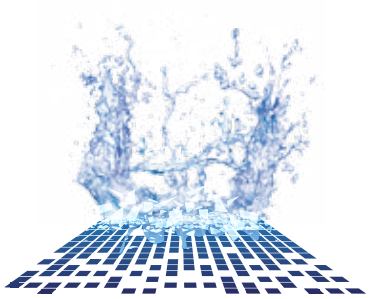

CYFY 2013

THE INDIA CONFERENCE ON CYBER SECURITY AND CYBER GOVERNANCE

14 - 15 OCTOBER 2013

OBEROI HOTEL - NEW DELHI

OBSERVER RESEARCH FOUNDATION

FICCI

REPORT

CONTENTS

CYFY 2013

THE INDIA CONFERENCE ON CYBER SECURITY AND CYBER GOVERNANCE

14 - 15 OCTOBER 2013

OBEROI HOTEL - NEW DELHI

OUTCOME STATEMENT

Cyber space transcends boundaries to provide unprecedented levels of connectivity and empowerment to states, institutions and individuals across the globe. This fluidity of the cybersphere pawns 'cyber-gangsters', necessitating cyber-security on the one hand while raising the spectre of a 'big brother' state on the other, according to the Minister for Communications and Information Technology, Mr Kapil Sibal. Inaugurating the two-day workshop, he described cyber governance as something of an oxymoron and opined that a re-imagined notion of sovereignty was essential to develop an effective cyber security paradigm. The Indian National Security Advisor, Mr Shivshankar Menon, who delivered the keynote address, said that the internet is also the government's chosen platform for socio-economic empowerment schemes. This makes India uniquely dependent on the cyber-sphere for its development, while at the same time exposing it to heightened vulnerability.

If the past is any indication, India's growth and economic prosperity will be inextricably and intricately tied to the digital sphere. Hence, India's proactive engagement in the global norm-making process is important. India can and must be a rule maker and ensure that global norms pertaining to the cybersphere align with the opportunities this space has to offer its people. Additionally, the boundlessness of the cybersphere must be protected, but not at the cost of pluralism or access. Policy objectives must aim to build infrastructure and provide security and must seamlessly align with the inexorable logic of providing greater access through enhanced penetration.

Consequently, the internet, for India and many countries indeed, is a means and medium of greater freedom and democratisation. Therefore, discovering the median between access and security becomes a global imperative. Given India's democratic ethos and the sheer volume of cybersphere, it does (and will) account for India's policy responses which will inevitably shape the future of cyber space, its management and governance.

It was against this background that the inaugural and most comprehensive 'India Conference on Cyber Security and Cyber Governance – CyFy 2013' was held at New Delhi on October 14 & 15, 2013. Supported and guided by the Raytheon and the Bombay Stock Exchange, the event saw two days of engrossing debate, capturing the perspectives of over 250 international experts, parliamentarians, academics, industry leaders, media practitioners and civil society.

The gathering at CyFy 2013.

The following key conclusions emerged from the discussions:

» The tension between "multistakeholderism" and multilateralism should be resolved to further a cooperative framework in formulating cyber-security strategies. It is only with the participation of diverse stakeholders that a refined, legitimate and nuanced policy can emerge. A unilateral approach without systematic and periodic consultations with, and inputs of, the widest sets of stakeholders will be deeply counterproductive and can undermine the democratic nature of the cybersphere. However, the mechanism should be fair and equitable and inclusive for all parties involved.

» International cooperation is a must in responding to cyber-security threats and governance challenges. Conventions and treaties ensure agreed definitions on security issues, acceptable norms, confidence-building measures and will eventually shape an international framework to manage cyber space.

» Cooperation is beneficial in managing inter-dependencies that are inherent while seeking cyber-security, for which regional and bilateral cooperative measures can also be devised successfully. For instance, internet fraud and related crimes can be a potential area of cooperation given the minimal political underpinnings.

» It was emphasised that cooperation could be compromised by the national strategic interest of major powers and by viewing this space as a new 'zero sum game'. The tensions between great powers can undermine a multilateral approach to cyber-security and will have an asymmetrically negative impact on lesser powers.

» Public and private sector partnership (PPP) in policy-making is essential as the bulk of communications and certain critical information infrastructure networks are managed by the private sector. An information-sharing mechanism should be created to ensure timely responses.

» The bulk of cyber-security costs are currently being borne by the private sector. Like all issues related to national security, the government must take the lead, incentivise and guide developments in this sector and allocate specific funding. This funding should be spent on awareness campaigns, education, stakeholder consultations and capacity-building initiatives in the near to medium term. Similarly governments should invest in initiatives that improve cyber hygiene and data protection. A critical skills shortage exists and there should be an emphasis on training 'cyber builders' rather than 'cyber warriors'. PPP models and certifications regimes should be rapidly introduced to ensure both quality and numbers.

» Governments must standardise security measures, protocols and surveillance processes in order to ensure that they are neither sector-specific nor applicable only to individuals or companies. Greater transparency around security processes will also increase user confidence and allow greater vibrancy in spread and adoption of cyber platforms. This is important as the Government of India (GoI), like many other national governments, sees digital last mile connectivity as the most efficient mode for government-citizen interface in social and related sectors.

» There is today a collision of narratives on National Security and Individual Privacy. While this debate is important to have, the ideal for any security policy must be safe-guarding the private space of individuals and their freedom of expression. Governments have been unable to define and agree to a universal definition of "privacy" and due to the borderless nature of the internet there will be contests and hence there are concerns voiced by many stakeholders that need to be addressed.

» Additionally, collective security often gets an unfair advantage over individual privacy. Some questioned the efficacy of these security measures and if the gains from surveillance are worth the costs to privacy and whether there are alternatives to safeguarding national security while keeping privacy sacrosanct.

» It did appear from the discussions that privacy and national security concerns do not necessarily have to compete with one another. Concerns over security measures can be addressed by embedding privacy presets into surveillance mechanisms ab-initio. Targeted surveillance has proven effective, but too much surveillance is demonstrably counter-productive. More investment is needed to ensure privacy enhancing technologies along with sensitising the personnel who deal with the data while conducting surveillance. At the same time, discourse should not put a false dichotomy between free speech and privacy on one hand, and security in cyber space on the other. Stakeholders need be able to agree on the nature of regulation required to continue running an unhindered cyberspace.

» Certain core ideals must be preserved and propagated with respect to privacy. And creating a universal common and robust approach to privacy should be a key global objective to work towards. Such a definition would necessarily be the basis for any future rules-based cybersphere governed by internationally accepted norms.

» The issue of verifiable cyber-identity is also a contested one – on one hand being necessary to prevent crime but on the other being prone to abuse. The issue of identity is intricately linked to the notion of anonymity. A third party management of identity verification is a possible solution but one that requires extensive trust building between the various stakeholders.

» Transparency and accountability in formulating cyber policies, empowering non-government organisations (NGOs) as pressure groups, widespread consultation, research initiatives, public participation, and a robust media are all needed in order to help formulate effective cyber governance and security architecture. An international cyber management framework can establish best practices and norms. This framework can also analyse risks and create deterrence mechanisms and alliances.

To quote the Deputy National Security Advisor of India, Mr Nehchal Sandhu: "India has a national cyber-security policy, not a national cyber-security strategy." Policy is the route to building strategy but strategy is the articulation of an assessment of objectives, needs and aspirations of what citizens seek in a secure and democratic cyber space. CyFy 2013 is a first step in this process. It has initiated a plural and honest attempt to discuss, contest and discover contours of a national cyber strategy by bringing together domestic and international stakeholders and specialists, initiating the right conversations and encouraging debates that are critical to the formation of an enlightened cyber strategy for India.

SAMIR SARAN

Vice President
Observer Research Foundation

VIRAT BHATIA

Chair, Communications and
Digital Economy Committee, FICCI

INTRODUCTION

The rapid evolution of technology and the near omnipresence of the internet now mean that technical and policy-related challenges in the realm of space are mounting rapidly for both governments and other stakeholders, including the private sector, civil society, academia and the youth. Even as this virtual space allows unparalleled connectivity and communication, it is quickly becoming contested territory. People and nations are becoming critically dependent on inherently vulnerable and heavily networked infrastructure. Most militaries, organised crime syndicates, secret services and other actors have realised the underlying strategic potential of these critical vulnerabilities. Militaries can be disabled to alter defence postures. Critical infrastructures in public and private spaces can be manipulated to destabilise nations. Economies can be weakened through acts of sabotage and espionage. People can be polarised and mobilised through the nexus that is the World Wide Web.

None of these postulations are based on future scenarios. Each of them has been proven right in recent times. In spite of its life-altering advantages, the discourse around cyber space seems to be increasingly becoming securitised. However, cyber security can itself become a threat when abused, and cyber security strategies could place freedom and democracy, as we know them today, at risk. Dictatorships already exploit the notion of 'cyber threats' as an excuse to strengthen surveillance and censorship practices in their countries without appropriate oversight. Clearly, freedom of expression and privacy will be challenged and altered in many ways. Moreover, the role of the

Participants and Organisers of CyFy 2013: The India Conference on Cyber Security and Cyber Governance.

private sector, civil society, academia, technical communities and media is being redefined in a space that has been the traditional preserve of governments.

The time is right to comprehensively address the changing discourse. New threats from highly skilled, well-resourced multi-spectrum, non-State actors have to be acknowledged. New response strategies have to be formulated and significant impetus built towards capacity building to create the next generation of cyber defence warriors, given that traditional policing, prevention techniques and mindsets are likely to be ineffective and counter-productive. Additional problems associated with cyber security need to be tackled including technical, market and policy failures. Furthermore, the cost of implementing a national cyber security plan needs formal recognition in a government's budgetary process.

These issues need further and continuous deliberation. To this end, a Global Cyber Security Dialogue began in 2011 in London, continued with a second edition in Budapest, and was carried forward in Seoul in October 2013.

THE INDIA CONFERENCE ON CYBER SECURITY AND CYBER GOVERNANCE: A TURNING POINT

At a national level, this task is perhaps equally important for emerging countries that are characterised by lower connectivity and relatively lower dependence on IT infrastructure in the immediate future. They have a tendency of underestimating the nature, source and the intensity of 14 & 15 October 2013 cyber attacks in the future. However, they can learn from the experience of high-tech communities to create proactive, robust information societies, more sensitive and sceptical to informationalization and networking. This would enable the creation of new technological and strategic paradigms, which in turn the established information societies might learn from as well. Addressing these questions jointly and cooperatively, including by appropriate engagement of multi stakeholder groups is clearly beneficial. Nations states will have to respond to the challenges of this cyber-age through an unprecedented level of technical and legal collaboration. Trust will be key. Yet some experts see this as a 'zero-sum-game' and are creating strategic postures for national security purposes. Reconciling the two agendas for this most dynamic global common will be the central challenge of our times.

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

PROGRAMME AGENDA

SESSION I:

INAUGURAL SESSION

Welcome by **Sunjoy Joshi**, Director, ORF

Welcome by **Virat Bhatia**, Chair, Communications & Digital Economy Committee, **Federation of Indian Chambers of Commerce and Industry, INDIA**

Keynote Address by **Shivshankar Menon**, National Security Advisor, Government of INDIA

Inaugural Address by **Kapil Sibal**, Minister for Communications and Information Technology, Government of INDIA

Vote of Thanks by **C. Raja Mohan**, Distinguished Fellow, ORF, INDIA

SESSION II:

SOVEREIGNTY, INTERNATIONAL COOPERATION AND CYBER SECURITY: A TREATY DIALOGUE

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

MODERATOR

John C. Mallery, Research Scientist, MIT Computer Science & Artificial Intelligence Laboratory, USA

PANELISTS

Dirk Brengelmann, Commissioner for International Cyber Policy, Federal Foreign Office, GERMANY

C. Raja Mohan, Distinguished Fellow, ORF, INDIA

Boris Vasiliev, Expert, Department of New Challenges and Threats, Ministry of Foreign Affairs, RUSSIA

SESSION III:

THE FIRST LINE OF DEFENCE: THE PRIVATE SECTOR

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

MODERATOR
Vivek Lall, President & CEO, Reliance Industries Limited, INDIA

PANELISTS
Vijay Madan, Chief Mentor, Tata Teleservices Limited, INDIA

Joe Sullivan, Chief Security Officer, Facebook, USA

Gabi Siboni, Director, Cyber Warfare Program, Institute for National Security Studies, Tel Aviv University, ISRAEL

Kersi Tavadia, CIO, BSE Limited, INDIA

SESSION IV:

CYBER SECURITY: STRATEGIES AND RESPONSES

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

MODERATOR
Arvind Gupta, Director General, Institute for Defence Studies and Analyses, INDIA

PANELISTS
Nehchal Sandhu, Deputy National Security Advisor, Government of INDIA

Michael F. Gaul, Senior Advisor, Emerging Security Challenges Division, NATO

Oleg Demidov, The Russian Center For Policy Studies, RUSSIA

SESSION V:

DINNER TABLE ADDRESS ON "FREEDOM OF EXPRESSION IN THE INTERNET AGE

SPEAKER
Manish Tewari, Minister of Information and Broadcasting, Government of INDIA

SESSION VI:

KEYNOTE ADDRESS

SPEAKER
Jaak Aaviksoo, Minister of Education and Research, Republic of ESTONIA

SESSION VII:

IMPLEMENTING NATIONAL CYBER SECURITY POLICIES

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

MODERATOR

Virat Bhatia, Chair, Communications & Digital Economy Committee, Federation of Indian Chambers of Commerce and Industry (FICCI), INDIA

PANELISTS

Ram Narain, Deputy Director General (Security), Department of Telecommunication, Government of INDIA

Peter Grabosky, Researcher, Australian National University, AUSTRALIA

Jaak Aaviksoo, Minister of Education and Research, Republic of ESTONIA

SESSION VIII: INTERNATIONAL PUBLIC PRIVATE PARTNERSHIP IN CYBER GOVERNANCE

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

MODERATOR

Gabi Siboni, Director, Cyber Warfare Program, Institute for National Security Studies, Tel Aviv University, ISRAEL

PANELISTS

John C. Mallery, Research Scientist, MIT Computer Science & Artificial Intelligence Laboratory, USA

Eric H. Loeb, Vice President, International External Affairs, AT&T, USA

Prakash Nagpal, Senior Vice President, Product Marketing and Marketing, Narus, INDIA

Jennifer McArdle, Program Associate, American Association for the Advancement of Science, Center for Science, Technology and Security Policy, USA

SESSION IX: PRIVACY AND NATIONAL SECURITY

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

MODERATOR

Gulshan Rai, Director General, Computer Emergency Response Team - India (CERT-IN), Government of INDIA

PANELISTS

M.M. Oberoi, Indian Police Service, Joint Commissioner of Police, Delhi Police, Government of INDIA

Rajan Mathews, Director General, Cellular Operators Association of India, INDIA

Sunil Abraham, Executive Director, Centre for Internet and Society, INDIA

SESSION X:

MULTISTAKEHOLDERISM: AVOIDING THE PRISM PARADIGM

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

MODERATOR

Barkha Dutt, Group Editor, NDTV, INDIA

PANELISTS

Anja Kovacs, Internet Democracy Project, INDIA

Virat Bhatia, Chair, Communications & Digital Economy Committee, FICCI, INDIA

James Clarke, BIC, Project Coordinator, Waterford Institute of Technology, IRELAND

VALEDICTORY ADDRESS

Nehchal Sandhu, Deputy National Security Advisor, Government of INDIA

RAPPORTEURS FOR CYFY 2013:

James Clarke, BIC, Project Coordinator, Waterford Institute of Technology, IRELAND

Rahul Prakash, Junior Fellow, Observer Research Foundation, INDIA

Kanchi Gupta, Junior Fellow, Observer Research Foundation, INDIA

INAUGURAL ADDRESS

by KAPIL SIBAL
Minister of Communications and Information Technology,
Government of India

Kapil Sibal, Minister of Communications & IT during the inaugural address.

Distinguished delegates, first of all let me thank FICCI and ORF for inviting me here as the keynote speaker. You must have clearly understood by now that Mr. Virat has been entirely biased in my favour. I don't think that what he has told you are some extraordinary achievements, this is part of my job and this is what has to be done when you are in government.

This particular seminar which deals with cyber space and cyber security, I think is a very important event because I think the time has come for the global community to realise that this is not just our problem, it is everybody's problem. It is not just an individual's problem, it is just not a community's problem, it is not just one nation's problem, but it is a global problem; therefore, we need to address it together. Never before in the history of mankind will we create another world beyond the physical world. Our defence systems would be interconnected or atomic energy systems or nuclear installations will be interconnected, our aviation sector will be interconnected, our power grids will be interconnected, our public services systems will be interconnected, our commerce will be

interconnected, our transportation systems will be interconnected, and we will be creating an entirely different world away from physical world. Now, what is going to be the architecture of that world and how are we going to secure it? Is security an essence of creating that new world? I have to say that much of that world has been already created without interference from government organisations or third parties. Much of that world has been created because of the enormous freedom given to the communities which have been responsible for creating that world. In fact, over the last 15 years, 10 per cent of the GDP of the global community has increased of countries where cyber space is being used for empowerment of people, has increased because of what we have done with cyber space. So, it has enormous implications of empowerment and most of that empowerment has taken place because of the enormous freedom that people have enjoyed in that space. The question then arises that having enjoyed that freedom and having taken the world forward and having empowered ordinary citizens of the world, it's time for us to realise that there is another side to the argument, which needs to be addressed and I think this particular seminar is meant to address that side of the argument. That argument emanates from the fact that in this very space, there are gangsters, in this very space there are those who seek to destroy what others have built, in this very space there are those who have created flawed software or malware to actually interfere in processes that have been set up for the purposes of empowerment of people. This is in this very space that there are forces of disempowerment working against those who are sought to be empowered. Now can you then secure this space? I have always said that governance of the internet is an oxymoron. You cannot govern something that cannot be governed because there is no subject and there is no person who determines what that subject must do. There is no ruler and no ruled. There is no sarkar and no praja in Hindi terms. So, how do you govern such a structure? Can you govern it nationally? Can you govern it locally? Can you govern it globally? What does it take to govern this cyber space globally? Who must be the partners in setting up that governance structure? Nations should be partners, civil society should be involved, security establishments should be involved, or should it be as free as the structure that was built for the purposes of empowerment of people? These are very-very serious issues that are going to confront us in years to come. How you are going to deal with issues involving violation of cyber space? What laws should apply? Whose laws should apply? Mr. Sunjoy talked about the concept of sovereignty; there can be no concept of sovereignty in cyber space because there are no territorial issues involved. There is no territory in the cyber space. It is like the sovereignty of the minds. There are no disciplines, no boundaries, and no way to stop the flow of traffic. Remember that when you talk about security, you necessarily talk about preempting attacks. We are only secure till you are attacked, but in most issues in cyber space, you will seek security after you are attacked because it is impossible to secure you before you are attacked because you are dealing with fluid space where you don't know where the attack is going to come from. You cannot possibly deal with billions and billions of people around the world because the source of those attacks can be anywhere, in any

Kapil Sibal in discussion with the audience.

situation, from any part of the world. So, how do you preempt attacks and how then do you deal with issues of security? These are real issues that are going to confront us. Nations are trying to get together to decide as to what this governance structure is going to do. You have the UN governing structure and you have also the IGF. The IGF is saying: "This is not a space where anything should be governed, we have done quite well till now, we should be quite well in the future". There are other nations who say "no, we should have an ordered governance structure in order to ensure that we are protected from cyber attacks". Of course, these are real issues in the the context of national security.

Let me just give you my own view of what is going to happen in the future unless we get our act together. I think this debate is going to go along the ways the climate change debate has gone along. I am afraid, because everybody knows what the threat is. Everybody knows that by 2050, temperature is going to rise exponentially in this country and the world, but nobody is going to do anything about it because you need to protect yourselves. You are not willing to move forward in the global scenario because what is most important to you is your own way of life. I am afraid that is the same thing that is going to happen in cyber space because those who create information will protect their information. Those who are interested in their own security will protect their own security. Those who are the source of empowerment will seek to continue to empower themselves and disempower others. There will be no meeting ground unless the world stands up and says "this is not a space in which we can have a free-for-all situation where anybody can do what it likes to destroy the structures that have been built for the service of the people." I cannot imagine a situation where a whole power grid which distributes electricity to millions and billions of people is disturbed by a cyber attack and people just watch and see the havoc that is caused. We cannot imagine a situation like that. I think that this is something that I have said before in conferences as well, the internet space cannot be a free-for-all. At the same time, the freedom of the internet space is the source of empowerment. How do you make the two meet is the challenge that the global community has as we confront some of the situations that are before us. We have to ultimately conceptually first deal with it and conceptually the internet must become the equinet. We must move from the internet to the equinet. That space must be an equitable space, a space that protects our security not just at the individual level but at the national and local and regional levels. We need to protect our systems that can in fact, if malware is introduced in them, destroy the very future of nations and the future of communities.

That can only happen with others recognising the fact that their own protection is as important as the protection of their neighbours. If I may take a homely example, when you are in a homestead you feel protected because you feel that nobody is going to interfere in that homestead. You feel that there is a law-and-order machinery out there which will preempt such attacks and in the event such attacks take place, there is a belief that then those will be dealt with; therefore, in your home within your house, you feel secure. Can we bring about the same kind of security as we share in our homesteads where we live and what kind of architectural structure should be bring about to ensure that homestead security? That's really the challenge that we are confronted with.

Talking about sovereignty, I don't think there is an issue of sovereignty here. What is sovereign is data, not nations. What is sovereign is the integrity of that data. What is sovereign is not the power of data, but the use of data. Therefore whether it is used by an individual for purposes of privacy as in healthcare or in commerce,that must be protected because it is as important to protect that data as it is to protect national security. I don't think that we should actually weigh these two things because each needs to be protected and protected with passion, and unless we realise that I don't think we are going to bring about an equitable world in the future because the world of the 21st century is going to be entirely different from the world in the last 20 centuries. This world will be a new era of global cooperation where research is take place across boundaries, where intellectual property is going to be created across boundaries, where business activity is going to take place across boundaries, where sales and purchases are going to take place across boundaries, where healthcare is going to be delivered across boundaries, where education is going to be delivered across boundaries, and where security must also be protected across boundaries. If you realise that I think we would have won the battle. This is just a first step and I hope this seminar brings about some results. Thank you.

KEYNOTE ADDRESS

by SHIVSHANKAR MENON
National Security Advisor, Government of India

Thank you for asking me to speak to you at this timely conference on a topic of increasing importance. The quality and nature of participation in your conference from different sectors in India and from around the world is testimony to the broad interest and topicality of these issues. It also shows increasing recognition of the partnership that cyber security and governance require in order to be effective.

To tell an audience such as this about the significance of cyber security, or to describe the threats and risks we face in cyber space, would be to preach to the converted. Let me instead briefly describe to you what we have been doing to enhance our cyber security in India and then make a few general points about international cyber governance.

India today has the largest number of internet users after the USA and China. But internet and

NSA Shivshankar Menon delivering the keynote address.

communication technology use in India has its own characteristics. There are over 850 million mobile phones and about 670,000 km of optical fibre laid across the country; many of our major socio-economic programmes are delivered on IP based networks; and government and private sector networks are intimately interconnected. Overall levels of interconnectivity may be low in per capita terms relative to advanced economies, but the sheer numbers of people involved and the criticality of existing networks make their protection imperative. The consequences of manipulation, disruption or dislocation of networks can be potentially disastrous in terms of social order, economic loss and national security. We had an instance in 2012 of one such successful attempt resulting in the dislocation of several hundred thousand people, panicked by on-line threats and rumours. Several attempts at disruption or manipulation of Indian networks have been foiled, but we can hardly be satisfied with that. The danger remains from undiscovered attacks and others in the future.

The challenge in India, as elsewhere, lies in finding practices and policies that enable us to protect networks and cyber space while ensuring the free flow and access to information essential to a democratic society. The Government of India is strongly committed to preserving the democratic nature of cyber space, which is indeed one of its most attractive and enduring features, and the privacy of individuals, while securing cyber space for trusted e-commerce, security of data and protection of critical information infrastructure. Our citizens have a right to expect a safe and secure cyber space from government, industry, and all the stakeholders involved.

The National Cyber Security Policy and Framework approved by the government earlier this year adopts an integrated approach with a series of policy, legal, technical and administrative steps to construct a multi-layered approach and a clear delineation of functional responsibilities among stakeholders. Coordination and the sharing of information in real time will, of course, be the key to success. It also strengthens our assurance and certification framework to address supply-chain vulnerabilities, harden networks. We also will promote R&D on cyber security and capacity building.

One of the corner stones of the government's efforts is the protection of critical information infrastructure (CII). The Information Technology Act, 2000, defines critical information infrastructure as, "the computer resource, the incapacitation or destruction of which shall have debilitating impact on national security, economy, public health or safety." This is a relatively broad definition. As India's CIIs get increasingly inter-connected, inter-dependent, complex and distributed, CERT-IN tells us that they have faced a phenomenal increase in the number of cyber incidents and attacks.

CIIs will be notified under the Rules under the IT Act and a National Critical Infrastructure Protection Centre is being set up. In the meantime, the Crisis Management Plan has identified nine priority sectors for us to protect. These are defence, energy, finance, space, ICT, I&B, public essential

NSA Shivshankar Menon during his address.

services and utilities, law enforcement and security. Governments are actively partnering industry associations, service providers, and other stakeholders in joint efforts to secure cyber space. A Joint Working Group with representatives of government departments and the private sector has been set up and is looking at the establishment of Information Sharing and Analysis Centres (ISACs), testing and certification laboratories in the private sector, and Centres of Excellence for capacity building in various areas, including policy research, setting standards, cyber forensics and assistance to law enforcement agencies. We need to quickly augment our pool of skilled personnel to man the new cyber security structures.

India has recently obtained 'authorising nation' status under the CCRA regime for IT products. Testing labs in the country will now gain global recognition. This is an opportunity for industry to invest in product testing and certification facilities in India. DEITY's Standardization Testing and Quality Certification can now be a certification body and accredit private testing labs to operate the certification scheme for IT products. There has been a gratifying interest in industry to set up Telecom Testing Labs. It is our hope that with the progressive increase of manufacturing in India, CC test labs would also become viable. In the meantime we will be accepting reputed international certification while our own testing and certification facilities are being established.

Given the global and multi-national nature of ICT operations, it is not viable for each country to prescribe its own security standards in isolation. This would ultimately raise the cost of service and affect inter-operability. Hence the imperative need for international cooperation on standards and evaluation methodologies. At the same time each country has the sovereign right and duty to prescribe certification and assurance procedures and to satisfy itself as to the adequacy of the standards and that they are being respected.

India has sought to play a pro-active role in the UN Group of Governmental Experts (UNGGE) in evolving international norms of responsible State behaviour for submission to UNGA.

Our basic approach is to support democratic and representative internet governance, while preserving the strengths that come from the open nature of the domain, keeping interference at a minimum to keep it socially responsible and legal. The institutions that are invested with the authority to manage or regulate the internet should be broad based and institutionalised so as to be able to take on board the concerns and views of all stakeholders.

The internet is effectively a global commons; it cannot be managed only as private property. Its governance and architecture should reflect this fact. Take for instance the allocation of generic Top Level Domains, an issue that cannot be indefinitely corporatised. Decisions on applications for domains such as “dot Indians” or “dot ram” or “dot buddha” need to take into account national and cultural sensitivities. We must also find ways of making the internet impervious to possible manipulation or misuse by particular state or non-State actors.

How we secure private freedoms while preventing misuse of the internet, how we strike a balance between the open democratic nature of the internet and its management by a few, and still fulfill the demands of cyber security is one of the greatest challenges of our times.

There is a tendency to posit a false dichotomy or antagonism between free speech and privacy on the one hand and security in cyber space on the other. If cyber space is a global commons, as it seems reasonable to assume, there can be no absolute rights or obligations in the commons. The issue really is how much and the nature of regulation that we can agree among all the stake-holders. In India, all that the government and its agencies do in cyber space, whether it is monitoring or data protection or regulation, is governed by law, by the Indian Telegraph Act and the Information Technology Act. These laws do not distinguish between Indians and foreigners for these purposes.

This is not the first time in history that we face such questions with new and potentially disruptive technologies which rapidly become indispensable and ubiquitous. When aircraft, wireless and radio first began to be used, we heard similar arguments about controlling, limiting, monitoring and internationally safeguarding against the misuse of these technologies. What we ended up with was different from what was so passionately advocated in those debates and was certainly not what was originally envisaged. No doubt it will be the same with ICT in the future.

You will no doubt consider these aspects in the course of your conference, and I look forward to learning of the results. I wish you every success in your deliberations.

SESSIONS

SOVEREIGNTY, INTERNATIONAL COOPERATION AND CYBER SECURITY: A TREATY DIALOGUE

Moderator: JOHN C. MALLERY
Panel: DIRK BRENGELMANN, C. RAJA MOHAN, BORIS A. VASILIEV

Given the global and often borderless nature of cyber security issues, it is increasingly becoming difficult for nations to take a narrow sovereign approach while dealing with these issues. The questions is, if this is the trend is likely to continue, how can true international cooperation be attained if companies, governments and researchers do not share information with other nations? In this larger backdrop, participants discussed various issues including internet governance, which has been addressed in a number of forums such as the International Cyber conference in Seoul and the Internet Governance Forum in Indonesia in 2013. The discussions also covered how Indian laws and views can be coordinated with international norms and the challenges to becoming a signatory to any international treaty or convention on cyber security.

There is a need to address the technological, legal and societal approaches as they are critical to successfully dealing with the challenges in cyber space. Moreover, "when it comes to the role of the state, we should always ensure individual rights are part of the debate", says Dirk Brengelmann.

A number of countries remain unconvinced by this idea that cyber security can be addressed through international conventions. It is argued that existing national laws could serve as the appropriate framework.

At the moment, the Budapest Convention is the only international treaty related to cyber crime, and is open to all countries to ratify. The countries that have signed the Budapest convention include: Australia, Canada and United States, Dominican Republic, Japan and South Africa. While Budapest Convention was a platform to initiate international cooperation to combat cyber crime, there was an assertion that it does not yield cyber security in the larger context of networks or cyber war. However, there is a feeling within certain quarters that another cyber convention is not the ideal solution.

Russia, for instance, is less appreciative of the Budapest convention as it seeks a different approach towards cyber crime. Boris Vasiliev stressed that Russia "stands for the development (within the United Nations) of a convention on crimes in the use of information and communication

Boris A. Vasiliev, Dirk Brengelmann, John C. Mallery and C. Raja Mohan in discussion over a treaty dialogue.

technologies, which should be universal and take into account specialities of all countries without exception should be based on principles of sovereign equality of its participants and non-interference in the internal affairs of the states".

The view stems from a sense of insecurity that the convention could enable gathering of public data by Internet Service Providers (ISPs) of other nations, which could in turn enable foreign intelligence agencies to gather and analyse this data. Germany, on the other hand, has prioritised the privacy of its citizens while discussing cyber security issues and has given less attention to data thefts.

If nations address the issue of cyber crime through different approaches based on national priorities, it would inevitably lead to a debate for an international treaty or the cyber norms approach. At the same time, nations are also relying on bilateral mechanisms such as working groups to address these issues. This leads to the question of how would nations then agree on the accepted norms on a multilateral global level? For instance, "if the US, Russia and China decide the new internet norms, would the rest of the world accept them?" questioned C. Raja Mohan. Failing to agree on an international approach could lead to a transfer of criminal activities to a country that does not participate in the process or sign on to the final outcome. Another thorn in this trajectory is the role of non-state actors. According to C. Raja Mohan, "non-state actors with state support (where the state subsequently denies involvement) are the greatest threat" to cyber security.

Thus, there is a growing need for international cooperation as cyber security threats cannot be managed by national bodies. However, Mohan said that the current discourse on cyber strategy focuses only on applying international frameworks... "it ignores national strategic interests of major powers".

Some positive inputs for an international cyber treaty were highlighted including:

- Providing definitions on issues involved;
- Generating set of norms, what are acceptable norms of behaviours;
- Promoting confidence building measures between countries;
- Imposing some limits on what states can do to each other;
- Promoting an international organisation to supervise and manage the challenges in cyber security.

Conversely, the negative points of the international cyber treaty were highlighted, including:

» Tension between multilateral approach and what the great powers end up doing. The larger players do not always match what is agreed by the community as a whole. Dealing with what the great powers do is sometimes more consequential than conclusions from a multilateral discussion.

» Tension between the great powers themselves. One cannot ignore the political goals that nations are trying to achieve through international cyber laws. While the West seeks protection of information networks through a multistakeholder model, countries such as Russia and China support a multilateral model which enables government control over information flow.

» Logic of asymmetry between nations is a major concern. The effects of any international convention will not have the same impact across the board. Each region will take things differently. What could be normal in one nation could be a threat in another nation.

India appears to be favouring the multilateral approach where nations should agree to the goals and are also opposed to any level of discrimination. India feels the cusp in the debate has been reached and is, therefore, promoting a more practical approach in its global engagement and working with the rest of the world as a contributor to the international approaches with maximum impact.

The discussion focussed also on whether lessons learned from other international discussions could be applied to the cyber domain. For instance, looking at the parallels between cyber security and arms control, and/or chemical and biological warfare, and/or air space and what lessens can be drawn from these areas for cyber security. Within these areas, nations have used the defining of norms notion, enhanced understanding, capabilities, acceptance, and control. These could be become ideal starting points to reach at an international agreement on cyber space governance.

In conclusion, what is required is a nuanced international debate on taking the process forward. When it comes to the role of the state in cyber space, it is crucial to include and protect the needs of the individual citizens. The debate should attempt to box out the conflicts. In conclusion, cooperation and dialogue are the only possible ways forward, given the transnational nature of the domain and inability of states deal with the challenges at a national level.

THE FIRST LINE OF DEFENCE: THE PRIVATE SECTOR

Moderator: VIVEK LALL

Panel: VIJAY MADAN, JOE SULLIVAN, GABRIEL SIBONI, KERSI TAVADIA

Given that the private sector is the principle owner of majority of the information network infrastructures around the world, and also the most vulnerable to cyber attacks, they become first respondents by default and thereby becoming the first line of defence. In this regard, the role of the private sector in securing cyber space vis-à-vis the government, within the current market models and regulatory frameworks was discussed extensively. The merits of developing and strengthening of models for PPPs in the sphere of cyber security were debated. The effectiveness of information sharing and/or mutual self-defence pacts within the private sector and with the government was also discussed. Kersi Tavadia reiterated the importance of public-private partnership by stating that "the government must provide funding while the private sector provides expertise for training the cyber security experts needed".

Specific challenges addressed:

» As many of the private sector firms function within and outside their respective national boundaries, how

Gabriel Siboni addressing the audience and the panellists.

Vijay Madan putting forward his concerns regarding the first line of defence: the private sector.

can they be protected? Threats need to be categorised by looking at what is critical at the national level, at the industry level, for SMEs and large industrial levels were identified as the foremost step.

Trust between the private sector and public institutions is an issue in delivering cyber security.

» While security tools should be developed, governments should also invest more in education as at present the skilled workforce is falling below the requirement.

» Consumers also need to have basic education in terms of the threats they face, although it need not be as complicated as deciphering malware.

» Additionally, governments should train law enforcement officials and judges to get a deeper understanding of the various types of cyber related cases.

The panelists highlighted some ways forward on the protection of the private sector.

The formation of widely acceptable standards to assess cyber security practices among private sector players is vital. Within India, the government should look beyond using cloud for public services. It should position itself as a data centre location.

Joe Sullivan of Facebook was able to provide some working examples. Private sector companies such as Facebook are trying to build a community of security researchers all over the world. For instance, 60 people have been trained in India specifically on cyber security and locating vulnerabilities for Facebook. This approach, according to Sullivan, "demonstrates democratisation of security".

The approach in Israel towards cyber security was presented, which consists of subdividing computer systems into four groups:

» Most sensitive – military forces, intelligence, defence systems, sometimes government offices.

» National infrastructures – these are on a higher plane and have additional protections.

» Industries – food manufacturers, businesses, where no one specific tells them how to secure their environments and it is left up to the company's security policy, which inherently makes them more vulnerable.

» Civilian sectors – which can be considered the weakest points.

In Israel, instead of allowing the market forces to find a right balance towards security, the approach is to find a way to regulate a minimum level of defence mechanism which should be undertaken. For instance, companies are categorised in terms of the risks they face and the impact if a private sector system is hacked. In effect, the actual risk is analysed on the damaging effect to the public and not the company in particular. If the damage to the general public is likely to be heavy due to an attack on a particular company, then the government initiates defence/security measures dedicated to each category described above.

It was argued that it is possible to ascertain and define common measures between groups in different industries. For instance, 80 per cent of the industry could have common security measures, and the rest could have customised security and response measures depending on their categorisation and threats faced. One of the difficulties faced while following this approach is to determine who the central regulator is as companies are not specifically mandated to secure information by using a particular model. This vulnerability is one of the weakest links for cyber attackers to exploit. Therefore, there is a need to improve the private sector security mechanism that will reduce the vulnerabilities. Investment in cyber security capacity building in the public and private sectors is key to the reduction of vulnerabilities. Taking this model into consideration, Gabi Siboni stressed that "there is a need to have a central cyber security regulator the model for implementing cyber security regulation is similar to environmental regulation".

In the cyber security debate, policy and legal dimensions generally overshadow the human factor, and can be the most difficult to handle. Therefore, educational institutes should be set up and funded for cyber security. It was suggested that governments can undertake the funding part and private sector can contribute by sharing its knowledge and expertise. It was noted that the private sector also has the capacity to invest in training cyber security professionals.

Having requirements for sharing information and experiences within the private sector and between the government and the private sector was also suggested as a measure to ensure better cyber security. India has set up a Joint Working Group (JWG) on cyber security with a mandate to discuss both positive and negative experiences and to find solutions collectively. The approach being taken is that cyber security is a public good as a cyber attack has the potential to impact society at large and therefore, the security of cyber space cannot be the sole responsibility of the government or the private sector. In this regard, the focus should be on encouraging reporting of incidents and information sharing with respective national Computer Emergency Response Teams (CERTs). For instance, setting up a platform for regular meetings to learn about gaps and discussing industrial responses is a good starting point. However, information sharing within the industry was highlighted as a major stumbling block primarily due to the reluctance on the part of companies to share their failures. Another interesting point which emerged during the discussions was that private sector cyber security is not just about IT networks; it is also about industrial control systems, which are often outdated.

CYBER SECURITY: STRATEGIES AND RESPONSES

Moderator: ARVIND GUPTA

Panel: NEHCHAL SANDHU, MICHAEL F. GAUL, OLEG DEMIDOV

The rate at which cyber incidents are occurring is increasing exponentially and the types of threats are changing. There are now fewer Distributed Denials of Services (DDoS) attacks and an increasing number of malware based attacks instead. The higher speed and impact of such malware attacks are becoming a concern for governments across the board. Cyber crimes are also on the rise with an increase in 16 per cent of offenses in 2013. "Unless we can create a secure cyber space, there will certainly be a disruption of services in the very near future", said Nehchal Sandhu.

Against this backdrop, the best practices in the mitigation of high-profile risks including the protection of Critical Information Infrastructure (CII) were discussed. The North Atlantic Treaty Organisation, Russian and Indian approaches were discussed at length.

NATO's cyber defence policy is based on the following principles related to cyber security: protection of NATO's network of 28 allies; and protection of NATO's partners, including their strong partner network of 69 countries throughout the world. NATO cyber security strategies are organised under three categories: national strategies, training and infrastructure development. Programmes are designed to leverage expertise and have a multiplier effect.

The main objective of the NATO cyber security strategy is to improve the ability of NATO and partners to protect their infrastructures from attacks, by sharing best practices, improving cyber defences, and creating multi-agency centre audit teams to improve cyber security infrastructure.

While NATO is not a standards or norm setting organisation, it was pointed out that it could play a significant role in enabling its own members and partners to reach common goals with respect to establishing cyber standards for protection of networks and infrastructures from attacks.

While Russia still has not officially outlined a cyber security strategy, there are a number of documents that cover the international level aspects of cyber security. Moreover, "post-Snowden, the value of US-Russia cyber security cooperation has diminished", claims Helg Demidov.

Recently, in early August this year, a document was adopted which is called 'Principle of Russia's National Policy in the Field of International

Deputy NSA Nehchal Sandhu, Michael F. Gaul, Arvind Gupta and Oleg Demidov during the panel discussion on Cyber Securtiy: Strategies and Responses.

Information Security to 2020', which is primarily dedicated to global and international aspects of information security across four levels.

At the international level, Russia is seeking to promote global mechanisms to counter cyber threats through a legally binding document prepared under the aegis of the United Nations. At the regional level, Russia is addressing cyber security issues through the organisations it is a member of. At the national level Moscow seeks to prevent cyber wars and other large scale cyber events. It pays less attention to the private sector in implementing these tasks and goals. In January 2013, Russian Prime Minister Vladimir Putin signed an order for protecting government networks by Federal Security Services. At the same time, Russia is also setting up a national cyber command under the control of its armed forces.

On the other hand, over a period of time, India has developed a strategy for cyber security, with the caveat that within this strategy, it would ensure free flow and unhindered access to information for private citizens. The strategy must maintain a balance between what is in the Constitution in terms of democratic rights and the need to maintain the government systems' security and stability.

Another important aspect of the strategy is the inclusion of the private sector. India is hoping to achieve security of the global ecosystem that has flexibility in approach and accommodate mutations in cyber space, from time to time, as they naturally occur. The end goal is providing confidence to all stakeholders about safety, security and resilience of the cyber space in which they are dwelling.

The envisaged national security framework of India will consist of incorporating standards and best practices and, very importantly, India will have the capacity to certify products via multi-agency teams that will establish security related hardware and software research. In addition, the Indian government is discussing setting up of centres of excellence specifically in cyber security.

Within the framework, the technical and operational cooperation and specific roles will be properly defined. The framework will have a layered approach consisting of the following: capacity for 24/7 threat detection, enabling mitigation via a contact point for cyber attacks, platform for information sharing system at sectoral levels incorporating best practices

for cyber hygiene, all agency communication mechanisms, CERT teams and large numbers of sectoral CERTs that will operate on a 24/7 basis.

While India has published its cyber security policy, it is still necessary to put in place a national security strategy. Furthermore, India needs to address the drastic gap in the required and available cyber security professionals. It is estimated that India will need 500,000 cyber security professionals in the next few years.

At the international level, India supports prescribing security standards and evaluation methodologies. In fact, it argues that without international cooperation, it is hard to see how cyber security can be achieved.

Within India, a national cyber security policy has been published and a strategy and architecture is being formulated. Nehchal Sandhu says: ”For now we only have a cyber security policy in place, not strategy; that is still being formulated”. More work, therefore, is needed to craft its approach at the international level. With regard to partnering with other nations, the Indian view is that anything will be done to help citizens safely access the internet without worry of losing their data and information.

IMPLEMENTING NATIONAL CYBER SECURITY POLICIES

Moderator: VIRAT BHATIA

Panel: RAM NARAIN, PETER GRABOSKY, JAAK AAVIKSOO

In any democratic society, the protection of the citizen's privacy and cross-sector participation in policy making is a must while implementing cyber security policies. The private sector and civil society are important stakeholders whose participation is essential while creating and implementing such policies. Jaak Aaviksoo reiterated that "government policies and practices must be transparent...a robust NGO sector is necessary to pressurise the government to do this". Informing the public about such policies and actions and seeking their participation, when possible, should be done by governments. Any cyber security policy should be created and implemented with as much transparency as possible.

The bureaucracy which deals with cyber-related polices and its implementation should be clearly defined. Peter Grabosky noted that traditionally, "defence and intelligence organisations are averse transparency and scrutiny...there should be clear roles, powers and oversight". Various ministries, intelligence agencies and other relevant departments dealing with the issue

Estonian Minister Jaak Aaviksoo, Virat Bhatia and Ram Narain in discussion.

should have defined roles and responsibilities. A nodal point or a national coordinator is essential in the implementation of national cyber security policies. The focal point could also be a body that deals with the multiple cyber threats challenging the country. Clear communication and effective channels of communication should be established for providing timely resolutions.

The government needs to identify the sectors that it seeks to protect through such a policy. Apart from protecting government, industry and public communication networks from hacking attempts, the focus should also be on protecting critical sectors such as telecommunications, railways, airways, financial systems among others.

On the legislative side, the panelists felt that an effective regime is required to deter criminals from abusing the digital domain. To this extent, conducting a review of existing laws, creating new ones (if required) were identified as essential steps. However, while doing so accountability, checks and balances and an authorisation and oversight body should also be put in place to prevent misuse. Laws should define clearly the powers and limitations of any such institution or body which is designated to carry out such tasks. Creating laws in haste, as a knee-jerk reaction to incidents, should be avoided as it could sometimes lead to breach of constitutional guarantees such as freedom of expression.

While hiring and training cyber professionals, countries should focus on creating cyber builders' rather than 'cyber soldiers'. Building resilient systems and networks should be the priority. However, the focus on creating resilience should not be limited to national security and defence-related networks, but instead should be built around the society as a whole.

In India's case the gap in the number of cyber professionals required is unlikely to be covered up in the near term. While policies are implemented to deliver such a workforce in the medium-term, training courses and capacity building programmes for existing workforce should commence immediately.

Education was also identified as a critical component in strengthening a country's cyber infrastructure. While educating those who are directly dealing with the technology is essential, mass public education programmes are needed to raise the general cyber-awareness levels. Such mass programmes that focus on creating a culture of cyber hygiene can be undertaken by the government in collaboration with the private sector.

Given the transnational nature of cyber threats, international cooperation is an imperative for any national cyber security architecture to succeed. While political differences continue to prevail, discussions should be initiated with international partners and others to protect the digital sphere. Sharing of experiences in implementing national cyber security policies can also prove to be highly useful.

INTERNATIONAL PUBLIC PRIVATE PARTNERSHIP IN CYBER GOVERNANCE

Moderator: GABRIEL SIBONI
Panel: JOHN MALLERY, ERIC LOEB, PRAKASH NAGPAL, JENNIFER McARDLE

In terms of conflicts between states, the old architectures are increasingly not working. At the same time there is an increasing strategic competition between states. Therefore, a comprehensive cyber defence framework is required which identifies actors, motivations, capabilities, risks and create deterrent architectures and alliances. However, it should be understood that problems that are political in nature cannot be solved in the cyber domain through treaties and arrangements.

Cyber is by far the most complex policy issue as it cuts through various sectors and layers. These include socio-cultural, political, security and economic sectors. A person with malicious intent can enter into any of these sectors using cyber space. Today international security systems are destabilising as the conventional methods relied upon are within the physical proximity of target or the enemy. “In current warfare, there is a large reach, scalability and precision effects, exposing vast attack territories”, says John Mallery. Therefore, it is not the question of ‘if’ cooperation at both national and international level is feasible – it is essential that it is.

Prakesh Nagpal addressing the audience and his co-panellists.

Moderator Gabriel Siboni putting forth a point during the session.

There are two approaches that should be followed to address these challenges – a domestic and an international approach. At the domestic level, a threat model should be created which identifies the numerous threats, motivations and capabilities of the perpetrator. It should be followed by a security and resilience architecture which addresses and defends important societal systems including critical infrastructures.
A strategy should be designed to implement these plans and a monitoring and feedback mechanism should be created to ensure efficiency.

Practical areas of cooperation should always be identified on the grounds of alignment of interest. This would give way to build confidence and create a track record which would in turn provide the necessary platform for cooperation in trickier areas. Prevention of internet fraud was identified as one of the areas where international cooperation between governments and other stakeholders is possible given the minimal political underpinnings. It was suggested that an international cyber crime centre can be created that would be complementary to existing mechanisms such as Interpol, but would focus on solving crimes and achieving successful prosecutions. John Mallery also pointed out that "a comprehensive cyber defence framework includes threat model, strategy, identification and 'incentivisation' of actors".

At the private sector level, companies can help in mitigating risk by hosting each other's content in the face of a DDoS attack, in order to improve resilience. Companies can also share real-time analysis on cyber threat information. However currently, in many countries, there are disincentives on sharing which impedes optimisation of response. Jennifer McArdle pointed out that: "NGOs and industry have a role to play in building trust on cyber matters, especially if the government isn't able to do so NGOs can build trust in track II diplomacy (such as AAAS in North Korea)".

At the international level, a framework should be established that nations and enterprises agree upon. The best place to start with could be the partnership between the governments and industry organisations. With industries having a global

footprint it is likely that best practices adopted by one branch in one country are going to automatically proliferate into the other branches in other countries.

Given the multiple levels, states can resort to cross domain attacks in response to cyber attacks and enable cross sector deterrence, which is a threat of an adverse response or outcome associated with a potential action. However, it is important that the cross sector responses are based on credible threats. Scales of hostility and altruism should be developed which will enable states to make better proportionality judgements. Threats should be separated so that responses can be different on the basis of severity of the threat. This would also enable easy and timely delivery of response.

There exists a crossover threat between cyber, nuclear and space domains. Establishing best practices for nuclear weapons states and peacetime norms in the cyber domain are essential. Nuclear systems must be isolated and encrypted to reduce likelihood of destabilising cyber attacks. Making offensive techniques obsolete was identified as a possible measure. Given that self restraint could be asymmetric in nature, states can work towards making offensive techniques redundant.

Common education and training programmes were also identified as an area of cooperation. Sharing experience in spreading awareness and capacity building of masses is another area where likeminded nations can cooperate. International workshops and exercises with participation from all sectors (government and private) will help in understanding and managing interdependencies.

PRIVACY AND NATIONAL SECURITY

Moderator: GULSHAN RAI
Panel: M.M. OBEROI, RAJAN MATHEWS, SUNIL ABRAHAM

The number of people connected to social media in India make up 5 per cent of the country's population, lagging behind the world average of around 27 per cent. Nevertheless, the percentage is growing, due to India's young population and their increasing access to connective technology. There are 900 million mobile phone connections with at least 650 million unique subscribers, a number which is expected to grow. As it grows, and machine to machine connectivity increases, the amount of information generated increases exponentially. Gulshan Rai claims that according to a recent survey, "55% of Indians share everything or most aspects of their life on social media". The pervasiveness of technology, therefore, has given rise to questions about its relationship with information and data privacy.

There are laws and rules in place when particular, individual records are sought, even if they are not optimally implemented. Less clear are the red lines around mass surveillance, which is more likely to alarm everyday citizens. According to M.M. Oberoi, the imperative question is 'whether the

M.M. Oberoi, IPS, Delhi Police addressing the gathering.

gains of surveillance are worth the cost to a citizen's privacy?' There is a notion that collective security is more important than individual privacy, and so individuals must make some concessions.

A limited amount of surveillance yields a dramatic impact, but there is a saturation point after which the benefit is lost and surveillance becomes counterproductive – it undermines the security imperative. Sunil Abraham pointed out that "targeted surveillance, like salt in cooking, is critical... too much is bad". Targeted surveillance is therefore critical but blanket surveillance becomes counterproductive.

Concerns about invasive surveillance can be assuaged by incorporating privacy policies into the surveillance practice itself, for example by clearly defining user privileges and by having a machine mediate and audit the processes. There will be demand for this kind of 'privacy enhancing' technology, and a country as large as India should invest heavily in its development.

There is unease around 'big data' in a digital world where no data is deleted, and there are numerous elements in data collection networks. Ameliorative steps which can be taken include data limitation – not collecting data that is not directly useful; early 'anonymisation' – so that human rights are not compromised by data leaks; and decentralisation – limiting the extent of harm if one area of the operation is damaged. MM Oberoi re-iterates that "law enforcement must be sensitised... we can't compromise on the privacy of individuals... it's the individual for whom we maintain security".

Data must be monitored by operators and corporations to enhance and improve the customer experience – that is how they stay successful. Increased instances of terrorism require that the huge amounts of personal information available are accessed, integrated and analysed.

Increasingly the legal enforcement burden is being shifted to network operators. Where previously only connectivity was required, end-to-end security is now expected, with information protection included in that expectation. An added difficulty is that security measures, such as requirements to provide identity credentials to use cybercafés, or to subscribe to mobile phone and broadband connections, are being subverted. The proliferation of fake documentation and identity scams suggest that such policy prescriptions do not work across the

CERT-In Director, Gulshan Rai addressing the audience.

board and may even undercut security.

Privacy interference and surveillance measures can have a chilling effect on freedom of expression – particularly data retention policies, some of which are required by law. If citizens come to feel that they are being constantly monitored, they will begin to self-censor their activities and communication. Consumers who lose confidence in network operators and other institutions will find alternative sophisticated means of hiding information, through encryption or network configurations like TOR and VPN. The consequence of making citizens feel like criminals is that these security measures then make legitimate data analysis much more difficult for law enforcement agencies.

If anonymity online deserves all the criticism that it receives, anonymity in the offline world should perhaps also be removed – doing away with whistleblowers or anonymous newspaper informants. If instead anonymity is viewed as critical for the business of open governance and maintenance of a free media, the issue should be how anonymity can be appropriately protected when it comes to the internet.

Sunil Abraham quoted Bruce Schneier to explain the phenomenon: “Privacy is like a pre-condition for security, security is a pre-condition for liberty” - without privacy, society would be neither secure nor free.

Security agencies are often blamed for doing too much during times of peace, interfering in the private lives of citizens, and then of not doing enough when incidents occur. It was suggested that privacy concerns are used by companies to justify non-retention of information, when in fact it is simply a reluctance to invest resources. The rate of cyber ‘break-ins’ has led to the notion that we are now in a constant state of war – our networks constantly pinged and intruded upon.

MULTISTAKEHOLDERISM: AVOIDING THE PRISM PARADIGM

Moderator: BARKHA DUTT
Panel: ANJA KOVAKS, VIRAT BHATIA, JAMES CLARKE, MARTIN FLEISCHER

Barkha Dutt in converstion with Virat Bhatia, Martin Fleischer, Jim Clarke and Anja Kovaks.

There is a need for multistakeholders to work together in order to examine the 'big picture' with regard to guaranteeing citizens freedom, on the one hand and on regulating policy methods and controls to fight cyber crime and terrorism, on the other. Citizens need to have trust and confidence while acting within the cyber space.

There is a need to combine on-going legal and technological research to detect similarities and differences relevant to the design of legal rules pertaining to our digital society. The aim is to ensure that important aspects of the rule of law are indeed upheld and the risk of arbitrariness is minimised in ordinary citizens' digital lives. In many cases, the capture of data and information between citizens and public administrations, governments, banks and others, is potentially done without taking into account the privacy of citizens. As a result, the disquiet and discomfort

of the citizens in their digital lives is significantly on the rise and could lead to a potential disaster if not addressed.

The lack of clear definitions, the complexity of the ICT challenges and the lack of national and international coordination, means that there is no solid response or common approach to data collection to fight cyber crime and terrorism. In addition to the detrimental impact on citizens, this fragmentation extends to industry, academia and government.

It is, therefore, necessary to rebuild the trust and confidence of the citizens by enabling the understanding of this grey area of political and legal exceptions for data and information retention. The user must be included in the processes and procedures, in order for them to maintain high levels of trust and confidence in the ICT systems they are using.

There is an urgent need for the political and legal communities to come together to examine, define and make 'exceptions' for gathering of a person's data in a more transparent and understandable manner. Therefore, as Virat Bhatia suggested, "at the domestic level, we need a serious culture and belief in the multi-stakeholder dialogue process".

There were specific challenges that were highlighted during the session:

» As a consequence of the recent and repetitive revelations about rampant data collection, there is a disenfranchisement amongst citizens using ICT including significant confusion, distrust, and lack of confidence and if left to continue, the situation could escalate into a 'digital disaster', or even a 'digital doomsday' as expressed at the recent Digital Enlightenment Forum (DEF) 2013 in Brussels last month [http://www.digitalenlightenment.org/].

» Therefore, there is a need for networking collaboration between trans-domain international communities in order to enable the examination of the 'big picture' and collect personal data in a manner that restores trust and confidence of the digital citizens.

» Lawmakers need to pay more attention to the capability of ICT technology when regulating police methods in the digital realm and developing corresponding control criteria. Currently, there exist no individual groups, initiatives, or bodies, looking at this important area collectively.

» Typically citizens, lawmakers and technologists do not come together. This is mainly because these groups don't tend to collaborate together as they operate in a silo mode in their own structures and mechanisms. In addition, they have different focus areas and perspectives on subject matters and are involved in non-overlapping communities.

Currently there are efforts being made in this field. The following are some of the initiatives being taken internationally:

» There are numerous EU and India-based fora that are regularly highlighting this important topic.

» The EU-based initiatives include an International Advisory Group (IAG) and Working Groups (WGs) and events from the European Commission's FP7 Building International Cooperation for Trustworthy ICT (BIC) project [http://www.bic-trust.eu/events/].

» As mentioned above, this topic of multistakeholderism has been raised and discussed at the annual Digital Enlightenment Forum held last month in Brussels and there is an annual event held in the EU called the Cyber Security and Privacy Forum [http://www.cspforum.eu/index.php]. The Trust in the Digital Life initiative [http://www.trustindigitallife.eu/] has also raised this topic within their working groups. In addition, there is an Annual Privacy Forum held in Europe in which this topic has also been raised [http://privacyforum.eu/].

» Also in Europe, under the EU Cyber Security Directive, a Network Information Security Public Private Platform, or NIS Platform [https://ec.europa.eu/digital-agenda/en/news/nis-platform-kick-meeting-working-groups], has recently been set up and this topic has been raised a number of times already within their working group 3 on Secure ICT Research and Innovation. Within the WG3 of NIS Platform, there is a cluster entitled People and Citizen-Centric ICT, which is already highlighting and addressing this topic as part of the EU Cyber Security strategy.

» On a more micro level, there are a number of WGs that are addressing this topic already including BIC WG1, Human Oriented approaches for Trust and Security, and

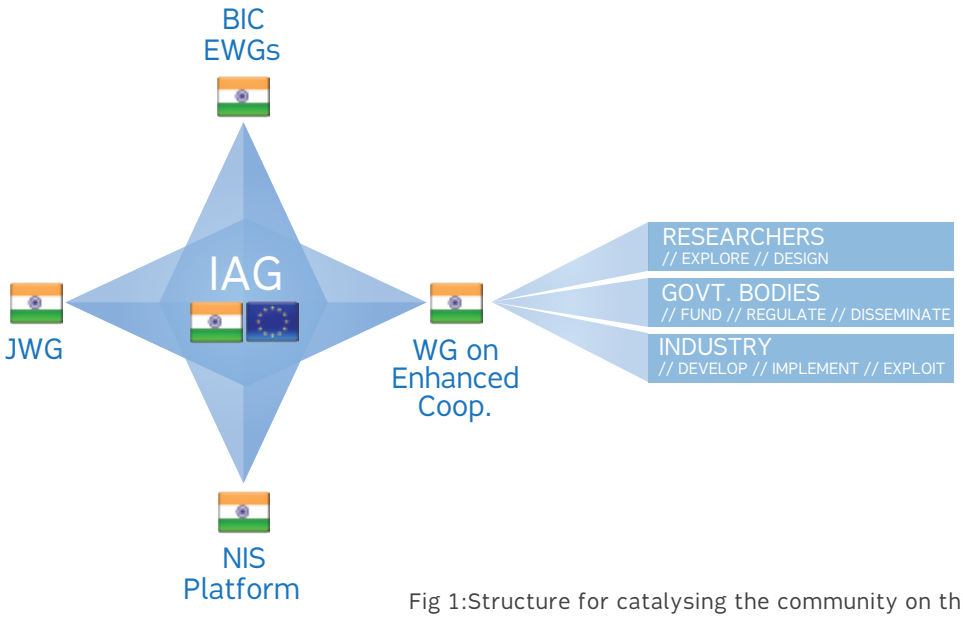

Fig 1:Structure for catalysing the community on this topic.

this has been highlighted as major issue in the India Extended Working Group [http://www.bic-trust.eu/2013/07/18/report-of-the-bic-india-external-working-group-launch-published/], which is a working group established with researchers in India looking at areas for cooperation with the EU and other countries (the Horizon 2020 research programme).

» In India, there is a working group looking at the issues raised in the Tunis 2005-WSIS entitled Working Group on Enhanced Cooperation. This WG recently held a meeting to discuss the bringing together of public and private and research communities to work through these important topics.

The way forward entails the proposal of an overall scheme of multi-governance, in effect opening internet governance, if we do not want, ultimately, a balkanization of the internet. At the moment, in the current structures of the different Directorates of the European Commission and other worldwide agencies and institutions dealing with cyber forensics, cyber security, cyber crime and cyber terrorism, there continues to be a different sense of urgency and major areas of attention differ even between the policy making and the research coordination elements. Therefore, it is essential to promote trans-domain networking and collaboration in this field bringing together the communities that wouldn't otherwise come together due to the way the research structures are currently in place. In this respect, it is necessary to take particular care to establish close links with national centres of excellence in cyber forensics, cyber security and research institutions throughout Europe, India and beyond in order to invite members to the relevant WGs, organise results-oriented workshops, training and awareness events, and other forums.

Figure 1 suggests how we can move forward with the community engaged within bridging the gap of public private participation in policy formulation in our digital society. There needs to be an umbrella event for the bringing together of the necessary stakeholders to work on this important topic. The other micro bodies, initiatives and working groups can also continue to contribute to these discussions within their own timescales in a coordinated manner as shown here in Figure 1. For such a complex issue, there will also be the need for liaising with other international initiatives and their events dealing with this global challenge.

FREEDOM OF EXPRESSION IN THE INTERNET AGE

by MANISH TEWARI
Minister of Information and Broadcasting, Government of India

Often it has fallen to my remit at conferences of the Observer Research Foundation (ORF) to sing for my breakfast, but singing for my supper would be a first with the ORF today. Before I comment to reflect on this subject, as Mr. Joshi was mentioning, you have had an extremely fruitful day and I would like to thank and congratulate ORF for holding this conference on a subject which is extremely topical and has been agitating the minds of not only policy makers but more importantly people all around the world. Invariably at conferences like this, especially when I have my very dear friends and my constant companions present, I begin with a confession that whatever I say out here I speak for myself and it would be inappropriate for me to be really binding the Government of India (GoI) to the views which I express at any academic forum. Of course, if there are any questions later as to what aspect falls within the domain of the policy of GoI, I would be more than happy to answer that either publicly or privately. Mr. Saran and Mr. Joshi asked me to reflect on the concept and the idea of the Freedom of Expression in the Age of the Internet. Before I dwell on this

Manish Tewari, Minister of Information and Broadcasting delivering the dinner table address on Freedom of Expression in the Internet Age.

subject, let me first try and broadly map the fundamental transformation that has changed and defined the communication landscape over the past two decades. Maybe thereafter I would try and ideate on how this and other factors have shaped the whole discourse on the freedom of expression in the very interesting times that we live in. It would be non-sequitur to say that the new frontier in the cyber age is undoubtedly digital. Eric Schmidt and Jarit Cohen in their seminal treaties, The New Digital Age, made some very prescient observations which I have paraphrased as follows: The internet is perhaps the largest experiment involving anarchy in the world and it has succeeded.

Today, the internet represents the largest ungoverned space on planet earth. Never before in the history of mankind have so many people from so many places had so much power on their fingertips. Every two days, more digital content is created than from the dawn of civilization until 2003. What is evolving is a tale of two civilizations: One is physical that has evolved over the million years and one is virtual that is very much in the formative stages. The new media or the social media as we call it, rides on the back of this world wide web. In India, as we speak, there are 124 million people who use the internet. The figure is expected to grow to 370 million by 2017. Facebook tells me that they have 80 million people as their customers in India. Twitter says that they have 18 million, and I know that this entire universe is expanding exponentially every day. Now, here lies the rub. Over two decades ago English, French, Spanish, Russian, and now Mandarin and some other international languages have been the medium of diplomacy, literature, governance, social interaction, and trade. These languages now have a new companion, one that promises to shape an overwhelming architecture of human engagement in the days ahead called binary and it is the language of digital communication. Many years ago, the 10 numerals were replaced by 2 i.e. 1 and 0 in the binary model. Today, the same is happening with language where the English alphabet 'soup' when digitized is reflected by 1 and 0. Alongside the language, behaviour and norms are increasingly conditioned by this binary on-and-off, yes-and-no, are the star cruise of conduct on the internet. We are confronted by a new dual reality; one in which the entire digital world is a binary governed by 1 and 0 and the interface and regulation is still humour or analogue as humans except for some of us, still do not live in the binary. Therefore, this is the real debate in the digital world. Privacy is either on or it is off. In the real world, it is much more nuanced. In the digital world, freedom of expression is either on or off. In the real world, again it is far more subtle if not complex. The reality is that we are struggling with shaping the analogue interface to the digital world. It is ironic because it is the classical case of the tail wagging the dog for the lack of a better expression.

This conference is being held to ideate solutions and how fundamentally an analog civilization will come up with responses to an emerging digital

civilization that is just beginning to appear over the horizon. What we are experiencing is technology rapidly outpacing our cognitive abilities limited by vocabulary. What we confront is a digitally reactive society either unwilling or unable to evolve responses to a rapidly changing milieu. While these challenges do stare us in the face, I don't think that there is any room for digital chauvinism for the simple reason that one person's freedom can very rapidly translate into another person's fright and then the question emerges as to who intervenes, who decides what is freedom and what is fright. For all the absolute privacy and the absolute freedom of speech advocates here and around the world, I would say what solutions are you offering for those most likely to get hurt by your absolutism? Are you in fact offering solutions or stating your rights? Who intervenes and more importantly who protects, I think is an equally important question, or are we going to become the wild west cowboy country or continue to be an ethos or a civilization which is still governed by certain rules and by certain norms. We hear both sides of the debate every day. What we are looking for is the medium, the balance that will lead to solutions. Should we allow "trespassers will be shot" type of rules for encroaching on personal cyber space? What are the personal boundaries? Is it feasible to allow real world norms to flow to the virtual world without real world laws also following suit in their wake? Of course, all of this will have to be in the context that the internet is a challenge and an opportunity without a passport and hence laws and norms will be need to be re-imagined if they are to be effective; yet, it does not mean that we see the task of governance to the unknown and the variables without a constant and in a sense allow Darwinism to define cyber reality or for that matter hijack democratic processes.

What right now seems to be perhaps the law of the jungle running under Darwinian principles, it has to be made accountable and responsive to the greater common good. Then the quintessential question would emerge and it would of course be raised as to who defines common good and to that I would like to respond in all humility that democratically elected governments still represent the legitimate will of the people even today. Conversely, if we look at the other side of the argument, we must also accept that anarchy to a degree must be the salient feature of the internet domain and in that sense it gives voice to millions and reach to those without access. We must also allow a million mutinies to flower on the net as they unleash creativity which refines the human experiment on a daily basis. The reality also is that without there being a jungle somewhere, evolution and the survival of the fittest invariably comes to a grinding halt, but here lies the paradox again. On one hand, the cyber world enables grassroots democratisation like nothing before, but on the other we have seen the same medium also having the potential for enormous destruction inflicted through the same rights that enable emancipation and invariably and unfortunately the victims more often than not are the newly emancipated. No government must seek to

restrict this feature and those who try to do so, do it at their own peril. We have seen this happening with the Great Wall of China where in spite of a ban on Facebook and Twitter, the Chinese social media, the Weibo, if I have pronounced the world correctly, has grown just as big and loud with the government hard pressed to control it. Given how big and how quickly the Weibo has proliferated, a turn back to a no-social-media paradigm is something which even the most hard line Chinese communist party possibly also would not be able to implement.

We in India have been grappling with this question. As most of you know, freedom of expression is guaranteed by our Constitution; however, it has reasonable restrictions. Therefore, in the offline world while protests are allowed, if the government feels that it could cause communal disharmony or become a law-and-order situation, it has to step in and do the policing. The conundrum is how the shades of gray would play out in the black-and-white world of binary. In the past year-and-a-half, some major incidents have reinvigorated the discourse as to how the potential problem of offensive communication over the internet needs to be or can be surmounted. During your deliberations today, somebody must have flagged the mass panic of people from the north-eastern part of India who had to flee from cities in South India in July last because of mischievous messaging that claimed that they would be targeted if they do not leave. Despite messages from the government over the same medium, we could not ebb that exodus. Ultimately, the government had to cut SMSs to only 5-a-day to stop further spread of rumours. In Jammu & Kashmir, the chief minister took a decision to block the internet for some time when news of the Innocence of Muslims video took the world by a storm. He did not want to risk any flare ups in his state of the kind being seen in other parts of the world. Similarly, last month in the central Indian state of Uttar Pradesh, there were riots in a city called Muzaffarnagar and there was news of a video on YouTube which inadvertently ended up fanning these flames of communal situation. In that situation, one must wonder what the government's action should be. On one hand, it is believed that a person who initially posted this video a few years back did so to raise public outrage against extra-judicial execution. A couple of years later, you see the same video being circulated to fan communal conflagration. Intent of the initial poster, those who posted it during the recent riots in North India, is easy to pinpoint. This is unusual. Most often intent becomes very difficult to prove. Given this paradigm, we must pause to consider at what point a personal tweet, essentially a digital freedom of expression, turns into a mass broadcast, a telecommunications business in effect, one that you would agree should certainly be amenable to certain standards of accountability at least.

When talking of the internet and freedom of expression, it is easy to be absolutist where you are not responsible for keeping the peace; however, everyone must remember that along with the

wonderful positive development, the internet has brought us creativity, employment, e-governance, and more connectivity. There are areas which are hidden from the public view that are negative. This is the dark net as the scholars call it and it consists of terrorist networks, cyber criminals, and other insidious networks that aim to twist the internet to their advantage - what I often refer to as the spectre of the hidden people. There is no choice for governments but to be alert. The entire point of this conference as was explained to me, the CyFy, is to discuss some mechanisms to ensure that the internet stays positive, freedom of cyber navigation is stored, and the internet remains free and safe just like any of our other global commons. But there is more to democracy. It is the responsibility of the government to keep you safe even when you are fast asleep. What should the government do when it knows certain people are using the internet to fan violence? This is where concepts of surveillance, monitoring, and cyber experts come in. This is the real world we unfortunately live in; so should not the government have both, a legal and technological way to stop such activity.

We see cases in the real world where indisputable rights require courts to intervene to enforce them. We have seen this debate over Park51 Islamic Center in Manhattan, also in Europe where legal mechanisms finally enabled the building of a mosque that was opposed by local residents. If this is the case of rights in the real world, I fail to see why the outrage or what is an effect of the baby steps of norms evolving in the virtual civilization. Being a democracy, it is imperative that business in civil society come to become a part of this process to come to the table to take a multistakeholder approach to talk about how best to keep the freedom of expression alive in the Internet Age, and this sometimes means deciding what our safeguards are, where the digital redlines are and the nuances of the new language of our times, the binary. In any democracy, the sine qua non is the freedom of the people, but the social contract also entails that the freedom is based on guarantees and security to these same citizens. One is not exclusive of the other; rather I would argue they are deeply symbiotic. We need to seriously introspect as to what would happen if agreed rules of international engagement do not emerge as a binding international compact that encompasses states and other entities that control the underlying hardware of the net. Would this lead to the vulcanisation of the internet? A related question which also needs to be considered is, is access to the internet considered a right or is it a privilege or is it a market good that is if you cannot afford it then you should remain offline? Should internet openness be at all filtered, monitored, obstructed or manipulated as some people refer to it. What restrictions may exist in response to the potential legal economic and security challenges raised by the new media? Finally, the question which possibly really keeps policy makers awake at night is that at what point in time does a cyber attack qualify as an act of war in the physical space? This transformed

communication paradigm has its implications on the social milieu and social norms. In fact, the time is just right to also introspect about the distinction between the right to privacy and the right to anonymity. For instance, one should not feel free to launch hate campaigns in the name of right to anonymity and infringe upon someone's privacy. Therefore, all stakeholders should deliberate the need to strike a right balance or in other words find the equilibrium between the right to privacy and if at all there is a right to anonymity. Five billion people are expected to join the net in the next decade; it could happen sooner. Thus, the internet will spread to some of the most remote and at the same time some of the most unstable parts of the world. There will be an increased information access to healthcare, education, and just as much as more connected word, but we must be aware that there is a lack of a delete button on the internet. As we become more and more active online, the digital imprint that we create will only increase. This is especially true for young people growing up now for many of whom use online platforms as a natural extension of their physical lives. By the time a person is in his/her 40s, he/she would have accumulated and stored a comprehensive online narrative, all facts and fiction, every step and every time spanning every phase of his/her life; even rumours will live forever on the internet.

Let me conclude by quoting President Franklin Roosevelt who said "the only sure bulwark of continuing liberty is a government strong enough to protect the interest of the people and a people strong enough and well enough informed to maintain its sovereign control over the government". This is the balance we all seek. This is I think the task of this conference and many other conferences which would be held in the future to find this golden mean and I can assure you that policy makers around the world would be listening and taking on board very seriously the solutions that you have to propose. Once again, I would like to thank ORF for inviting me here and all of you for having had to bear with this harangue at dinnertime. Thank you very much.

NATIONAL STRATEGIES FOR CYBER CHALLENGES

by JAAK AAVIKSOO
Minister of Education and Research, Republic of Estonia

Dear friends, excellencies, ladies and gentlemen, let me start with a small reflection on internet. I believe internet is a young lady who has barely turned 30. She was born out of national ambition, academic curiosity, laid and educated by millions of private admirers, and today cherished by billions of us. Every third citizen on the earth is in one way or the other related to this realm. She got into the realm we call cyber space and she rolls in her own way. You may ask why I call the internet as she. I do so because internet is young, beautiful, dynamic, and fully surprising, and we all know she is also unpredictable. There are threats. Like in the real world, there are bad guys and there are good guys and we have to learn to live with this reality. On a more serious note, on several fora at global and national level, we have discussed cyber security, cyber defense and everything related to managing the threats that emerge from this new reality. My personal experience as I said before starting was in 2007. I was second week in the office of the minister of defense where the government took a decision to relocate the Soviet Time War Memorial and that resulted in extensive attacks on our cyber infrastructure. What it looked like? In a country where you have only few banks, actually two banks having a share of 90 percent of the market, were basically down. E-services were broken. Distributed denial of service attacks brought down online news. At the same time, we had riots on the streets and people starting asking "who in-charge is and what is going on." I think it was for the first time people realized that cyber threats can be perceived or even it can be a real national security threat. Since then we have discussed these cyber threats on several fora and we have developed defenses, we have developed strategies, we have tried to manage cyber crime and cyber espionage, cyber sabotage, cyber terrorism and pornography. We had to tackle a multitude of phenomenon and most probably gone half the way to solve it. I have to remind the normal aspect of Estonia and internet. Freedom is important. As for Estonia, we have been proud to be ranked by Freedom House the No. 1 country by Internet Freedom. Unfortunately, we were toppled last year by Iceland. We will try hard the next year to gain back the No. 1 internet status in the future. In all our countries including Estonia we have cyber security strategies, action plan, different meets to fight the threat and to address the multitude of threats from cyber space. We need to develop

and make them more detailed, more effective, and more engaging; but another important feature I think is we need to understand the logic of development of cyber space. Minister said yesterday that internet is an oxymoron and he had his arguments and I do have mine. Internet essentially is an environment and in the case of environment it is wise to not to think in the terms of eliminating or blocking the threats, but rather building resilience. Building resilience is a somewhat different attitude; resilience of the whole community of consumers or the whole society instead of building particular defenses around national, sectorial, institutional, or personal interests. We need actually the both, the resilience I believe is more important. It is like people living close to sea manage waves and floods, and those close to geological disruptions the earthquakes. They learn to live with it. So, once again, we need plans but also we need public awareness, rules of behavior, cyber hygiene, and simple common sense very many of us including myself sometimes lack when we are left alone with a computer. Building this culture which I call cyber hygiene is very-very important. We may defend our institutions and our classified networks to the utmost extreme but when anybody of our employees finds a memory stick on his doorsteps and plots it into a wrong computer, we have a problem. So, the human factor should not be underestimated rather the other way round.

I start with a few remarks on cyber. I think we sometimes tend to mistake cyber. We believe that cyber space is all virtual, obscure, not transparent, and so on, and it is true to a certain extent, but only to a certain extent. I think we should never forget simple things. First, people and only people make things happen, both bad and good. Cyber does not make things happen; people make things happen and there is always a physical effect in real physical space. It has a location, it has content and we can see and understand what has happened. So, it starts and ends in physical space. The act carried out by a bad or a good guy is real and the outcome is real, and it actually does not matter how many times the signal circles the globe before it hit the target. From this basic understanding, I think we can draw fundamental consequences in the field of cyber defence in response to cyber attack. If the effect of an attack is an extensive material damage or loss of lives, which in ordinary space can be called an act of war, it is an act of war also if it was carried out via cyber space. What is the consequence? Kinetic response is appropriate. There have been theoretical discussions. Can we imagine of a nuclear response? I would answer one should not exclude in principle. As you heard before, after the attacks in 2009, Estonia together with its NATO partners established a NATO Cooperative Cyber Defence Center of Excellent in Tallinn and one of the publicly available products of that institution is a book called The Tallinn Manual on Cyber Warfare. This reflects in the way our NATO partners and us understand how we should legislate into the area of cyber conflict and cyber war closer to every day life. When somebody is killed with a knife or shot to the gun, he or she shall be punished and there is no doubt about it. When it is done via internet, it is no difference. The same should apply. However, we see applying

Special Address by Jaak Aaviksoo, Minister of Education and Research, Republic of Estonia.

this principle, a number of practical problems, sometimes conceptual problems. If somebody robs a bank with a gun, there is a public perception of the man as of a robber. When somebody steals millions from a bank via internet, there is a possibility that he may become a hero and the victim might be the bank or even the incorporate for not building appropriate defences. We should work on the public awareness side of this problem.

What can our governments do on national level? I am only addressing a few issues, which I think are relevant on a broader respect of societal responsibility. Internet commons is a public good. We have common interests of all consumers, so we could take the attitude of consumer protection. If we really want to achieve resilience of our societies, we need to cooperate and build cooperative defences, and it is because of the network nature of the internet. Potential offence is also networked, so must be the defence and this is essential. What does that mean? I gave you three suggestions what a government might do to build resilience instead of the hierarchical differences where possible use of community and industry standards to protect your critical infrastructure, institutions, and organizations instead of creating norms and regulations that regionally protect your society. Secondly facilitate cooperation, offer expert support, organize voluntary cyber defence formations. In the example of Estonia, we have a paramilitary defence league very much like the American homeguard and we have created cyber units voluntarily which involved cyber security specialists from the private sector as well as academic sector. They work together in peaceful times and in the case of emergency be mobilized like the defence league itself. Thirdly, very many cyber attacks and events are not reported because of the damage to reputation of institutions. Banks do not do that. Major companies do not do that. Government offices do not do that. The government has the possibility to offer clearing house service together and distribute best practice without naming and shaming those who have been attacked. There is a vast experience available, but it is distributed and is not available to those who want to build defences, so I think the government might contribute to developing such structure.

Last but not least, everything we face in the form of threats is first and foremost related to trust and confidence. It is wise to bear in mind that you can only trust somebody. You cannot trust internet per se or its services; you can trust somebody you know, that means you need an identity. I fully agree with what Minister Sibal said yesterday, the issue of identity is essential for one to tackle the problem of security on internet. The identity in internet is a growing concern and we need trustees for reliable identity management. We need a third body who may trust me and my partner so that

my identity can be proven by an independent trustworthy partner. The governments, I believe, have the responsibility to make trusted identity available. The governments may offer it through the government agency as they often do, but they also may do that through trusting a private partner. For instance, a telecom company! We have done both in Estonia. I would like now to involve you in demonstration of how far we are willing ready and practically able to go in the case of Estonia involving Estonian citizens and residents. Estonia has offered electronic ID cards to all citizens and residents and on the forthcoming Sunday, Estonia holds local elections. Since 2007, the government has made possible to cast your vote via internet. Electronic ballot boxes are open since last Friday. Ladies and gentlemen, I would like to cast my vote on location elections in Estonia right here. This is the electronic identity card. I have another government trusted identity together with the Estonian Telecom and that sits in my i-phone. In principle, I can sign legally binding documents using these two devices from my computer up here on the stage including casting my vote on local elections. I hope this device will read the data and present on the monitor.

I wanted to finish with thinking a little bit why this is all together possible. First, because Estonian citizens trust their government because they are ready to have an electronic identity and there is no problem of the big brother, so we are not afraid of our governments that they follow what we are doing. Secondly, the governments must trust their people so that they don't misuse document. We don't sell our cards, pin codes, etc. The people have to trust the government that there is no election fraud in the electronic environment. The code that carries out these operations is made publicly available for public scrutiny. Everybody can read the code, try to corrupt it. We have invited hackers who could corrupt the systems so that we can prove and improve the system and make it more resilient and functional. What I want to tell you as a final conclusion is that the main task of the governments and societies is to build the appropriate culture of living in the real as well as virtual space. This is a national undertaking which governments can do that, companies can do that, military can do that, people can make that happen. It takes time and it evolves through confidence building measures, build trust, building relations and partnerships which you can trust, and by that means minimizing the risks and building the necessary resilience without excessively restricting the freedom of the wonderful internet. Thank you for your attention.

VALEDICTORY ADDRESS

by NEHCHAL SANDHU
Deputy National Security Advisor, Government of India

Dr. Raja Mohan, Samir, and colleagues in the audience, I can see that you have dealt with a number of issues in the last two days and the account that Dr. Raja Mohan has so competently rendered makes me shrink away from making any comments about anything he has dealt with. But I am happy to hear from him that this is just the beginning and that there will be a process of engagements, small and big, to continue to discuss these subjects. I must say that when Samir and Mahima first came to see me, they had intended to steer this debate in a very different direction.

It took us a lot of doing to make them understand that cyber security is quite different from a host of other things that they talk about. One of the key points that we have to understand is that if people have to preserve their privacy and conserve their information then that is only going to be possible if you have secure cyber space. If cyber space is not secured then nobody's information and identity and or anything else is going to be safe.

Deputy NSA Nehchal Sandhu addressing the audience during the valedictory address.

A couple of words about the three aspects that Dr. Raja Mohan raised. One is that in this day and age, international cooperation has become a must. If you have actually to investigate cyber security incidents and ultimately make sure that you are able to get to the root of where the threat originated, attribution is becoming a big-big problem. No single country can ever aspire to create capacities to get to the bottom of every attack. Therefore, this is an area where there will have to be international cooperation, will have to seek assistance of a large number of partners abroad and I suspect that some kind of a modus will have to be found where we can get to the bottom of these.

The second is about surveillance. We just talk about the difficulties that service providers have in terms of contending with the requirements that are posed by agencies and police, etc. I would just like to assure this house that first of all whatever is carried out is done in accordance with law. More importantly, there is a three or four step process before any approvals are granted for any such activity. Secondly, there is a very strict regime that was instituted by the Supreme Court in 1999 with reference to how you can access people's communications and it is important for agencies to confirm that they are confirming with each one of those stipulations. Thirdly, there is a review process and the review process is the hands of people who have nothing to do with the authorisations that take place. The distance between the review process and the operating levels provides for a degree of assurance that there is no activity being carried out which is not in accordance with law.

Thirdly, I was just wondering whether during his talk this morning, the Estonian minister for education and research mentioned that every Estonian citizen has an electronic ID. It is an immutable electronic ID and nobody can use any access device to get onto the internet without providing that identity. You could pretty well question this modality for those who are champions of privacy, anonymity, and so on that flies in the face of all of that because you are forcing people to say who they are, whether they are coming through a PC or through a mobile device of whatever. Of course, reassuringly he mentioned that the institution of this kind of a programme requires a lot of money and it costs them a lot even though they have a very small population, so it is not going to be applied in any case in India with billions that we have to deal with. As Samir just reminded me and this is something that the minister was threatening to do yesterday, they had elections in Estonia and while he was here in this event, he exercised his right to vote through secure channels which are available to him by using his electronic ID and he managed to get his vote logged. I think we are quite some distance away from any of that kind of activity. Samir just noted when I brought it to his attention that this is obviously a big day for India. You have the two most prominent

industry associations spending the same two days discussing cyber security at two different venues in the same town. Obviously, this called for better cooperation because you would have had better impact if you had done one now and one a month later. With the attention spans of people being brief and as short as they are, I suspect this concurrent holding of two events on the same subject was not ultimately a good idea. But I am glad this happened and I am glad that ORF and FICCI have partnered to create this and that there is intent to carry forward the process through a series of discussions.

I thought I will use this opportunity to go back to a point that Dr. Raja Mohan raised a little while back with reference to the session on private-public partnership. This might be as good a forum as any for me to state that the GoI has committed to partnership with the private sector in the realm of cyber security. The fact that we have a joint working group with significant participation by private sector players is testimony to our earnest desire to a list the support of relevant elements of the private sector. This is a recognition of two or three factors: One is that the private sector is a much larger user of the internet than the government. Secondly, there is significant private sector participation in critical infrastructure, and unless the private sector is on board, we could have big trouble. Thirdly and most importantly, the huge talent pool that we have in the private sector is something that the government can usefully leverage in advancing its efforts for making sure that we have a secure cyber ecosystem within the country.

There are some specifics that I would like to raise in this context, something that you might regard as what the private sector could do for itself. With the large amount of revenue that we generate through IT services and IT-enabled services in conjunction with foreign partners, many of our companies need to make sure that they handle traffic security and that all the data that they have is kept protected, and so on and so forth. So, I suspect that a lot of activity goes on in the private sector to make sure that there is no breach of any of that because if that happens then they would lose business. Our expectation is that as they proceed to reinforce their cyber defences, they would also be kind enough to share with us their experiences, in the sense that when they sense attacks or if they were to revert quickly, that would be a very useful process because attacks are not necessarily directed at small segments of sector and could be pretty wide ranging. Secondly, as they move to fortify themselves against further attacks, if they could keep us in the loop, then we would learn from what they have done to reinforce our own systems. Thirdly, I suspect that awareness of the need to maintain cyber security is something that is retained at midlevels within corporate hierarchies and CEOs of most of our companies do not necessarily have the kind of awareness they need to have with

reference to the essentials of cyber security. I say this with reference to the power sector for example where a lot of our systems can possibly get compromised and you could have huge failures, so I think there is a need for the private sector to invest in terms of educating the higher levels of the corporate managements about the threats of cyber security. Whenever you have your annual conventions and so on, it might be worthwhile for you to introduce this as a subject. Fourthly, I mentioned earlier that there is a huge talent pool in the private sector and that is something we want to leverage. We also know that there is a huge amount of R&D being carried out in the cyber security domain that companies tend to keep for themselves. I think the time has come now when what they regard as not so sensitive could potentially be sold in the market to other players so that other elements of the private sector can protect themselves. Through the joint working group that we have, we are looking forward to significant participation from the private sector in developing cyber security standards, and now that India has become an authorising nation under the CCRA regime a couple of weeks back, we now have the ability in the STQC at Kolkata to further authorise testing laboratories. We are going to have a similar arrangement through DTSC in Bangalore and I think there is an opportunity for the private sector to establish testing laboratories which they could submit for validation to the STQC and there will be enough clientele for you to sustain yourself.

There is a point that Dr. Raja Mohan made a little while back about the need for manpower. The national cyber security policy talks in terms of creating 500,000 cyber security professionals in the next few years. This is not going to happen even if the government was to dedicate all its efforts, and it is therefore necessary for the private sector to avail this opportunity. It is actually a business opportunity for you. Besides the National Institute of Electronics and Information Technology, NIIT, APTECH, and so on, which could actually get into the domain of training cyber security professionals, we are in the process of initiating processes for testing and certification of such cyber security professionals, so that once they emerge from these institutions they are fit enough to assume duties at the practical level. There is another window for the private sector. The principle scientific advisor to the prime minister has been given sizeable funds to promote R&D, and there is sufficient scope within that scheme for private enterprises to present the project proposals to him and to partake of the funds that government has made available to him for pursuing cogent schemes that would result in a worthwhile product or even systems or processes that would help us better protect our cyber domain.

In conclusion, I would like to compliment ORF and FICCI for having organised this event for identifying significant issues that needed to be addressed and for marshalling the support of wide sections for dealing with pertinent issues in a detailed manner. Thank you all.

CYFY

THE INDIA CONFERENCE ON CYBER SECURITY AND CYBER GOVERNANCE

ANNOUNCING CYFY 2014

OCTOBER 15-17, THE OBEROI HOTEL, NEW DELHI

TOPICS INCLUDE:

- CYBER LAWFARE
- LIVING WITH CYBER INSECURITY: CYBER SECURITY VS CYBER RESILIENCE
- PREPARING FOR CYBER ARMAGEDDON: IS CONFLICT INEVITABLE?
- THE ROLE OF EMERGING POWERS IN CYBER GOVERNANCE
- RETHINKING THE GLOBAL CYBER MARKET
- PRIVACY IS DEAD?
- DECONSTRUCTING MULTISTAKEHOLDERISM
- IS INDIA A SWING STATE: BRIDGING THE DIGITAL BINARIES

Please contact us to stay updated and/or to find out about sponsorship packages.
mahimakaul@orfonline.org or cyfy@orfonline.org

NOTES

NOTES

NOTES

FOR MORE INFORMATION, PLEASE CONTACT:

Observer Research Foundation
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