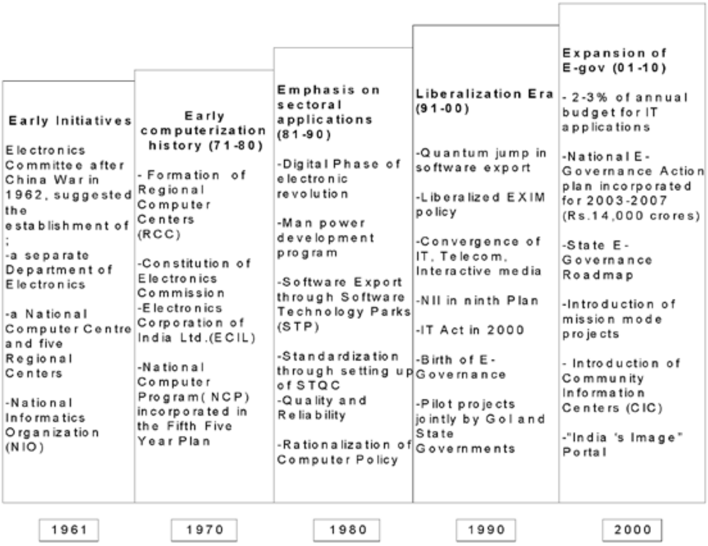
Information Security Landscape in India

MANMOHAN CHATURVEDI
MP GUPTA
JAIJIT BHATTACHARYA

India's information policy has its roots into aftermath of the two early wars India fought after gaining independence from the British rule in 1947; one with Pakistan immediately after independence and the other one with China in 1962. Today we see massive efforts on laying telecommunications networks, back-end computerisation, converging technologies, developing sound monitoring systems and heavy emphasis on e-governance. Figure 1 depicts very succinctly the decade-wise evolution of e-governance systems in India.

It describes the Indian experience of technology in the government in two phases. In the first phase (late 1960s to 1980's), IT was used for in-house government applications with principal focus on Central Government requirements in defence, research, economic and monetary planning and certain data intensive functions related to elections, census and tax administration. This phase ('Pre-Internet era') saw only computerisation of basic processes for government offices, without connectivity provided for integration. The second phase (the 'Post Internet era') started off with major efforts in e-governance. The National Informatics Center (NIC) set up in the early seventies played a crucial role in deployment of e-governance applications. In 1998, Prime Minister Vajpayee set up a high powered National IT task force that made 108 recommendations. This resulted into some major policy initiatives such as creation of a separate Ministry of Information Technology in the year 1999, approval of IT Act 2000 by the Parliament and a policy of allocating 2 to 3% of the budget for IT in each government ministry. Further, in the 'Tenth Five Year Plan' (2002-2007) the Government of India allocated $3.2 billion towards e-government applications in the country. There has also been an increasing involvement of international donor agencies such as DFID, G-8, UNDP and World Bank under the framework of e-governance for development. All these culminated into the announcement of a National-level E-Governance Plan (NEGP) by the IT Minister on 16 May 2006 with an outlay of 33000 crore Indian rupees with an aim to create the right governance and institutional mechanisms, set up core infrastructure and policies and implement a number of Mission Mode Projects at the Centre, State and integrated service levels to create a citizen-centric and business-centric environment for governance. Apart from Mission Mode projects, other three major components of NEGP include creation of State Wide Area Network; State Data Centre (SDC) and 100,000 Community Service Centers (CSC) to serve among a cluster of 6 villages in the country and provide a range of services (more than eighty). Now every state of India has an IT Policy in place and is involved in the development and implementation of new projects across the various departments of the government viz. land records, agriculture, finance, insurance, banking, education etc. There are more than 7000 government websites to offer a variety of services to users.

Figure 1: Transition of Indian e- governance systems over the decades (Source: Gupta, 2010)



Early Initiatives

Electronics Committee after China War in 1962, suggested the establishment of ;

-a separate Department of Electronics

-a National Computer Centre and five Regional Centers

-National Informatics Organization (NIO)

1961

Early computerization history (71-80)

- Formation of Regional Computer Centers (RCC)

-Constitution of Electronics Commission

-Electronics Corporation of India Ltd.(ECIL)

-National Computer Program(NCP) incorporated in the Fifth Five Year Plan

1970

Emphasis on sectoral applications (81-90)

-Digital Phase of electronic revolution

-Man power development program

-Software Export through Software Technology Parks (STP)

-Standardization through setting up of STQC

-Quality and Reliability

-Rationalization of Computer Policy

1980

Liberalization Era (91-00)

-Quantum jump in software export

-Liberalized EXIM policy

-Convergence of IT, Telecom, Interactive media

-NII in ninth Plan

-IT Act in 2000

-Birth of E-Governance

-Pilot projects jointly by GoI and State Governments

1990

Expansion of E-gov (01-10)

- 2-3% of annual budget for IT applications

-National E-Governance Action plan incorporated for 2003-2007 (Rs.14,000 crores)

-State E-Governance Roadmap

-Introduction of mission mode projects

- Introduction of Community Information Centers (CIC)

-"India 's Image" Portal

2000

The enactment of IT Act 2000 by the Indian Parliament was the most significant step that allowed electronic records, digital signatures and a notification in electronic gazette to be legally recognised.

The enactment of IT Act 2000 by the Indian Parliament was the most significant step that allowed electronic records, digital signatures and a notification in electronic gazette to be legally recognised. Further, to give effect to these provisions appropriate amendments have been made in the Indian Penal Code-1860, the Indian Evidence Act-1872, the Bankers' Books Evidence Act-1891 and the Reserve Bank of India Act-1934. These amendments have made these statutes compatible with the "e-justice system". Despite an IT Act in place, the recent few years have seen rise in hacking, website defacement, breach of privacy and data theft. The BPO industry was much affected. In view of this, the IT Act 2000 has been substantially amended to deal with new forms of Cyber Crimes like publicising sexually explicit material in electronic form, video terrorism, and breach of confidentiality and leakage of data by intermediary and e-commerce frauds through the IT Amendment Act 2008 which was passed by the two houses of the Indian Parliament on December 23, and 24, 2008.

Industry Response

After liberalisation of the Indian economy, the large size of the Indian market attracted Foreign Direct Investment (FDI) to provide both telecommunication and IT services. According to the Department of Industrial Policy and Promotion (DIPP)[1], the telecommunications sector which includes radio paging, mobile services and basic telephone services attracted FDI worth US$ 1.33 billion during April-January 2010-11. The cumulative flow of FDI in the sector during April 2000 and January 2011 is US$ 10.26 billion.

Poised to become a US$ 225 billion industry by 2020, the Indian IT industry has played a key role in putting India on the global map. The export revenues are estimated to have aggregated to US$ 59 billion in FY2011 and contributed 26 per cent as its share in total Indian exports.[2]

The roll out of 3G services followed by Next Generation Networks (NGN) is on the horizon. These services are fast becoming a vehicle for Value Added Services (VAS) that is certain to drive the e-commerce and e-governance applications. However, the initiatives to secure these services are not moving at the same pace. The reason is not far to seek. Unless strict regulatory and legal frameworks force the adoption of best practices for cyber security the organisations both in private and government sector tend to dither.

Indian IT and ITeS/BPO (Information Technology enabled Services / Business Process Outsourcing), which started with the advantage of low-cost human resources, have now moved on to add quality and diversity as its differentiators. They will now need to tackle the problem of offering consistent data security to the customers at an affordable cost. IT (Amendment) Act, 2008 has certain provisions to deal with this. The security landscape, however, is constantly evolving, as the threats, consumer perceptions and legislative and regulatory strategies keep changing. These are the challenges that will need to be met with effective responses. Different countries have enacted laws to deal with Data Protection and Data Privacy. In view of the multiplicity of privacy legislations worldwide, the service providers in India are faced with a major challenge of demonstrating compliance with laws of countries where the data originates.

In a response to this, National Association of Software and Services Companies (NASSCOM) established Data Security Council of India (DSCI) as a self - regulatory organisation (SRO) in August 2008. DSCI, through a number of security awareness seminars and workshops, has brought out several manuals on best practices and standards for enhancing trust.

CERT-In (Computer Emergency and Response Team- India) under the Department of Information Technology (DIT)[3] was set up in January 2004 to provide both reactive and proactive services and also create awareness on various aspects of cyber security. In 2008, its role was partially improved and incorporated under the amendments to the IT Act 2000 (IT Act 2008). CERT-In functioning under DIT is India's response to cyber threats with mandate to become the nation's most trusted referral agency of the Indian community for responding to computer security incidents as and when they occur.

Figure 2 illustrates the growing number of Indian incidents reported by the CERT-In from 2004 to 2010. Figure 3 describes the categories of the incidents reported in 2010 in India. As can be seen, attacks on the websites account for maximum share of the recorded incidents in the year 2010 (61%). In a digital economy a website is the most essential component of e-governance and e-commerce initiatives. The threat vector is targeted at the root of the online systems and therefore, needs urgent attention.

Figure 2: Incidents Reported by CERT-In 2004–2010 (Source: CERT-In, 2012)

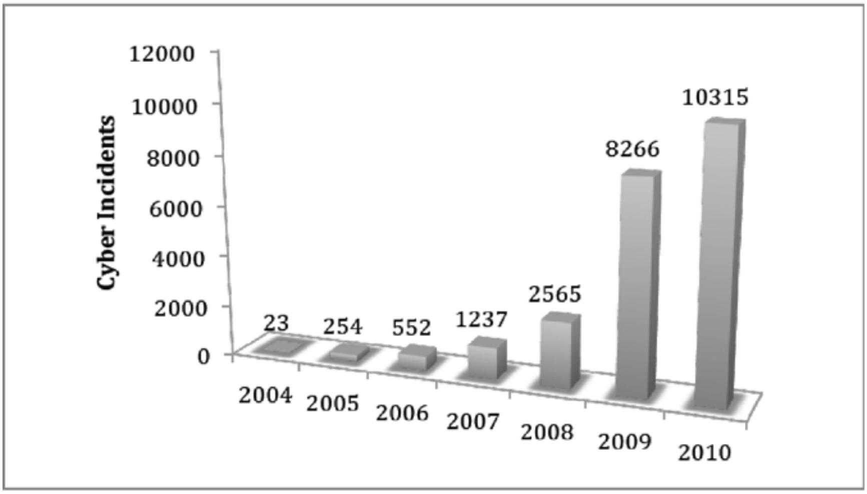
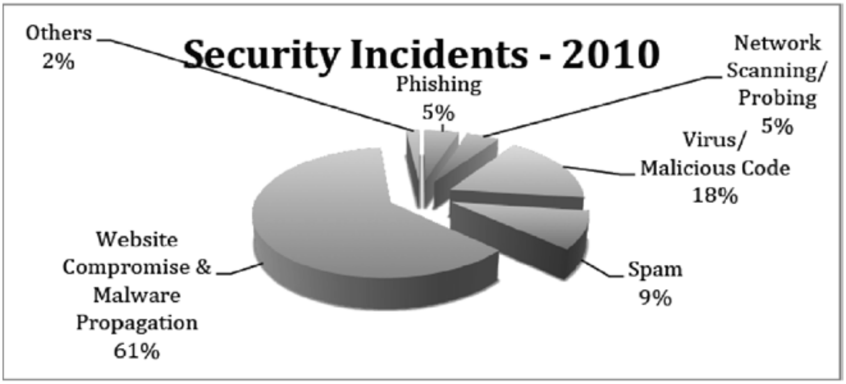


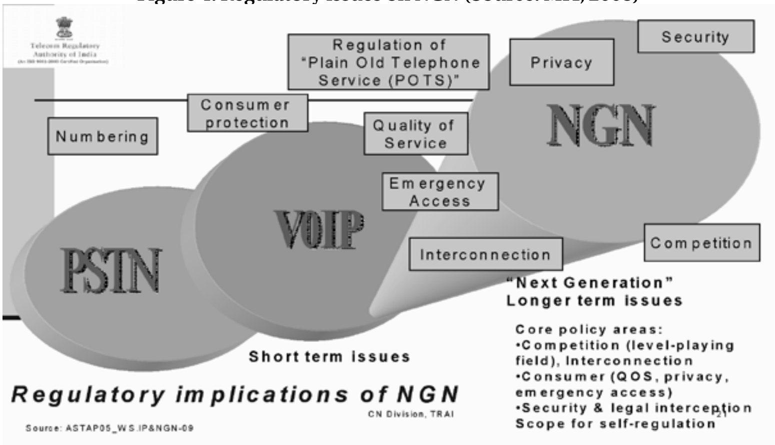
Figure 3: Categories of the 2010 incidents in India (Source: CERT-In, 2012)



Evolution of Next Generation Networks

The growth of IT sector in India has been fuelled by equally impressive growth in telecommunication infrastructure. The world is moving towards converged networks being referred as 'Next Generation Networks (NGN)'.In the coming decade the NGN is likely to replace the legacy networks. This upcoming national information infrastructure would be marriage of IT and telecommunication infrastructure with various regulatory and security challenges that need careful scrutiny.

Figure 4: Regulatory issues on NGN (Source: MIT, 2008)



Telecom Regulatory Authority of India (An ISO 9001:2000 Certified Organisation)

Regulation of "Plain Old Telephone Service (POTS)"

Security

Privacy

Consumer protection

Numbering

Quality of Service

NGN

Emergency Access

VOIP

PSTN

Interconnection

Competition

"Next Generation" Longer term issues

Core policy areas:
•Competition (level-playing field), Interconnection
•Consumer (QOS, privacy, emergency access)
•Security & legal interception
Scope for self-regulation

Short term issues

Regulatory implications of NGN

CN Division, TRAI

Source: ASTAP05_WS.IP&NGN-09

Regulatory issues on deployment of NGN

The deployment of NGN throws up many regulatory challenges as highlighted in Figure 4 . License conditions and regulations need to be revisited with a light touch regulatory approach with participation of all stakeholders to ensure smooth transition.

In case of legacy networks the business model, network and competition were already in place before establishment of a formal regulatory framework. NGN permits us a window of opportunity to review regulatory framework by a proactive consultation process and spirit of accommodation amongst all stakeholders. Regulators in many developing countries including India (MIT, 2008) have begun the process of firming up broad principles for NGN deployment ahead of actual transition. The telecom sector in India is on a growth profile, and time is ripe to examine regulatory and licensing approaches for NGN deployment. New competitive networks are just being established and the consumer's take-up of IP services and Broadband is at a nascent stage.

Table 1: Security aspects of NGN (Source: MIT, 2008)

Security Aspects of NGN	
National Security and Infrastructure Protection	• Network attack mitigation • Public safety emergency and law enforcement/national security assistance • Priority access during or after disaster • Priority service provisioning and restoration • Analysis and reporting of network metrics and outages
Legal System Requirements	• Cyber crime mitigation • Digital rights management • Fraud detection and management • Judicial evidentiary and forensics

Security aspects of NGN

Some of the regulatory requirements pertaining to security aspects of NGN are highlighted in Table 1. As can be seen Cyber Crime mitigation is one of the dimensions of security aspects. Actually the NGN which is an IP protocol based network is expected to inherit many of the known vulnerabilities of current generation Internet infrastructure. Therefore, all policy initiatives to counter cyber threats are equally applicable to the evolving NGN. As highlighted by the Table 1 the security issues connected with NGN have additional dimensions besides Cyber Crime mitigation. National security is likely to be impacted by a changeover to NGN as a replacement to the comparatively secure traditional PSTN network.

The transition to NGN from legacy networks in India and rest of the world is essentially driven by technology but fuelled by innate needs of individuals and society to acquire functionalities that provide ubiquitous connectivity. It changes the way society and individuals within society function. The convergence of voice, video and data services provides an opportunity for telecom service providers to minimize the operational costs while offering niche applications to ever increasing users. ITU's Telecommunication Standardization Sector ITU-T report "Trends in Telecommunication Reform: the Road to NGN" published in September 2007, predicts that full implementation of NGN in fixed line networks in developed countries will be deployed by 2012 and in mobile networks by 2020 (Next-Generation Networks and Energy Efficiency, 2008). According to another report by the Telecommunication Development Bureau of International Telecommunication Union (Developments of Next Generation Networks (NGN): Country Case Studies, 2009) a number of market players around the world are already operating NGN core networks, increasing numbers of market players are deploying NGN access, and others have made significant commitments to roll out fiber access networks or have migration plans for moving to all-IP networks. It is therefore safe to predict that the transition to NGN is certain to take place.

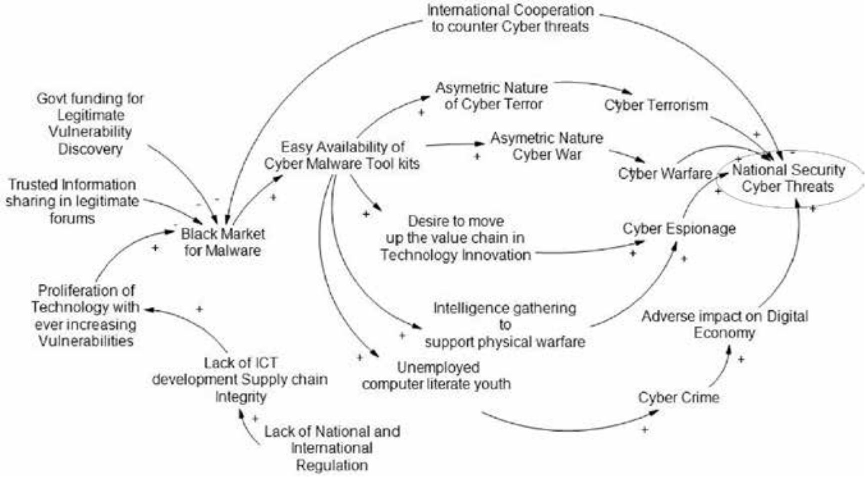
Like any major transition the existing framework of regulation needs to be revisited to ensure a smooth change over. Choice is not about whether to transit but when to transit. Vacillation to finalise rules of the game can harm our national interest as we should be in step with the rest of the world that stands on the cusp of future opportunities. In a globalised world we cannot insulate our ICT infrastructure from rest of the world. International effort coordinated by ITU on this subject is moving ahead in a focused manner. The Department of Telecommunication and Telecom Regulatory Authority of India have taken proactive measures to generate a consensus amongst all stakeholders as we move in unchartered waters.

The security challenges, as described earlier, are more daunting with NGN as compared with its traditional predecessor PSTN telecommunication network. The national initiatives for combating Cyber Security threats need to be augmented for safe migration to NGN from earlier safer, though technologically outdated and operationally uneconomical, PSTN based telecommunication infrastructure.

Threat Scenario at National level

Figure 5 attempts to describe through an illustrative causal loop diagram the threat to national security from diverse dimensions. The challenge to a nation state is to initiate comprehensive steps to mitigate the ill effects of the causes of the threat. For example in Figure 5; trusted information sharing in legitimate forums, government funding for legitimate vulnerability discovery and international cooperation to counter cyber threats are three illustrative steps attempting to counter the threat chain and are having a negative (-) sign on the arrows emanating from them. We need to identify a comprehensive and parsimonious set of steps that can be initiated at the national level to address the emerging threats.

Figure 5: Illustrative Causal Loop Diagram for Cyber Threats to National Security


International Cooperation to counter Cyber threats
Asymetric Nature of Cyber Terror
Cyber Terrorism
Govt funding for Legitimate Vulnerability Discovery
Easy Availability of Cyber Malware Tool kits
Asymetric Nature Cyber War
Cyber Warfare
National Security Cyber Threats
Trusted Information sharing in legitimate forums
Black Market for Malware
Desire to move up the value chain in Technology Innovation
Cyber Espionage
Proliferation of Technology with ever increasing Vulnerabilities
Intelligence gathering to support physical warfare
Adverse impact on Digital Economy
Lack of ICT development Supply chain Integrity
Unemployed computer literate youth
Cyber Crime
Lack of National and International Regulation
+
-

National level agencies connected with Information Security

A draft National Cyber Security Policy put up for public consultation in March 2011(National Cyber Security Policy, 2011) describes following organisations connected with national level cyber security issues. The brief description about their roles provides us a peep into the dynamics of cyber security initiatives at national level. However, in the absence of an official hierarchical structure amongst these organisations in the draft policy, the picture seems fragmented. A more detailed structure with a clearly defined accountability matrix is essential for any meaningful analysis of its efficacy.

a. National Information Board (NIB)

National Information Board is an apex agency with representatives from relevant departments and agencies that form part of the critical minimum information infrastructure in the country. NIB is entrusted with the responsibility of enunciating the national policy on information security and coordination on all aspects of information security governance in the country. NIB is headed by the National Security Advisor.

b. National Crisis Management Committee (NCMC)

The National Crisis Management Committee (NCMC) is an apex body of Government of India for dealing with major crisis incidents that have serious or national ramifications. It will also deal with national crisis arising out of focused cyber attacks. NCMC is headed by the Cabinet Secretary and comprises of Secretary level officials of Govt. of India. When a situation is being handled by the NCMC it will give directions to the Crisis Management Group of the Central Administrative Ministry/Department as deemed necessary.

c. National Security Council Secretariat (NSCS)

National Security Council Secretariat (NSCS) is the apex agency looking into the political, economic, energy and strategic security concerns of India and acts as the secretariat to the NIB.

d. Ministry of Home Affairs (MHA)

Ministry of Home Affairs issues security guidelines from time to time to secure physical infrastructure. The respective Central Administrative Ministries/Departments and critical sector organisations are required to implement these guidelines for beefing up/strengthening the security measures of their infrastructure. MHA sensitises the administrative departments and organisations about vulnerabilities and also assists the respective administrative ministry/departments.

e. **Ministry of Defence**

Ministry of Defence is the nodal agency for cyber security incident response with respect to the Defence sector. MoD, IDS (DIARA), formed under the aegis of Headquarters, Integrated Defence Staff, is the nodal tri-Services agency at the national level to effectively deal with all aspects of Information Assurance and operations. It has also formed the Defence CERT whose primary function is to coordinate the activities of services/MoD CERTs. It works in close association with CERT-In to ensure perpetual availability of Defence networks.

Ministry of Defence is the nodal agency for cyber security incident response with respect to the Defence sector.

f. **Department of Information Technology (DIT)**

Department of Information Technology (DIT) is under the Ministry of Communications and IT, Government of India. DIT strives to make India a global leading player in IT and at the same time take the benefits of IT to every walk of life for developing an empowered and inclusive society. It is mandated with the task of dealing with all issues related to promotion and policies in electronics and IT.

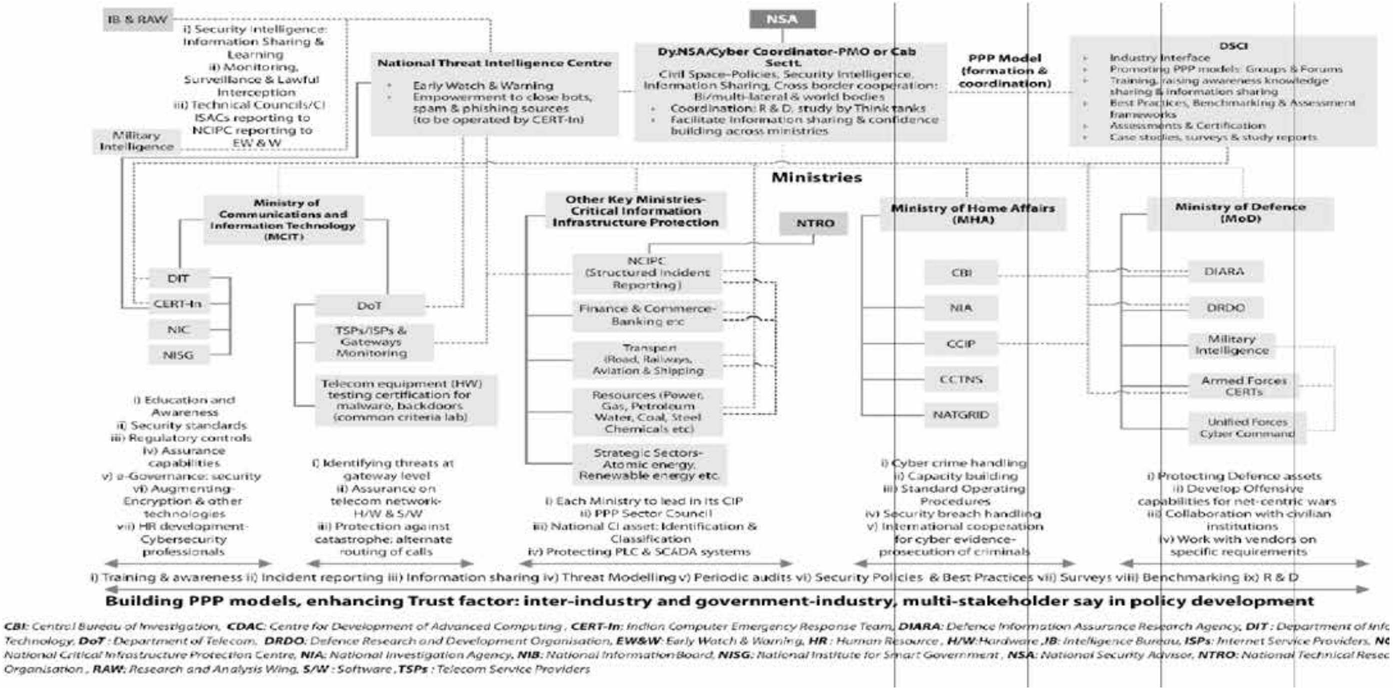
g. **Department of Telecommunications (DoT)**

Department of Telecommunications (DoT) under the Ministry of Communications and Information Technology, Government of India, is responsible to coordinate with all ISPs and service providers with respect to cyber security incidents and response actions as deemed necessary by CERT-In and other government agencies. DoT will provide guidelines regarding roles and responsibilities of Private Service Providers and ensure that these Service Providers are able to track the critical optical fiber networks for uninterrupted availability and have arrangements of alternate routing in case of physical attacks on these networks.

h. **National Cyber Response Centre - Indian Computer Emergency Response Team (CERT-In)**

CERT-In monitors Indian cyberspace and coordinates alerts and warning of imminent attacks and detection of malicious attacks among public and private cyber users and organisations in the country. It maintains 24x7 operations centre and has working relations/collaborations and contacts with CERTs all over the world and sectoral CERTs, academia, and public and private Internet Service Providers and vendors of IT products in the country.

Figure 6: National Structure for Cyber Security (Source: NASSCOM-DSCI, 2012)


IB & RAW
i) Security intelligence: Information Sharing & Learning
ii) Monitoring, Surveillance & Lawful Interception
iii) Technical Councils/CI ISACs reporting to NCIPC reporting to EW & W
Military Intelligence
National Threat Intelligence Centre
• Early Watch & Warning
• Empowerment to close bots, spam & phishing sources (to be operated by CERT-In)
NSA
Dy.NSA/Cyber Coordinator-PMO or Cab Sectt.
Civil Space–Policies, Security Intelligence, Information Sharing, Cross border cooperation: Bi/multi-lateral & world bodies
• Coordination: R & D, study by Think tanks
• Facilitate Information sharing & confidence building across ministries
PPP Model (formation & coordination)
DSCI
• Industry Interface
• Promoting PPP models: Groups & Forums
• Training, raising awareness knowledge sharing & information sharing
• Best Practices, Benchmarking & Assessment frameworks
• Assessments & Certification
• Case studies, surveys & study reports
Ministries
Ministry of Communications and Information Technology (MCIT)
DIT
CERT-In
NIC
NISG
DoT
TSPs/ISPs & Gateways Monitoring
Telecom equipment (HW) testing certification for malware, backdoors (common criteria lab)
Other Key Ministries-Critical Information Infrastructure Protection
NTRO
NCIPC (Structured Incident Reporting)
Finance & Commerce-Banking etc
Transport (Road, Railways, Aviation & Shipping
Resources (Power, Gas, Petroleum Water, Coal, Steel Chemicals etc)
Strategic Sectors-Atomic energy, Renewable energy etc.
Ministry of Home Affairs (MHA)
CBI
NIA
CCIP
CCTNS
NATGRID
Ministry of Defence (MoD)
DIARA
DRDO
Military Intelligence
Armed Forces CERTs
Unified Forces Cyber Command
i) Education and Awareness
ii) Security standards
iii) Regulatory controls
iv) Assurance capabilities
v) e-Governance: security
vi) Augmenting-Encryption & other technologies
vii) HR development-Cybersecurity professionals
i) Identifying threats at gateway level
ii) Assurance on telecom network-H/W & S/W
iii) Protection against catastrophe: alternate routing of calls
i) Each Ministry to lead in its CIP
ii) PPP Sector Council
iii) National CI asset: Identification & Classification
iv) Protecting PLC & SCADA systems
i) Cyber crime handling
ii) Capacity building
iii) Standard Operating Procedures
iv) Security breach handling
v) International cooperation for cyber evidence-prosecution of criminals
i) Protecting Defence assets
ii) Develop Offensive capabilities for net-centric wars
iii) Collaboration with civilian institutions
iv) Work with vendors on specific requirements
i) Training & awareness ii) Incident reporting iii) Information sharing iv) Threat Modelling v) Periodic audits vi) Security Policies & Best Practices vii) Surveys viii) Benchmarking ix) R & D
Building PPP models, enhancing Trust factor: inter-industry and government-industry, multi-stakeholder say in policy development
CBI: Central Bureau of Investigation, CDAC: Centre for Development of Advanced Computing , CERT-In: Indian Computer Emergency Response Team, DIARA: Defence Information Assurance Research Agency, DIT : Department of Info
Technology, DoT : Department of Telecom, DRDO: Defence Research and Development Organisation, EW&W: Early Watch & Warning, HR : Human Resource , H/W:Hardware ,IB: Intelligence Bureau, ISPs: Internet Service Providers, NC
National Critical Infrastructure Protection Centre, NIA: National Investigation Agency, NIB: National Information Board, NISG: National Institute for Smart Government , NSA: National Security Advisor, NTRO: National Technical Resea
Organisation , RAW: Research and Analysis Wing, S/W : Software ,TSPs : Telecom Service Providers

It would work with Government, public and private sectors and users in the country and monitor cyber incidents on continuing basis throughout the extent of the incidents to analyse and disseminate information and guidelines as necessary. The primary constituency of CERT-In would be organisations under the public and private sector domains.

i. **National Information Infrastructure Protection Centre (NIIPC)**

NIIPC is a designated agency to protect the critical information infrastructure in the country. It gathers intelligence and keeps a watch on emerging and imminent cyber threats in strategic sectors including National Defence. It would prepare threat assessment reports and facilitate sharing of such information and analysis among members of the Intelligence, Defence and Law enforcement agencies with a view to protecting these agencies' ability to collect, analyse and disseminate intelligence. NIIPC would interact with other incident response organisations including CERT-In, enabling such organisations to leverage the Intelligence agencies' analytical capabilities for providing advanced information of potential threats.

NIIPC is a designated agency to protect the critical information infrastructure in the country. It gathers intelligence and keeps a watch on emerging and imminent cyber threats in strategic sectors including National Defence.

j. **National Disaster Management of Authority (NDMA)**

The National Disaster Management Authority (NDMA) is the Apex Body for Disaster Management in India and is responsible for the creation of an enabling environment for institutional mechanisms at the State and District levels. NDMA envisions the development of an ethos of Prevention, Mitigation and Preparedness and is striving to promote a national resolve to mitigate the damage and destruction caused by natural and man-made disasters, through sustained and collective efforts of all Government agencies, Non-Governmental Organizations and people's participation.

k. **Standardization, Testing and Quality Certification (STQC) Directorate**

STQC is a part of Department of Information Technology and is an internationally recognized Assurance Service providing organization. STQC has established nation-wide infrastructure and developed competence to provide quality assurance and conformity assessment services in IT Sector including Information Security and Software Testing/Certification.

It has also established a test/evaluation facility for comprehensive testing of IT security products as per ISO 15408 common criteria security testing standards.

l. **Sectoral CERTs**

Sectoral CERTs in various sectors such as Defence, Finance (IDRBT), Railways, Petroleum and Natural Gas, etc, would interact and work closely with CERT-In for mitigation of crisis affecting their constituency. Sectoral CERTs and CERT-In would also exchange information on latest threats and measures to be taken to prevent the crisis.

While efforts to protect the organisational information system assets can be initiated by adopting any of the available guidelines and third party audit of the actual implementation, the challenge of cyber threat still remains.

Cyber Security Advisory Group recommended National Structure for Cyber Security

A Cyber Security Advisory Group (CSAG), having representation from public and private sectors, under aegis of NASSCOM and DSCI (NASSCOM-DSCI CSAG Report, 2012) has recommended an organisation structure (Figure 6) to address the key Cyber Security concerns at the national level. This structure would enable effective and efficient decision making which involves consultation across multiple stakeholders – policy makers, various ministries, state governments, defence, intelligence, LEAs, private sector among others.

The structure attempts to capture the roles and responsibilities for every stakeholder; establish coordination and information sharing mechanisms; focus on building PPP models and create an environment for enhancing trust between the industry and government. The structure may evolve with the working experience to meet emerging challenges.

Need for a comprehensive view of national cyber security initiatives

While efforts to protect the organisational information system assets can be initiated by adopting any of the available guidelines and third party audit of the actual implementation, the challenge of cyber threat still remains. The reason for this dichotomy lies in the nature of cyber infrastructure which emphasises interconnected information systems. Organisational boundaries merge very quickly with national and international boundaries for any meaningful exploitation of the IT assets. This feature of the networked information systems is the primary reason of the challenge where the chain is as strong as the weakest link. Like biological viruses the malware (viruses, worms and Trojans) in cyber systems require international agreements and regulatory framework to mitigate their virulence.

In today's globalised world the need for international cooperation and regulatory framework can hardly be over emphasised. Still a nation state continues to be the logical entity to implement the agreements reached at international forums. How does one measure the cyber security readiness at national level? The agreements can be on various procedural issues to deter cyber crime or non use of offensive Information Warfare capabilities during peace. The various aspects of the national cyber security initiative need to be viewed through a comprehensive framework applicable at national level. The issues or framework applicable to organisations both public and private within a nation would of necessity have different focus and attention to details than the national perspective.

Concluding Remarks

This position paper has attempted to describe India's present Cyber Security landscape. The historical perspective and compulsions of a globalised information society seem to drive the current policy initiatives at national level. The structure recommended by the Cyber Security Advisory Group (CSAG) should provide a good beginning. The experience gained by the stakeholders can inform further policy initiatives. Emphasis on international treaties, sharing of best practices and joint research initiatives can provide the much needed bedrock for a cyber secure nation.

Air Commodore **Manmohan Chaturvedi** (Retd) is at the School of Engineering and Technology, Ansal University, Gurgaon.

Mr **MP Gupta** and Mr **Jaijit Bhattacharya** are from the Deptt of Management Studies, Indian Institute of Technology, Delhi.

References

Gupta, M.P.(2010).Tracking the evolution of E- Governance in India, *International Journal of Electronic Governance Research, January-March 2010,vol.6,No1,pp.46-58.*

MIT(2008),Ministry of Information and Communication Technology, http://mit.gov.in/default.aspx

National Cyber Security Policy (2011), India's National Cyber Security Policy draft v1.0, 26 Mar 2011, www.mit.gov.in

NASSCOM-DSCI (2012),"Securing Our Cyber Frontiers", available at www.dsci.in . Accessed on 20 April 2012.

Air Commodore Manmohan Chaturvedi (Retd) is at the School of Engineering and Technology, Ansal University, Gurgaon.

Mr MP Gupta and Mr Jaijit Bhattacharya are from the Deptt of Management Studies, Indian Institute of Technology, Delhi.

Notes

1. IBEF (India Brand Equity Foundation), http://www.ibef.org/industry/telecommunications.aspx, accessed on 11 June 2011.
2. IBEF(IndiaBrandEquityFoundation),http://www.ibef.org/industry/informationtechnology.aspx, accessed on 11 June 2011
3. Ministry of Information and Communication Technology, http://mit.gov.in/default.aspx, Accessed on 11 June 11.