dialogues between agencies are also taking place. Technical institutions like the CERT India, STQC, which is the standards organisation - and standards are very important - are also cooperating with their international counterparts.

What are the challenges before us? Since we are dealing with an extremely difficult issue, there are a number of challenges to tackle. Early implementation of the cyber security policy and architecture, finding the necessary resources - human resources, financial resources - and getting public-private partnerships going are some of the challenges that we face. As I have mentioned earlier, human resources is a big issue; we should have a large pool of cyber security experts, professionals in very large numbers - we are talking about millions here - to step up research and development in high-technology areas in order to make cyber security products and services and make India a manufacturing hub.

As you know, the Prime Minister has been talking about Make in India, and this is across sectors. I think cyber security provides an excellent area where we can begin to implement Make in India, which means our universities, our institutions should have the necessary infrastructure to produce experts. Then, we should have public-private partnerships to manufacture some of these products, and of course have in place the required ecosystem, i.e. testing, evaluation, etc. So, India is at a point where if we produce cyber security products and services, and collaborate with partners, it will also address other important issues: It will help fulfil the Make in India goal, it will provide jobs and it will also take advantage of the fantastic demographic dividend that we have at this moment.

In conclusion, I would like to summarise the four-five points: Firstly, a robust cyber security architecture is being constructed in India and new capabilities in the cyber area are being built, which I believe will also affect India's negotiating position. The second point is that as geopolitics evolves, India will engage with the international community to enhance cooperation in the field of cyber security and will try and foster peace and stability, which is so important. As India becomes

more digital - and that is beginning to happen - India will have a greater presence in cyberspace and will participate in the growth of internet and internet governance to make it more democratic while retaining the free flow of information. Finally, new opportunities are arising for the private sector to take part in making India a manufacturing hub of ICTs and cyber security products.

Thank you very much.

Survey Highlights: State of the Debate 2014

Observer Research Foundation

In the months leading up to Cyfy 2014, ORF conducted a survey of Indian internet users to determine their views on a wide range of cyber issues, and lay out the 'state of the debate' in the country. The survey began with general questions about how Indians perceive the internet, and what it is used for; respondents overwhelmingly said the internet was primarily used for communication purposes. Users were also polled on questions of ownership and responsibility for internet security, testing assumptions about how much end-users pay attention to the internet in the stages before it reaches them. A majority or respondents felt that there should be greater regulation of the internet, though more than a third felt that regulation was adequate or could even be reduced. They were less decisive when questioned about who should frame such regulations, with most opting for regulation by the government or by multistakeholder groups which include users rather than service providers or international organisations.

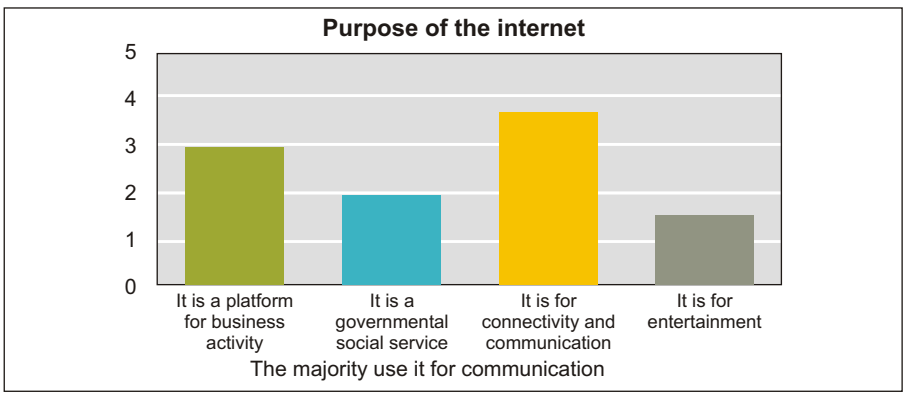
Asked about the impact of the internet on the right to freedom of expression, a significant majority were of the opinion that it had been enhanced by the internet, though more than half said that such freedom should not be absolute. This led to questions about Indian laws specifically. Most respondents were aware of laws like section 66A of the Information Technology Act and the effect they could have on internet usage, and they differed in their opinions about whether or not such laws were compatible with India's constitution. There was also general support for formalising the right to be forgotten in India, despite just over half of those surveyed suggesting that de-indexing search results went against the fluid nature of the internet.

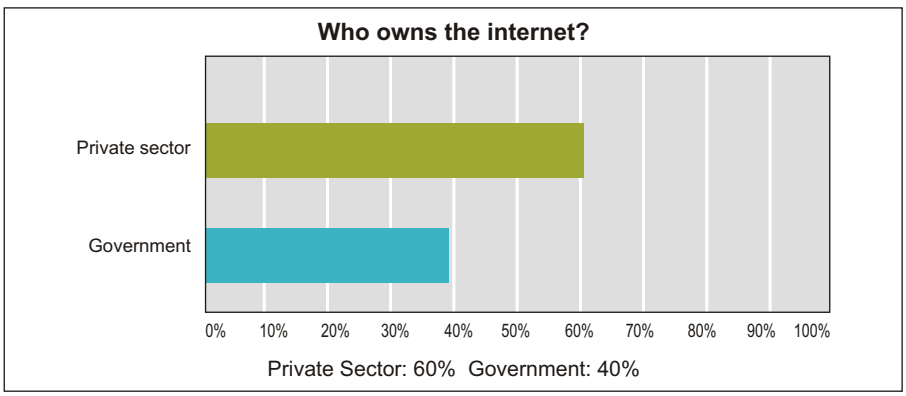
Users were also asked about their personal experiences online; most held the belief that their data was being accessed by companies providing the services they used. Close to two-thirds of respondents had been personally affected by cyber crime, with nearly the same number admitting to pirating software or downloading illegal content.

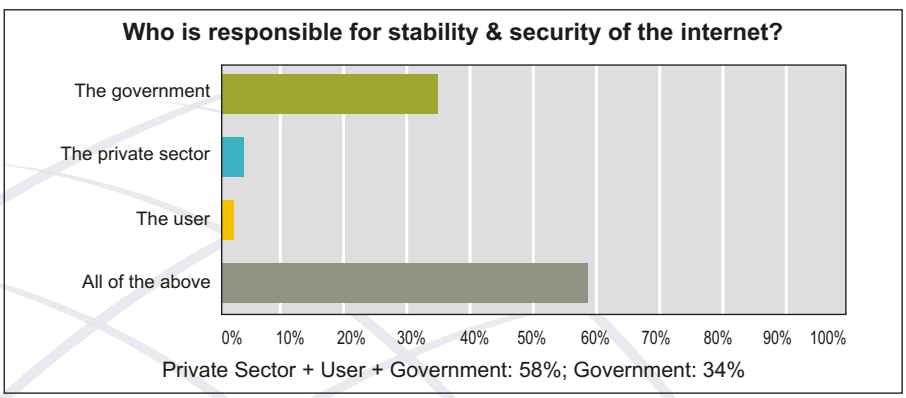
Overall respondents tended to support a multistakeholder model for internet governance. More than half of those surveyed opined that the Indian policy should be decided by the government,

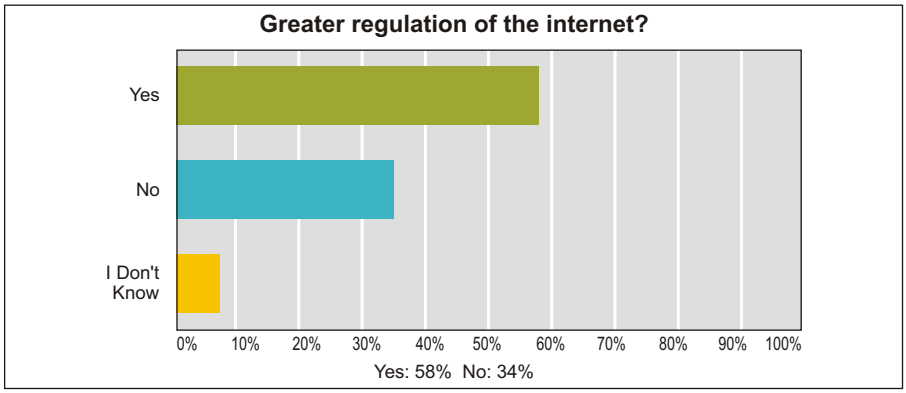
the private sector, civil society and the technical community working together. They also felt that multistakeholder groups like the Internet Governance Forum were the best platforms for India to engage with on an international level.

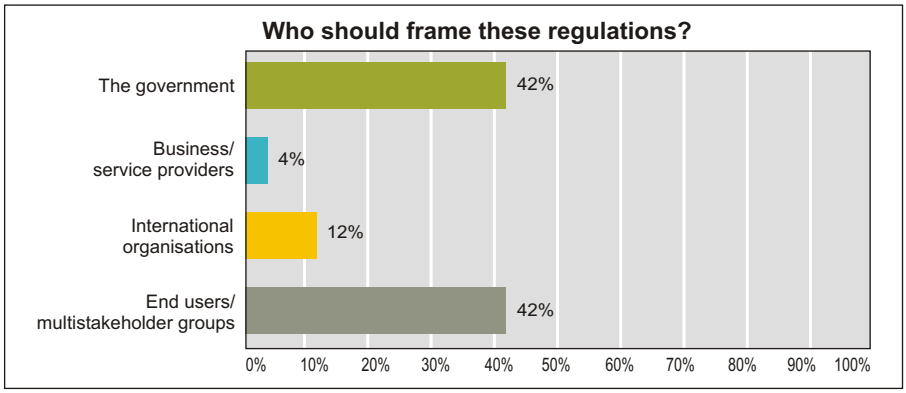
A selection of the results, displayed in the following pages, were presented for the first time during Cyfy 2014.

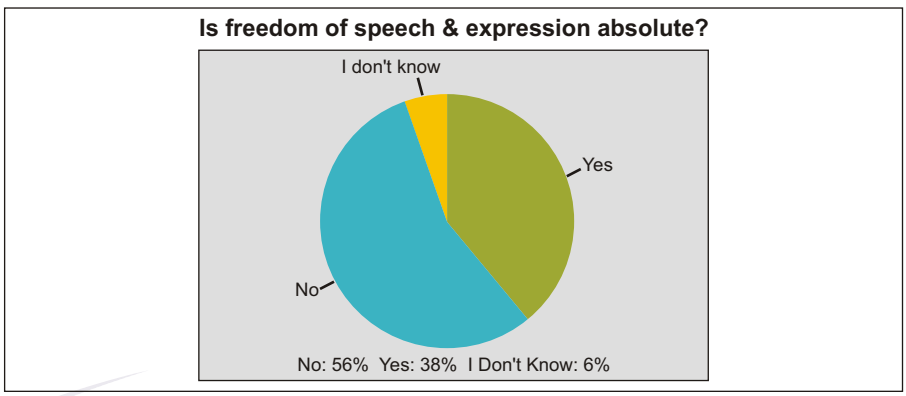


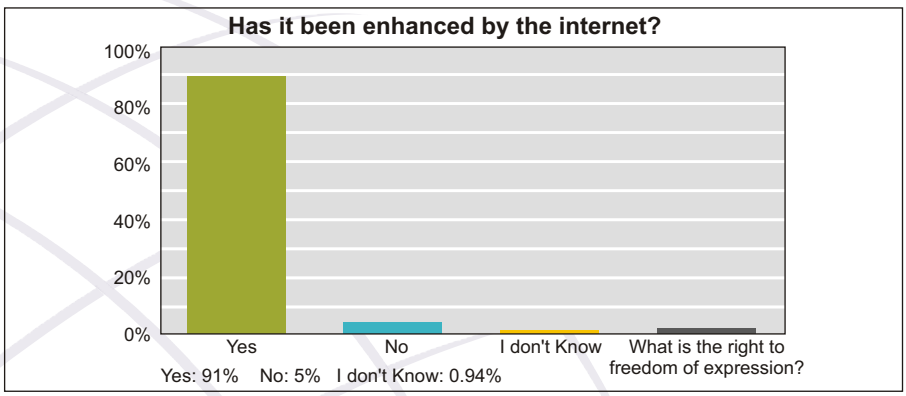


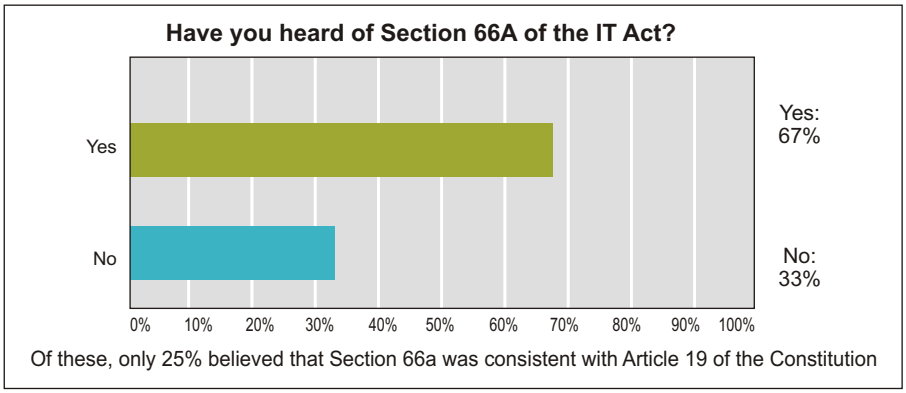


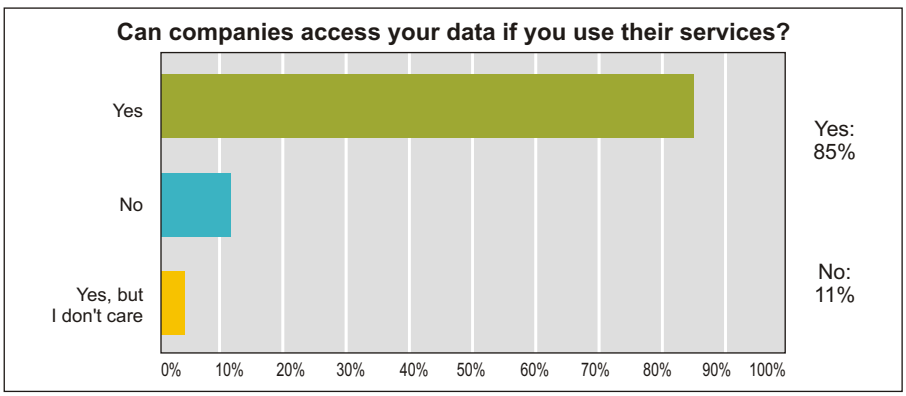

Greater regulation of the internet?
Yes
No
I Don't Know
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Yes: 58% No: 34%

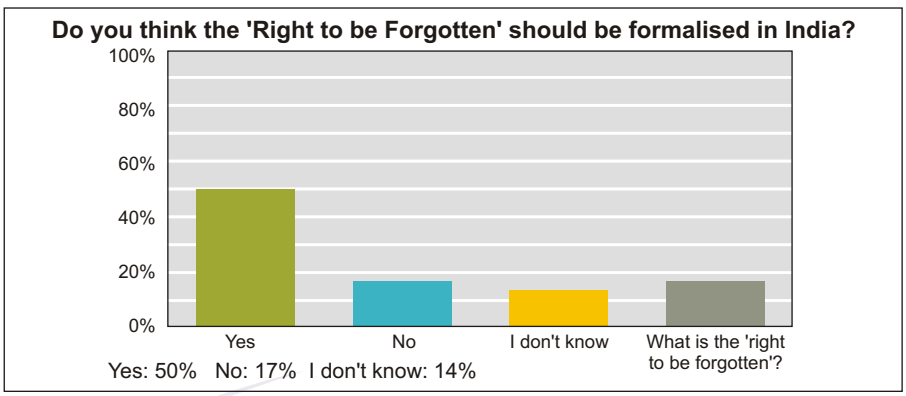

Who should frame these regulations?
The government
42%
Business/ service providers
4%
International organisations
12%
End users/ multistakeholder groups
42%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

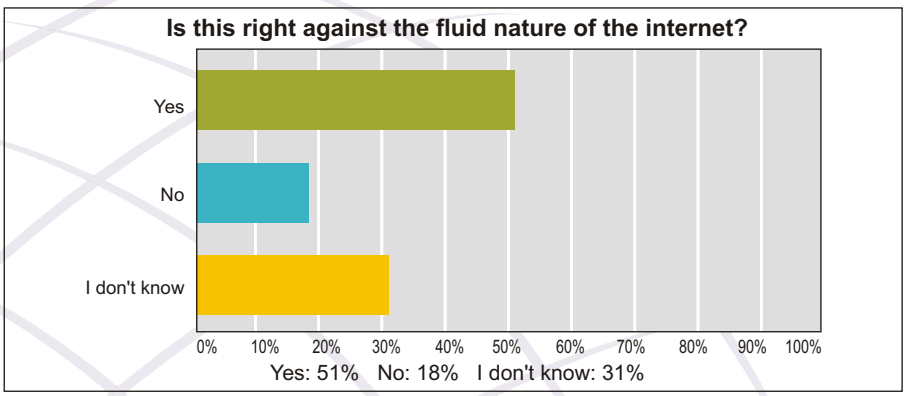

Is freedom of speech & expression absolute?
I don't know
Yes
No
No: 56% Yes: 38% I Don't Know: 6%


Has it been enhanced by the internet?
100%
80%
60%
40%
20%
0%
Yes
No
I don't Know
What is the right to freedom of expression?
Yes: 91% No: 5% I don't Know: 0.94%

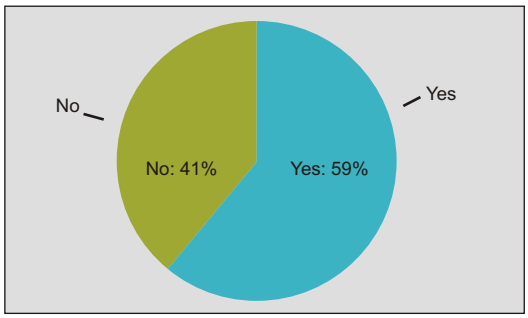

Have you heard of Section 66A of the IT Act?
Yes
No
Yes: 67%
No: 33%
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
Of these, only 25% believed that Section 66a was consistent with Article 19 of the Constitution


Can companies access your data if you use their services?
Yes
No
Yes, but I don't care
Yes: 85%
No: 11%
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

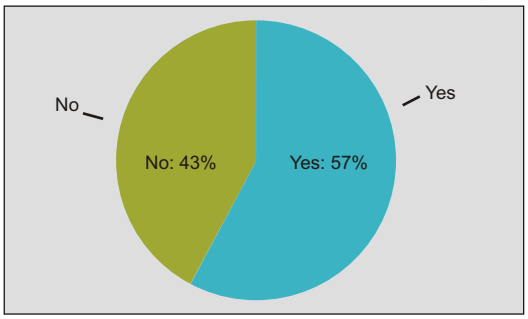

Do you think the 'Right to be Forgotten' should be formalised in India?
100%
80%
60%
40%
20%
0%
Yes
No
I don't know
What is the 'right to be forgotten'?
Yes: 50% No: 17% I don't know: 14%


Is this right against the fluid nature of the internet?
Yes
No
I don't know
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
Yes: 51% No: 18% I don't know: 31%

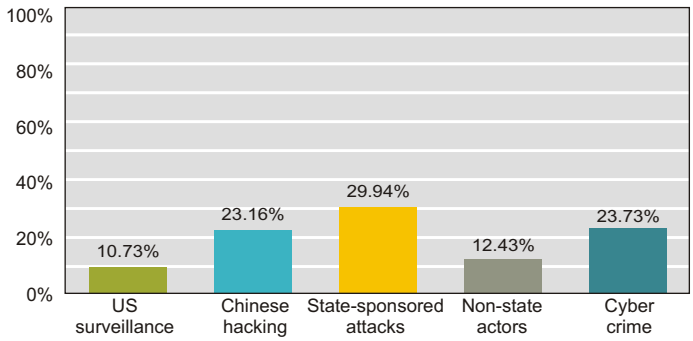
Have you been a victim of cyber crime?



Have you used pirated software or downloaded illegal content?



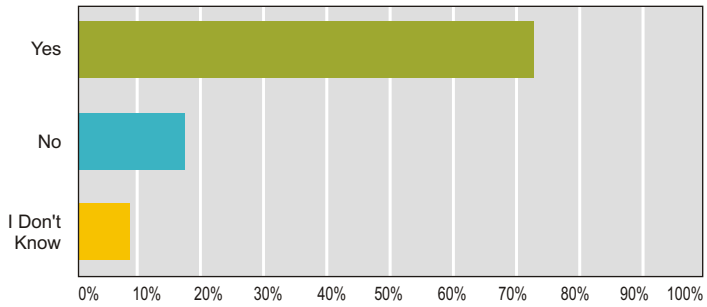
What is India's biggest cyber security threat?



Do know about e-surveillance programmes in India?

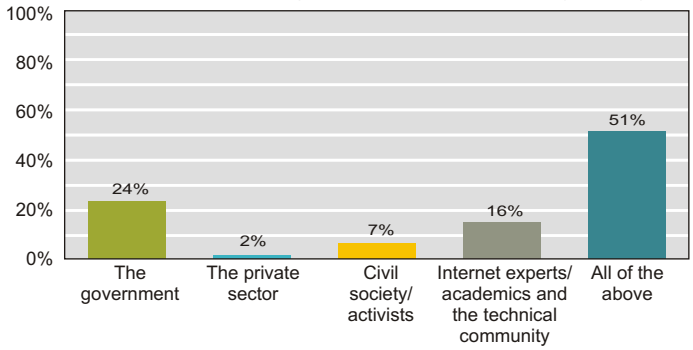
Answer Choices	Responses	
Yes	**20.83%**	40
Yes, and I think it should be there	**23.96%**	46
Yes, but I don't support that	**11.98%**	23
No	**27.08%**	52
No, and I think it should be there	**10.94%**	21
No, but I don't support that	**5.21%**	10
Total		**192**

Does this sector offer attractive opportunities and career options?

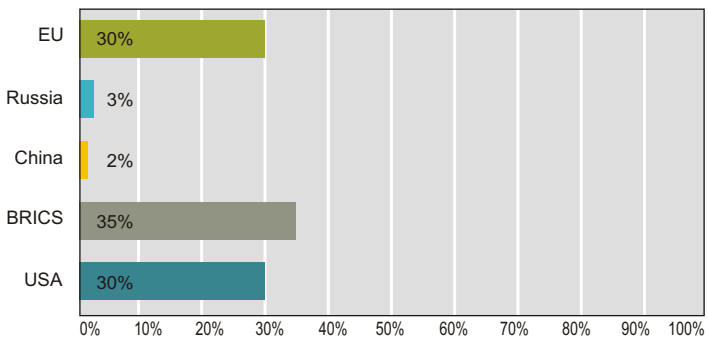


Yes: 73% No: 17%

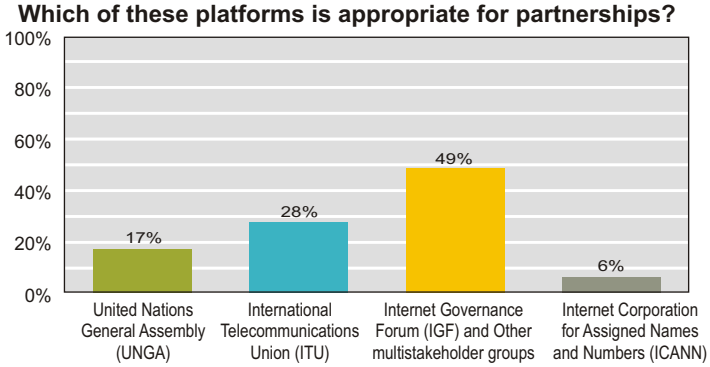
Who should speak for India on governance and security policy matters?



On internet governance and security, who should India partner with?



Which of these platforms is appropriate for partnerships?



Observer Research Foundation (ORF)
20 Rouse Avenue Institutional Area
New Delhi 110 002
India

Ph. : +91-11-43520020, 30220020
Fax : +91-11-43520003, 23210773
E-mail: contactus@orfonline.org

For details log onto: **www.cyfy.org**

To watch the conference highlights please go to:
http://cyfy.org/video/cyfy-2014-the-india-conference-on-cyber-security-and-cyber-governance/

Announcing Cyfy 2015: October 14 - 16

EVENT PARTNERS

SPONSORS

KNOWLEDGE PARTNERS