Conference on "India's Cyberspace"

"Building a secure and resilient cyberspace"

26 June 2014

Inspire Hall, Hotel Le Meridien, New Delhi

AGENDA

10:00 am – 11:30 am

INAUGURAL SESSION

Welcome Address : Dr. Suraj Kumar, Chief Mentor, Neeti Foundation

Theme Address : Dr Vivek Lall, President & CEO, New Venture, Reliance Industries Limited

Industry Address : Arvind Chandrasekar, Director, Government Affairs, AMD India

Chief Guest:
Shri Ram Narain Singh
Member (Technical)
Cyber Appelate Tribunal

Vote of Thanks by : Satya N Gupta, Senior Visiting Fellow, Neeti Foundation

11:45 am – 1:00 pm

TECHNICAL SESSION ON "IDENTIFYING THE ROADBLOCKS IN THE SECURITY OF INDIA'S CYBERSPACE"

Moderated by : Cherian Samuel, Associate Felow, Institute for Defence Studies and Analyses

Theme Address : Ram Narain, DDG (Security), Department of Telecommunications

Speakers:

- Sanjay Bahl, Senior Consultant, Cert-In
- Dr. S M Bhaskar, Director, National Technical Research Organisation (NTRO)
- Vikram Tiwathia, Associate Director General, Cellular Operators Association of India
- Deepak Maheshwari, Head – Government Affairs, Symantec Corporation
- Ashim Sanyal, Chief Operating Officer, Consumer VOICE

1:45 pm – 3:00 pm

TECHNICAL SESSION ON "ADDRESSING THE ROADBLOCKS WITH INDUSTRIES PARTICIPATION"

Moderated by : Satya N Gupta, Senior Visiting Fellow, Neeti Foundation

Speakers:

- Suresh Kumar Gupta , Principal Advisor, Telecom Regulatory Authority of India
- R R Mittar, DDG, Telecommunication Engineering Centre
- Dr Prem Chand Executive Director, Codenomincon Software (I) Pvt. Ltd.
- Anita Mittal, Principal Consultant, National Institute for Smart Government
- Dr. Debabrata Nayak, Chief Security Officer, Huawei Telecom
- Mohit Rampal, Regional Manager, India and South Asia, CISSP, Codenomicon Software (I) Pvt. Ltd.

3:00 pm – 3: 15 pm

Summing up & Vote of Thanks : Dr. Suraj Kumar, Chief Mentor, Neeti Foundation

OBJECTIVE OF THE CONFERENCE

At the completion of one year of release of National Cyber Security Policy, Neeti Foundation along with Indian Computer Emergency Response Team (CERT-In), Department of Electronics & Information Technology organised the conference on "India's cyberspace" on 26 June, 2014 New Delhi.

The purpose of the conference was to identify the policy and technical issues faced by the stakeholders, especially the Government ,in building an eco-system for cyber security in the country. Post the identification of issues, the solutions with the participation of the industry were also brought to light at the conference.

The conference had representation from key stakeholders:

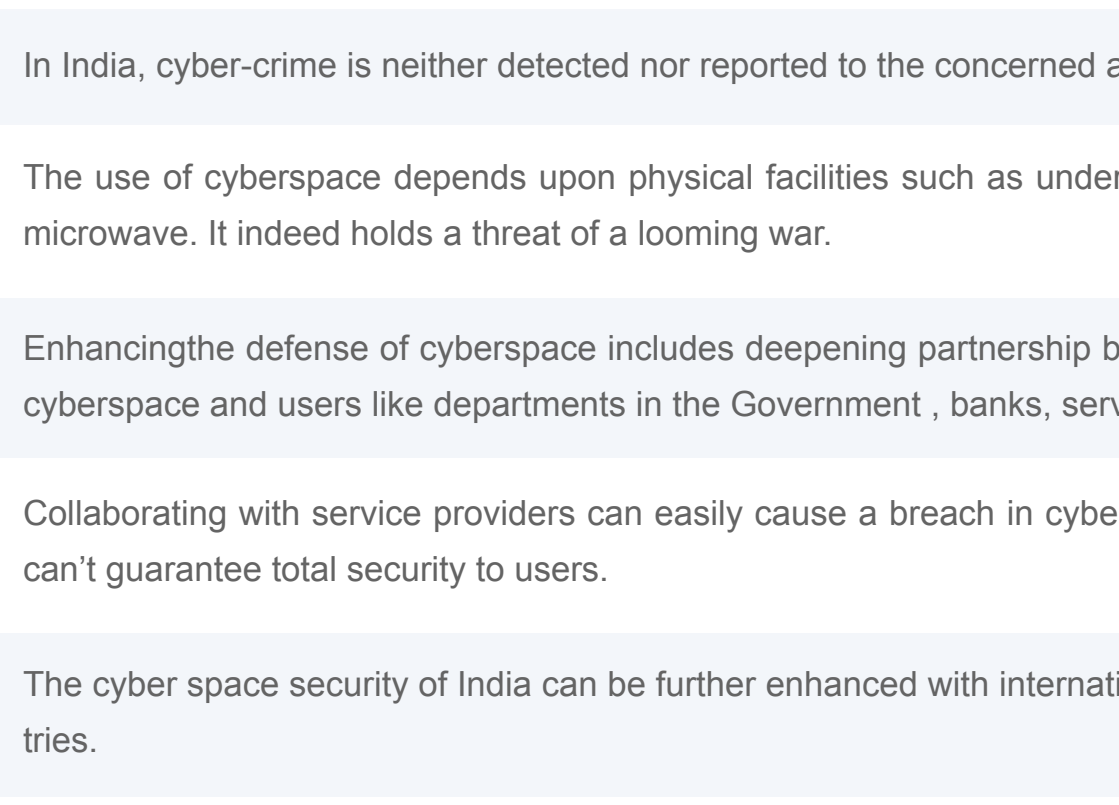
Department of Telecommunications	Institute for Defence Studies and Analyses
Cyber Appellate Tribunal	National Institute for Smart Government
Telecom Regulatory Authority of India	Telecommunication Engineering Centre
Cert-In	Consumer VOICE
National Technical Research Organisation (NTRO)	Reliance Industries Limited
Cellular Operators Association of India	AMD
Codenomicon Software	Symantec Corporation
Huawei	

The conference saw participation from representatives across the stakeholders like Department of Electronics & IT, Department of Telecommunications, Telecom Regulatory Authority of India, Telecommunication Engineering Centre, Cert-In, Aircel, Survey of India, Ebay, Embassy of Sweden, GIZ, IIT Delhi, Innovate Infosec, JNU, NDMA, Net4 India, NICSI, Tech Mahindra, Verizon, Yahoo, UTL India, Consumer VOICE, Vodafone, BSNL, AICTE etc to name a few.

PARTNERS

EXECUTION PARTNER

CONFERENCE PROCEEDINGS



Inaugural Session

Objective: To give a brief scenario of the present cyber security ecosystem in India.

Dr. Suraj Kumar, Chief Mentor, Neeti Foundation welcomed the guests and commenced the conference. In his opening remark he mentioned that with respect to National Cyber Security Policy-2013, the point of departure of our consultation today pertains to an awareness generation, national cooperation and prioritization of national level programs for cyber security in India.

The key points mentioned by the distinguished speakers during the sessions

The development of internet and low cost wireless communication has led to phenomenal increase in its use in the socio- economic and political space. Cyber-security embraces the public and private sector and a broad range of issues including trade, commerce, national security and industrial espionage.

India has to contain known and unknown adversaries in the issues of cyber-attacks. India lacks in the combative measure in field of cyberspace.

In India, cyber-crime is neither detected nor reported to the concerned authority in a timely manner.

The use of cyberspace depends upon physical facilities such as undersea cables, telephone exchanges, routers, optical fibers, and microwave. It indeed holds a threat of a looming war.

Enhancingthe defense of cyberspace includes deepening partnership between public organisation charged for securing partnership of cyberspace and users like departments in the Government , banks, service areas as well as individuals.

Collaborating with service providers can easily cause a breach in cyberspace. Even the best uses of firewall, anti-virus, log in control can't guarantee total security to users.

The cyber space security of India can be further enhanced with international cooperation, protocols and agreement accepted by countries.

Debate on cyber-security has thrown up issues of privacy, security and sovereignty etc. and each area requires close scrutiny. Till now, not much significant progress has been made in this direction by the authorities.

A country which houses a global gateway on internet service provider, can invoke its sovereignty to secure its access to the hub on the ground of national security.

IT revolution has provided a platform to criminals and terrorists to make anonymous attack on the targets. A cyber-criminal staying in any part of the world can inflict a cyber-attack on any other country. Thus, international legal issues on cybercrimes are complicated and it has become very difficult to punish the offenders as authorship of the crime is very difficult to establish in such circumstances. At present we lack with established law to punish any such crime.

International cooperation with enhanced trust on the partners is required to control cyber-crimes. Anexample of an international cooperation is "Russian government distrust for the 'Budapest Cconvention'. Russia's suspicion arose from the clause, which authorized an external agency to investigate Russian citizen on Russian soil without Russia's permission. They had no objection with joint action against national syndicate."

The National cyber security policy envisages around 5 lakh information security professionals, whereas, in reality there is only less than 500 such people presently working in the government . Department of Information and Technology has prepared B.Tech and M.Tech curriculum on cyber-security. The Government needs to implement it immediately with effective tools and techniques to improve the number of information security professional.

Presently the level of cyber-security risk is very high in India. Also the number of websites being defaced in India is very high. With the increasing number of mobile devices with internet facility in India, the level of cyber-security risk will increase. India is only reacting to the situationrather than preparing a framework that will proactively check cyber threat for the computer/mobile phone users.

India should largely address cyber security issues at a physical level. Loss of data and identity theft is a bigger problem, which looms large ahead of the country. It will get more complicated once India fully becomes a part ofthe IP rule/ regime.

India has a huge number of accounts on social media platforms of Facebook, Twitter, emails etc. This accounts for a huge share of complexities as all these are exposed to an element of risk. Today, lot of organizations have has moved to cloud computing, because, it has brought about the ease of doing business. On the other hand however there is the increased risk and vulnerability to its data.

No of connected devices per person in India in 2010 was 0.7, but come 2020, India will move 6.5 per person. This can be attributed to the burst of dual SIM phones, tablets and smart phones. Today, several organisations are moving to the use of their own devices, which puts individual data on serious threat.

To counter the date theft several military organisations have curtailed the use of a smart phone but that may be not the long term solution.

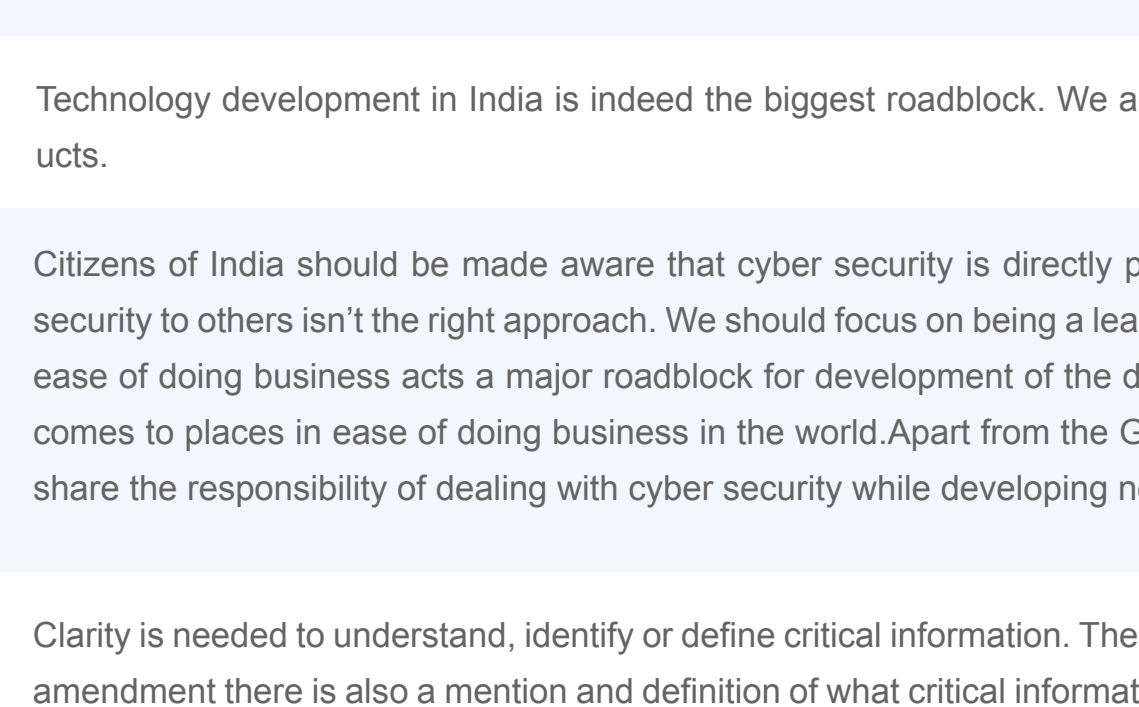
A lot of data is saved on official computersof various governmentgovernment departments which is vulnerable to data theft across the world. For example: Recently, flame targeting of PCs in the Gulf region has cost several countries huge losses, as energy data was lost. The only country which came out with data was Bahrain, and the loss was estimated to $130 Billion in next 15 years.

India should also start considering application level attack, which is quite possible now thanks to the 4 MBPS of speed that is easily available to users. With the impending integration of 4G and 5G we will become even more vulnerable to phoenix attacks.

Cyber security has also been given much importance in The Companies Act of 2013. It is of primary importance while running businesses in India. The need of the hour is thereforeample coordination between the gGovernment and corporate sector in the cyber space.Together,they should share the responsibility for training cyber experts and sharing the information on real time basis.

A lot of importance has been put on a layered approach to cyber security.It can be elaborated with an Open Systems Interconnection (OSI) model {The OSI model provides a conceptual understanding of LAN/WAN internetworking}, where we have two important layers for cyber security. One is a physical layer; another layer is an application layer. In our enthusiasm most of us focus on the application layer, as it is more focusedand innovative. Today, the need of hour is devisingcyber security method that is fail-safe for the physical layer.

IDENTIFYING THE ROADBLOCKS IN THE SECURITY OF INDIA'S CYBERSPACE



Objective: To bring the representatives from stakeholders like government, think-tank, consumer group and industry on a common platform to identify the key roadblocks faced in building a secure and resilient cyberspace.

Opening the session Mr. Cherian Samuel, Associate Fellow, Institute for Defence Studies and Analyses (IDSA), said identifying the roadblocks in security of cyberspace in India; is not in the hands of one organization but in the hands of many people.

The key pointers mentioned by the various distinguished speakers in the sessions were as follows:

Cyber security demands much higher depth of understanding technology than using it. Today, India has evolved as consumer of technology rather than developer of the technology.The cyber security threat can't be dealt with without us being the manufacturers of technology.

Wherever technology impinges on the commercial considerations, the other countries are happier to part with technology as we consume and pay for it. But technologies, which are related to cyber security, are not being shared. We need to develop indigenous technology for cyber security.

Technology development in India is indeed the biggest roadblock. We acquire technology rather than developing our indigenous products.

Citizens of India should be made aware that cyber security is directly proportional to national security. Thus outsourcing our national security to others isn't the right approach. We should focus on being a leader in cyber security rather than being led by the world. In India, ease of doing business acts a major roadblock for development of the domestic industry. India is ranked at the position of 136 when it comes to places in ease of doing business in the world.Apart from the Government , the onus is also on the youth of India who should share the responsibility of dealing with cyber security while developing new businesses.

Clarity is needed to understand, identify or define critical information. The IT Act Section 17- mentions a protective system and in its 2008 amendment there is also a mention and definition of what critical information infrastructure is. There is lack of awarenesson the provision of the IT Act.

Section 43A of IT Act- hold a 'body corporate' accountable to protect data privacy of data subject (provider of information).

Section 66F- Cyber terrorism, any attack on critical information infrastructure, there will be life imprisonment. There has to be legal cooperation with the other countries at the international level to punish cyber criminals across borders.

Prioritization of the Critical information infrastructure (CII) is an urgent need across government and private sectors. The major threats to CII the identification of critical assets prioritization and how to find CII protection index.

Security is asovereign right, which the Government is duty bound to implement and protect. All the efforts related to cyber security should to be led by the Government and supported by the private sector.

The salary paid in the gGovernment today is very low compared to the private sector, thusthe best brains of the country work in the R&D department of private companies.

The government shouldconsider higher investments into our put in a lot of money into our academic institutions for building skilled human resources with specialization in cyber security and attacks

There is Lack of security trained as well as certified resources to run and continuously monitor technical infrastructure and protectthe information across the government and public sector.

There is ambiguity with regards to the organizational reporting structure of a CISO.

There is a gap with respect to the organizational infrastructure policy, guidelines, standards and best practices. This leads to lack of security audits as well as using validated and certified ICT products.

Security governance at the leadership and board level is missing.

Using any new technologies/applications in the market is possible threat and users should be aware of the implications before using it. For ex: Users keep downloading viruses and don't even know if they should report it and where.

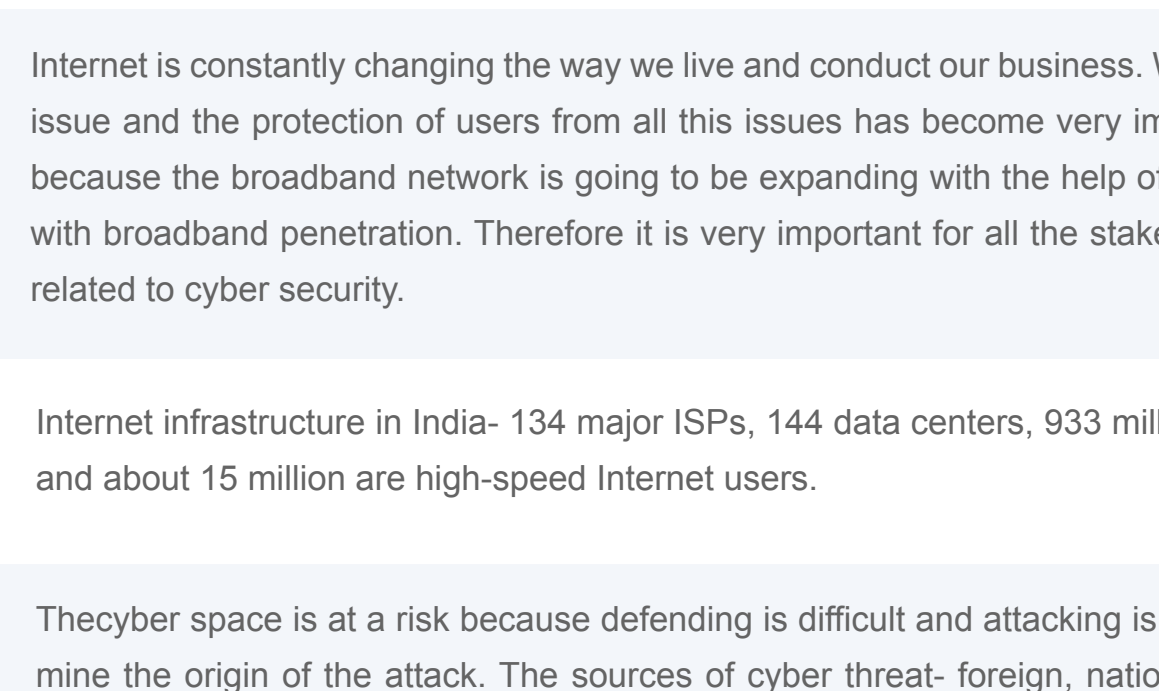
Lack of collaborative R&D with the industry exists in cyber security.

We don't find much of human resourcesin the areas of security divisionof the organizational and other places. There are no courses explaining or teaching legal contracts from a security purpose and what are their implications.

Issues and challenges from testing and evaluation of ICT and infrastructure components need to be addressed.

Inconsistent global laws leading to delay and non-availability of cooperation in cybercrime. Also trust deficit in public and private partnership adds to it.

TECHNICAL SESSION ON "ADDRESSING THE ROADBLOCKS WITH INDUSTRIES PARTICIPATION"



Objective: To bring the representatives from stakeholders like government and industry on a common platform to find solutions to the above identified roadblocks

The key points mentioned by the various distinguished speakers in the sessions are as follows:

Total security industry in USD 160 billion globally. Around 50% of it is in US and 40% of it is in Europe, for rest of the world it's for 10%. In India the government is the largest owner, operator of the critical infrastructure. Thus the government has to invest supporting and encouraging the development of the domestic industry.

Unfortunately enforcement in India is a huge roadblock. Another bigroadblock in this India is the lack of standards as they clearly haven't been updatedand have not kept pace with the rest of the world.

Internet is constantly changing the way we live and conduct our business. With the rapid growth of internet, security has become a major issue and the protection of users from all this issues has become very important. Cyber security is going to have a lot of significance because the broadband network is going to be expanding with the help of government to the village level, so the entire country will be with broadband penetration. Therefore it is very important for all the stakeholders to be aware of all the importance and all the issues related to cyber security.

Internet infrastructure in India- 134 major ISPs, 144 data centers, 933 million mobile phones out of which 414 million are Internet users and about 15 million are high-speed Internet users.

Thecyber space is at a risk because defending is difficult and attacking is easy. Because it is a borderless territory,it is difficult to determine the origin of the attack. The sources of cyber threat- foreign, national, criminal groups, hackers and terrorists and the types of attacks they face are internet spoofing, data theft, malicious soft wares, malware and so many more.

Malware has become a very big threat with authors of malware focusing on detection and new infection methods. The threats are based on application. Cyber threat has evolved over a period of time. 32% are phishing threats, 29 viruses, malicious, 18% network, scanning and proving thefts. The trends show that we are seeing the cyber threat is sophisticated trends, attackers are refining their methods and consolidating assets and creating global networks. Also now there are not individuals, but group'scoordinating with each other with those thefts.

Awareness is lacking but we should not go overboard and create a scare. There has to be a balance between threats and creation of awareness and training and retention.

Currently the cyber security policy in India is should focus on IT Act 2000 amendment bill, best practices ISO 27001, security assurance framework with the companies, capacity building as an ongoing process, forensic centers. Government has implemented mandatory ISO 27001 by all critical sectors and this standard has 3 components- technologies, process incident reporting and monitoring. Out of 7735 certificates issued worldwide, 296 have been issued in India and a majority of these are given in the IT, ITS and the BPO sector.

Cyber security has to be a network element approach:

1. Service providers, which are known as OTT (over the top service providers) –Google, Facebook, Flipkartetc.
2. Telecom service provider, which are becoming a bearer
3. Terminal like laptops and now smartphone, tablets etc.

Already the DOT has made a policy mechanism for testing the equipment to be inducted. The only thing we should look forward to into in the near future is an identifiedan identified lab within the country so that any OEM can approach the lab and get the equipment security certificate. One of the roles that DOT is investigating is the inherent indigenous certification. Every country is doing this process like in US, China, Japan.

If we have to consider R&D for cyber security in India one thing that we can do is to make a multi-terabyte router.

Some countries have a very dedicated policy of how their international traffic will go. The international traffic is only being exchanged on a very minimal inter connection. Not every technology is being used, to use international traffic exchange. If India has to make its cyber space secure one input can be that we carry out very concentrated R&D to make very big routers and it should be mandatory by government that every internet packet is exchanged and the other technology if we deploy in conjunction with this is called a Deep packet inspection(DPI). There are a lot of researches going on, on how to make a deep packet engine because the problem with DPI is that the moment we start seeing every packet, that was that packet is containing then we end up slowing the line speed. The other challenge apart from reducing the line speed is the power consumption of such a huge processing.

The recent worrying trend is known as BYOD- Bring your own device. A lot of companies for professional reasons have a mobile workforce and there are disgruntled insiders. Counter to the BYOD is a new concept, which is emerging, which is called COPE- Corporate owned personally enabled which means that the company will buy the smartphone and give it to the workforce and they will enable that what applications a particular employee at what level will be able to access. Another recommendation will be that there is a thing known as secure software development.

In mobile network security there is mobile handset, mobile backbone and mobile servers and mobile applications. These are the basic foundation and building blocks. It depends on how the threats are characterized. We have to understand where the threat lies and what is the cost associated with it. If it is a network operation or it is redeployment.

It is not the role of the equipment manager to design the operator network. So the ownership lies with the operator to integrate all the security controls stage by stage.All these things depend on various aspects that depend on how actually you can cater and bundle in a package and sell. So this depends on security in built in each and every stage. First we have to see the core of every device, how it actually bears and that depends on developing the software lifecycle process.

About
Neeti Foundation

Neeti Foundation is an independent think tank registered under Indian Trust Act, 1882 emerging as a center of excellence for public affairs and advocacy. It is a public policy research and training network based in New Delhi & Washington DC. We are guided by an Advisory Board consisting of eminent economists, academics, jurists and leaders from media, civil society, bureaucracy and corporate sector. Our mission is to foster leadership based on enduring values. We a non-partisan platform for addressing critical issues and generating political will and public action to implement the required solutions

Neeti has an unmatched network of human resources work on policy analysis, capacity building and program implementation. These consist of researchers, apex level training institutions, governance experts, development practitioners, political leaders, media persons, and international partners

Our mandate is to build networks and evolve policies and innovative solutions, economic and political issues for India and South Asia – a region that combines the most pressing development challenges globally as also a combined GDP in excess of USD 5 trillion. We endeavor to bring together all stakeholders on a shared platform to debate and find solutions to issues related to India's development. By doing so, Neeti Foundation seeks to emerge as a premier forum for neutral yet passionate intellectual discourse and hands-on action.

It is our policy to share with the public our knowledge products, training modules and program documents, following an open source, copy left philosophy

WHAT WE DO

Forum for Inclusive Governance
The Forum has been created to narrow the gap between the theory and practice of democratic governance. Accordingly, we work with institutions and citizens towards faster and more inclusive growth. We work towards reinforcing good governance, strengthening capacity through Information & Communications Technology (ICT), partnering with civil society and the private and public sector (including financial institutions), to meet global and national goals for inclusive, sustainable development. We also provide training and programme management support for Financial Inclusion and Corporate Social Responsibility (CSR) initiatives by the public/private sector. These would be the areas of core competence for Neeti Foundation.

Forum for Energy & Environment
Within this Forum, Neeti Foundation works on policy reform and advocacy for sustainable management of energy and environment, including power sector reforms and climate change mitigation and adaptation. Sustainable human development means that the citizens experience a better quality of life and our natural resources, including Water, Land and Forests are sustainably managed and conserved. Policy analysis and building capacity for improved access to energy resources and low carbon economy will be a special area of focus for the forum.

Forum for International Cooperation
Neeti Foundation recognizes the critical need for internationalfor international cooperation and dialogue on trade, security, intellectual property rights and global public goods. We work towards bringing stakeholders together to debate and discuss issues crucial to international relations through workshops, conferences and seminars. The forum also focuses on human security, internet governance and cybersecurity.

Forum for Political Leadership
This forum will focus on generating political will for reform and improved understanding amongst politicians, their staff and campaign teams regarding laws, policies and best practices pertaining to economic and social development. We undertake research on parliamentary practice, thematic issues and constituency profiling to engender evidence based advocacy and action.

Youth Leadership Initiative
This will be a unique initiative at Neeti Foundation. We will support promising youth as "Leaders of the Future". The initiative will consist of training sessions and workshops with proven and emerging leaders from various fields, including social entrepreneurs, leaders of Self Help Group federations and elected representatives, especially women.

Join the conversation at
www.neeti.foundation

you can also email us at
info@neeti.foundation