Cyber Security Infrastructure in India: A Study

M M Chaturvedi[1]*, MP Gupta[1] and Jaijit Bhattacharya[1]

ABSTRACT

Need for cyber security infrastructure to protect the evolving ICT infrastructure in modern information society does not need any emphasis. ICT infrastructure is the thread through which all critical national infrastructures are woven together. Existence of a trustworthy cyber security infrastructure is a precondition for all E-governance and E- commerce initiatives being taken world over. Attempt is being made in this paper to present a snapshot of this infrastructure, likely trends and imperatives that emerge from this study in Indian context.

Keywords: Vulnerability of ICT infrastructure, Regulatory framework for ICT infrastructure, cyber security standards, Next Generation Networks, e-governance, e-commerce.

1. Background

Critical infrastructures are indispensable for the modern society (e.g. banking-finance, energy, communication, commerce, health care, transport), and their failure to meet an expected service level might have a significant impact on the society. An emerging issue is that infrastructures, until now independent, are becoming entangled into network-of-networks. It is this interconnection where the information and communication technologies play a pivotal role. Following paragraph from the executive order of President George W. Bush issued on 16 October 2001 summarizes the key issue in the aftermath of 9/11 attack on the trade tower in USA (Bush,2002)

"The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures. The protection program authorized by this order shall consist of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. Protection of these systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors".

When infrastructures are interconnected, new vulnerabilities might arise from the common links, failures might propagate through the different systems, intrusion and disruption in one infrastructure might provoke unexpected threats to others. In such cases, the question of specifying dependability and trust requirements and translating them as performance and functionality requirements for other systems becomes vital (Masera, .Wilikens. 2000). At the regional and international level, cooperation and coordination amongst countries appears essential using a comprehensive approach. Framework for cyber security and critical

[1] Department of Management Studies, Indian Institute of Technology Delhi, Hauz Khas, New Delhi 110016, India,
* *Corresponding Author:* (E-mail : manmohanchaturvedi@yahoo.com, Telephone: +91 9871078151)

information infrastructure protection would entail a national strategy and creation of legal frameworks to curb cyber crime. Regional workshop on frame works for cyber security and critical infrastructure protection held at Hanoi in August 2007 under the aegis of International Telecommunication Union (ITU 2007) has highlighted the need for national frame works. Many researchers agree that the infrastructure is its own worst enemy because of its complexity (Eeten et al, 2006). Systems begin to blend into one another due to increasing use of ICTs and increasing functional demands and it is useless to try to maintain a separation of systems, each with an internally demarcated mode of responsibility. The distinction between inside and outside the system, and even the concept of systems boundaries as such, becomes blurred.

2. Threats to ICT Infrastructure

Means to exploit, distort, disrupt, and destroy information resources range from hacker tools to devices such as electro magnetic weapons; directed energy weapons; HPM (High Power Microwave) or HERF (High Energy Radio Frequency) guns; and electromagnetic pulse (EMP) cannons. The attack against an information infrastructure can be carried out with both physical implements (hammer, backhoe, bomb, HERF, HPM) and cyber-based hacking tools (Chaturvedi et al, 2007). The same is true for the target: It can be cyber, consisting for example of information or applications on a network, or physical, such as computers or a telecommunications cable. Infrastructure threat matrix (Table 1) distinguishes four types of information attack, all four of which involve the malicious use of the information infrastructure either as a target or as a tool. (Dunn, 2006).

Table1: Infrastructure threat matrix

		Target	
Means/ Tool	Physical	Physical 1) - Severing a telecom cable with a backhoe - Smashing a server with a hammer - Bombing the electric grid	Cyber 2) Use of electromagnetic pulse and radio-frequency weapons to destabilize electronic components
	Cyber	3) - Hacking into a SCADA system that controls municipal sewage - “Spoofing” an air traffic control system to bring down a plane	4) - Hacking into a critical government network - Trojan horse in public switched network

(Source: Dunn, 2006)

3. Initiatives at International level

Cyber security is attracting enormous attention from several international governing and security bodies, including the United Nations (UN), the Organization for Economic Cooperation and Development (OECD), and the North Atlantic Treaty Organization (NATO). Despite this attention, however, there is still no single international governing body whose sole mission is addressing cyber crime. Instead, this issue has become a primary focus for many of these organizations’ subordinate organizations, such as the United Nations’ International Telecommunication Union (ITU) (Nain et al, 2007).

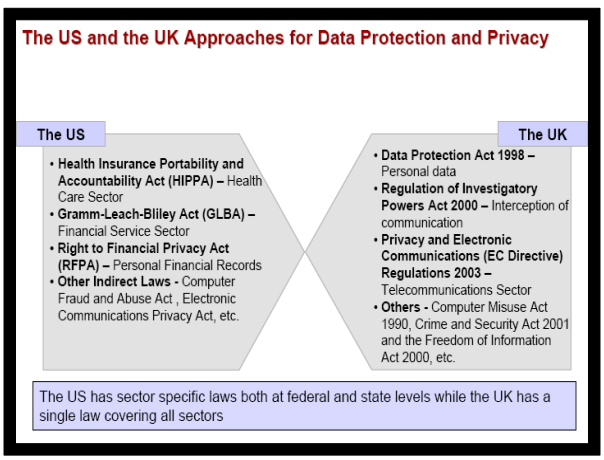
In the 2001 resolution 56/183, the United Nations General Assembly called for the creation of a World Summit on the Information Society (WSIS) where both public and private industries could “…harness synergies and creation of cooperation among the various information and communication technologies initiatives, at the regional and global levels.” (ITU/WSIS, 2002) The Information Telecommunication Union (ITU) was selected to serve in a managerial role over the Summit. The World Summit was held in

two phases: in Geneva in December of 2003 and Tunis in November of 2005(WSIS, 2006).The objective of the Geneva phase was to develop and foster a clear statement of political will and develop a plan for the foundations of "…Information Society for all…" and general plan of action. (WSIS, 2006) Following the meeting, two major areas were seen as important, "…building confidence, trust and security…" and "…establishing stable regulatory frameworks." (WSIS, 2006) Reports from each summit were produced, with the latest update published in June 2007.

In 2006, the United Nations formed the United Nations Group on Information Society (UNGIS) to coordinate the United Nations' efforts on the outcomes of WSIS. "UNGIS serves as an interagency coordinating mechanism within the UN system to implement the outcomes of WSIS. The Group enables synergies aimed at resolving substantive and policy issues, avoiding redundancies and enhancing effectiveness of the system while raising public awareness about the goals and objectives of the global Information Society. UNGIS also works to highlight the importance of ICTs in meeting the "Millennium Development Goals." UNGIS lists its objectives as: the facilitation of synergies between organizations belonging to the UN system to maximize joint efforts, avoidance of duplication and enhancement of effectiveness in achieving the WSIS outcomes, and the promotion of public awareness about WSIS implementation by the UN system. (UNGIS, 2007)

During the last twenty years, security concerns have increasingly impacted on the development and exploitation of Information Systems (IS), both in public and private sectors. The pressure is still increasing in many sectors and organizations, where specific regulations impose advanced security Risk Management (RM) practices. This is the case, for instance in context of USA, with the Sarbanes-Oxley act, which concerns the integrity of financial and accounting data, or, in the banking industry, where the new Basel II agreement defines rules which determine the level of "frozen" capital for financial institutions, based on the maturity of their RM activities, including those related to their IS (Mayer et al, 2006)..

Safeguards have been adopted by countries by enacting laws and directives. The US and the UK have well-defined and comprehensive laws on data security and privacy. The US has sector-specific laws and laws at the federal and the state level. The UK has a comprehensive Data Protection Act covering all sectors.Figure 1 below provides a view of USA and UK approach to data protection and privacy (Saravade,2007).



(Source: Saravade, 2007)

Figure 1: USA and UK approach to data protection and privacy.

Nain et al (2007) have provided an excellent over view of international initiatives to secure cyber space.

According to authors the international landscape of cyber security appears to be somewhat variable. As the magnitude and locality of international, regional, and non-governmental organizations continue to increase, one would expect that the overall effectiveness of cyber security-related mechanisms, laws, programs, countermeasures, and initiatives would improve proportionally. Many new organizations and advocacy groups with cyber security interests are now gaining ground, and most large international organizations are beginning to understand and react to the criticality of information security vulnerabilities. However, due to a general lack of publicly available, up-to-date metrics and statistics on cyber security activities, it is difficult to provide complete justification for these conclusions. The Council of Europe Convention on Cyber crime and the World Summit on the Information Society under aegis of ITU may provide some of the only measurable signs of progress to date in the global initiative to secure cyberspace

4. India's Challenge

Post liberalization, Information Technology (IT), electricity and telecom sector has witnessed large investments by private sector. Infrastructure development using private investment is being pursued in many developing countries including India. However, inadequate focus to disaster preparedness and recovery in regulatory frameworks is a cause of concern. No single operator controls the IT, Telecom or Power sectors and, therefore, responsibility to prepare for, and recover from, disasters is diffused. All operators are driven by the "bottom line," and cannot expend resources on activities that do not contribute to profit (Srivastava, Samarajiva, 2001).

Enterprise level customers value reliable service, including adequate levels of disaster preparedness and recovery. They would be willing to pay for the reliability and survivability of business critical ICT infrastructure. However, in the absence of institutionalized vulnerability analysis and benchmarking of ICT infrastructure, status quo is maintained.

In view of the grave repercussions of infrastructure failure in core sectors like power and telecom, government driven regulatory initiative would be justified even after liberalization. Pragmatic regulation would achieve twin objectives of attracting and retaining private investment to the infrastructure sector; and, efficacy in terms of disaster preparedness and recovery.

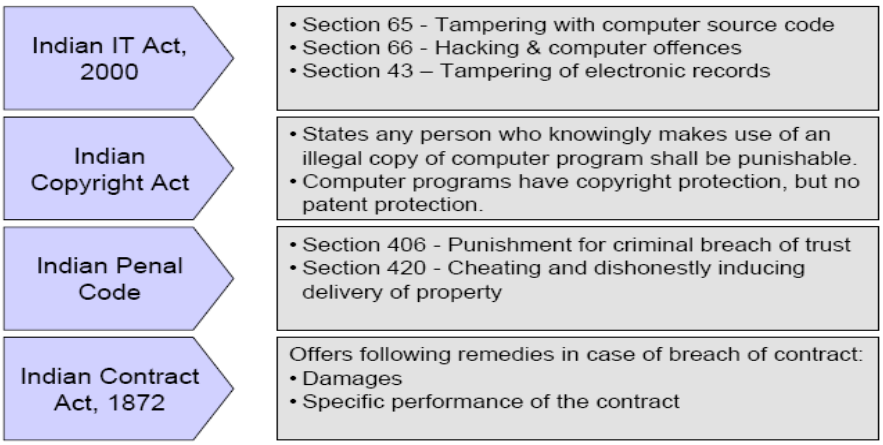
Government agencies, business houses and common citizen alike are embracing the fast evolving ICT infrastructure to facilitate India's march towards e-governance and e-commerce. However, vulnerability of this infrastructure to natural and man made disaster and consequent cascading effect on our national security remains unarticulated.

National Telecom Policy (NTP, 1999) while emphasizing the need for growth of our communication infrastructure, does not specifically address vulnerabilities and action plan. National Disaster Management Authority has highlighted the need for reliable and robust communication support for disaster management and expected performance objectives are being firmed up (NDMA, 2008). Objectives enunciated on official web site of India's Department of Telecommunication (DOT, 2008) do not make any specific mention on this subject. It is surmised that policy makers know these vulnerabilities and suitable remedial measures are being taken. It would be prudent to bring these issues in the open through government–industry dialogue to evolve mutually beneficial arrangements

5. Initiatives taken in Indian Context

India started a process of economic liberalization in the 1990s. One of the main features of this process has been to simplify rules and regulations to attract foreign investment. As a result of this, India is becoming easier to enter from a regulatory and commercial point of view but there are still issues to overcome, one of them being Indian privacy standards for the outsourcing company. India lacks specific laws on privacy and

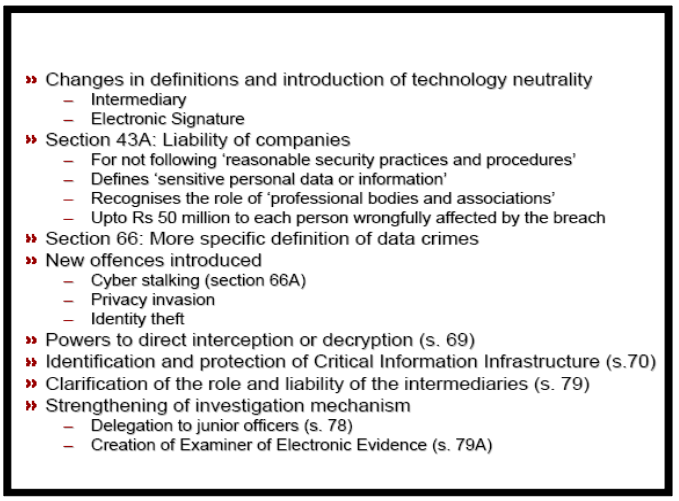
data protection, how ever, there are proxy laws and other indirect safeguards, which provide adequate protection to companies off shoring work (Yadav, N, Priyadarshini,T,2008). . Indian IT act in conjunction with other related acts as shown in figure 2 below provide basic legal frame work.



(Source: Saravade, 2007)

Figure 2: Legal Framework to support Cyber Security in India

As outsourcing becomes more widespread and competition in the marketplace grows, the ability to illustrate the existence and continued use of powerful safeguards will increasingly become one of the significant factors for companies that are deciding which provider to link up with. The Ministry of Information Technology, on August 29, 2005, proposed certain amendments to the Indian IT Act 2000 as indicated in Figure 3.These amendments have been incorporated vide Information Technology (Amendment) Act, 2006.



(Source: Saravade, ,2007)

Figure 3: Proposed amendments to the Indian IT Act 2000

Government of India's Initiatives

In 1975, during fifth five year plan (1972-77), Govt of India strategically decided to take effective steps for

development of information systems and information resources to overcome 'digital divide'

National Informatics Centre (NIC) created towards this objective has been instrumental in steering information and communication technology (ICT) applications in government departments at centre, states and districts facilitating improvement in government services, wider transparency in government functions and improvements in decentralized planning and management.

In 1999 central government created a new ministry of information technology (MIT) by merging the department of electronics (DOE), national informatics centre (NIC) and electronics and software export promotion council. New Telecom Policy (NTP) announced in same year provided the much needed policy framework. In recognition of the convergence of IT and telecommunication, Department of Telecommunication (DOT) was later merged with MIT to give birth to ministry of communication and IT. Creation of Telecom Regulatory Authority of India (TRAI) in 1997 and Telecom Dispute Settlement and Appellate Tribunal (TDSAT) in 2000 gave regulatory framework to India's fast evolving telecommunication infrastructure.

To customize applications for facilitating decision support in development and responsive administration NIC has established its project centre at National Informatics Centre Network (NICNET) nodes. NIC implements IT projects in collaboration with central and state governments in the area of E-governance. The cyber security of the ICT infrastructure being created for E-governance is responsibility of cyber security group in NIC. However NIC website does not provide any details (NIC, 2008).

STQC under Dept of Information Technology (DIT),Govt of India,(MIT,2008) provides assurance services for Software Quality testing, Information Security and IT Service Management by conducting testing, training, audit and certifications. Based on this concept a Conformity Assessment Framework (CAF) for e-Governance project has also been developed and is in operation.

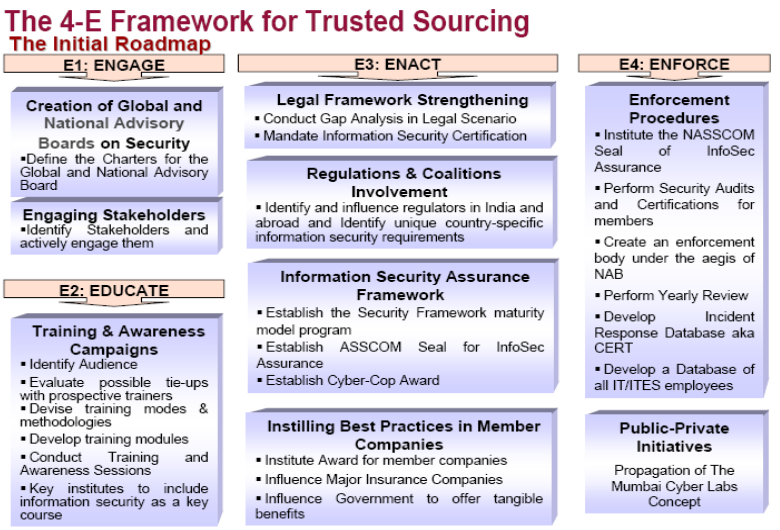
CERT-In functioning under DIT is India's response to cyber threats and has following charter, mission and constituency.

Charter
"The purpose of the CERT-In is, to become the nation's most trusted referral agency of the Indian Community for responding to computer security incidents as and when they occur ; the CERT-In will also assist members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents."

Mission
"To enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration."

Constituency
The CERT-In's constituency is the Indian Cyber-community.

India industry Initiatives
National Association of Software Service Companies (NASSCOM) is a premier trade body and chamber of commerce of the Indian IT and ITES industry. To meet the regulatory requirements of their clients in Europe and USA the member companies have embarked on embracing various International and Industry standards that have mushroomed to act as benchmarking frameworks. NASSCOM has proposed following 4-E framework (figure 4) to meet the trusted sourcing need of Indian IT industry (Saravade, ,2007).



(Source: Saravade, 2007)

Figure 4: NASSCOM proposed 4-E Framework for Trusted Sourcing

According to NASSCOM (Saravade, 2007), Data Security Council of India (DSCI) is being set up to meet IT security concerns in Indian context. DSCI is envisaged as a credible and committed body to uphold a high level of data privacy and security standards. DSCI shall be based on the following five guiding principles:

- Self-Regulation**:** The structure and operating procedures of DSCI rely primarily upon self regulation. Industry, rather than a governmental body, is best positioned to develop appropriate data privacy and security standards based upon its greater knowledge and understanding with the practical commercial issues involved. A self regulatory approach will allow DSCI to evolve and respond more effectively to developments in overseas and domestic markets.
- Adoption of best global practices: DSCI shall adopt the best global practices, drawing upon U.S. laws, the European Union Directive and Safe Harbor Framework, OECD guidelines, and Asia Pacific Economic Cooperation (APEC) Framework in designing the Code of conduct, which in turn, will continue to evolve with time and experience.
- Independent Oversight: The composition of governing body of DSCI shall be balanced with adequate representation of independent directors and industry specialists.
- Focused Mission: Initial focus of DSCI shall be its core mission of establishing itself with significant membership with focus on evolving the Code of Conduct and promoting a culture of privacy and security through education and outreach.
- Enforcement Mechanism: DSCI shall promote and encourage voluntary compliance of the code, but, in due course, will seek to create a mechanism for enforcement of the code to enhance its credibility among a variety of stakeholders.

6. India's ICT Infrastructure

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.

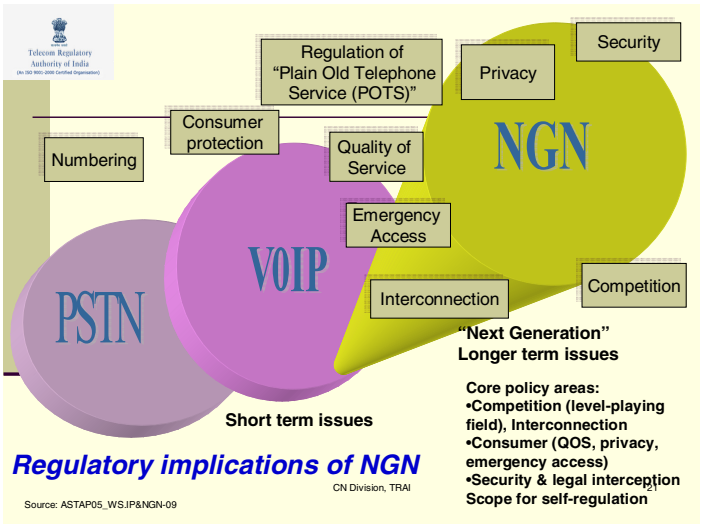


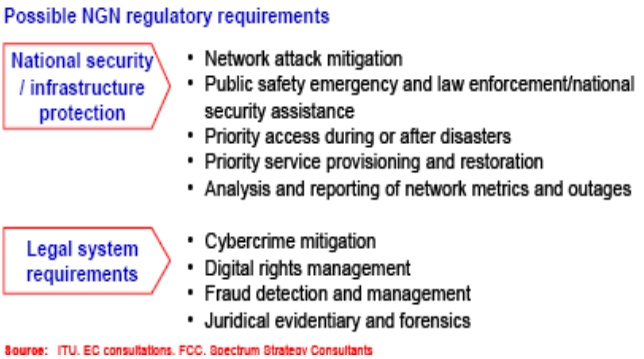
Figure.5: Regulatory issues (Adapted from TRAI Consultation Paper on NGN)

Regulatory issues concerning regulators around the world**:**
The deployment of NGN throws up many regulatory challenges as highlighted in figure 5.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 formal regulatory framework. NGN permits us a window of opportunity to review regulatory framework by proactive consultation process and spirit of accommodation amongst all stakeholders. Regulators in many developing countries including India (TRAI, 2008) have begun process of firming up broad principles for NGN deployment ahead of actual transition.

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 consumer's take-up of IP services and Broadband is at a nascent stage.

Some of the regulatory requirements pertaining to security aspects of NGN are highlighted in figure 6 below.



(Source: TRAI, 2008)

Figure.6: Security aspects of NGN

The recommendation on the security of NGN by expert committee on NGN vide para 3.4.2.2 (page 44 of report on NGN) (TRAI,2008) states:

"NGN-eCO acknowledged that security is of paramount importance to any network. Therefore, TEC may be asked to work on various aspects of security for the country keeping in view the global trends".

7. Imperatives for India's response to Cyber Threats.

If one looks at the challenges India faces in the backdrop of the task of steering our ICT infrastructure on a sustainable and safe trajectory various factors emerge which suggest a synergetic approach. The ICT infrastructure should support diverse social objectives of empowering our rural masses, E–Governance, E-Commerce and disaster warning/relief. The details of India's initiative to secure her cyber infrastructure as available through open source is in stark contrast to the initiatives taken by the USA in the aftermath of attacks in September 2001. While it is true that each country should initiate measures as suitable for its needs and at a pace that is viable in its context, India with her aspiration to be IT superpower in the coming decade can ill afford to lag behind. Various lead agencies in USA to protect her critical Infrastructure as described in 'The national strategy to secure cyber space' document (DHS, 2008) are shown in Figure 7.

The Homeland Security Act of 2002 in USA provides the basis for Department of Homeland Security (DHS) responsibilities in the protection of the Nation's Critical Infrastructure and Key Resources (CI/KR). The act assigns DHS the responsibility to develop a comprehensive national plan for securing CI/KR and for recommending "measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities."

USA has National Infrastructure Protection Plan (NIPP) in place under Department of Homeland Security (DHS,2008) with following goal:

*"Build a safer, more secure, and more resilient America by enhancing protection of the Nation's Critical Infrastructure and Key Resources (CI/KR) to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency***."**

The NIPP provides the unifying structure for the integration of existing and future CI/KR protection efforts into a single national program to achieve this goal. The NIPP framework will enable the prioritization of protection initiatives and investments across sectors to ensure that government and private sector resources are applied where they offer the most benefit for mitigating risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters. The NIPP risk management framework recognizes and builds on existing protective programs and initiatives.

Protection includes actions to mitigate the overall risk to CI/KR assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, this includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety programs, and implementing cyber security measures, among various others.

The White House issued 'The National Strategy to Secure Cyberspace' in February 2003.The Department of Homeland Security (DHS) established the National Cyber Security Division (NCSD) in June 2003 to serve as a national focal point for addressing cyber security issues and to coordinate implementation of the

cyber security strategy in the United States. NCSD's mission is to work collaboratively with public, private, and international entities to secure cyberspace and cyber assets, and to implement the actions and recommendations of 'The National Strategy to Secure Cyberspace'. The organization chart of NCSD is given in figure 8 below.

CRITICAL INFRASTRUCTURE LEAD AGENCIES

LEAD AGENCY	SECTORS
Department of Homeland Security	• Information and Telecommunications • Transportation (aviation, rail, mass transit, waterborne commerce, pipelines, and highways (including trucking and intelligent transportation systems) • Postal and Shipping • Emergency Services • Continuity of Government
Department of the Treasury	• Banking and Finance
Department of Health and Human Services	• Public Health (including prevention, surveillance, laboratory services, and personal health services) • Food (all except for meat and poultry)
Department of Energy	• Energy (electric power, oil and gas production, and storage)
Environmental Protection Agency	• Water • Chemical Industry and Hazardous Materials
Department of Agriculture	• Agriculture • Food (meat and poultry)
Department of Defense	• Defense Industrial Base

(Source : DHS,2008)

Figure 7: Critical Infrastructure Lead Agencies in USA

According to audit report submitted by Office of Inspector General (OIG) U.S. Department of Homeland Security in June 2007, there are still challenges in securing the cyber space in USA (OIG, 2007).While the National Cyber Security Division has made progress in meeting its mission, according to OIG report it can improve its efforts to secure the nation's cyber infrastructure in following areas:

- Establish priorities to ensure that its mission-critical tasks supporting its programs are completed timely.
- Develop enhanced performance measures that can be used to evaluate the effectiveness in meeting its mission.
- Fully develop its information sharing and communications programs with the private sector.
- Develop and implement enhanced procedures to ensure that all known cyber incidents from across the federal government are being reported.
- Ensure that its support systems comply with all 'Federal Information Security Management Act' requirements, including testing of contingency plans.

In Indian context creation of National Disaster Management Authority (NDMA) under an act of parliament was motivated by similar concerns for mitigating and managing national disasters from natural and

manmade causes. Its vision as given on website (NDMA, 2008) states:

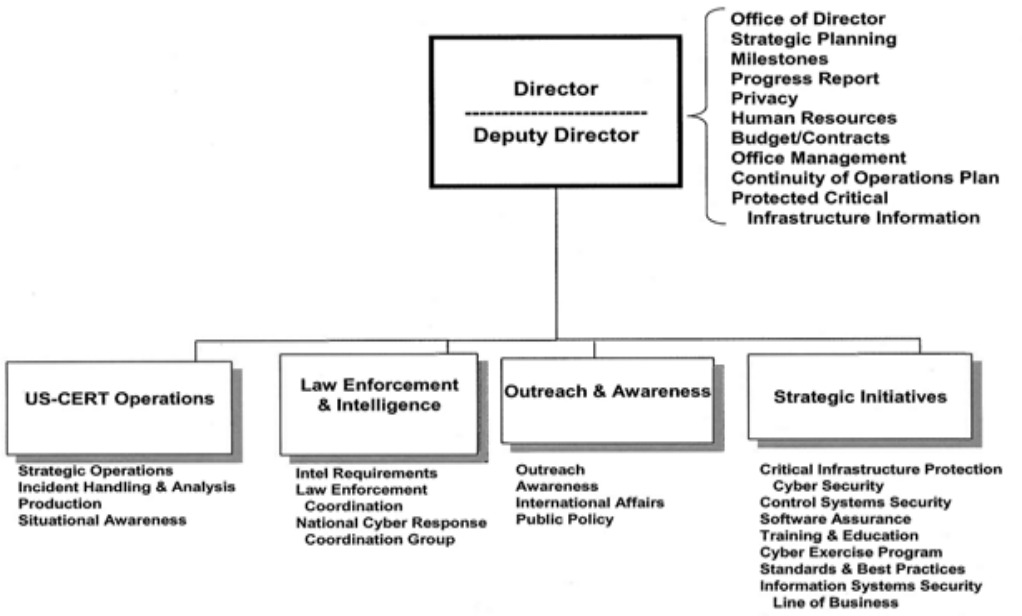


Figure 8: USA's National Cyber Security Division (NCSD) Organization Chart

"To build a safer and disaster resilient India by developing a holistic, pro-active, multi-disaster and technology-driven strategy for disaster management through collective efforts of all Government Agencies and Non-Governmental Organizations"

In order to translate this Vision into policy and plans, the NDMA which appears to be nearest to USA's Department of Homeland Security, has adopted a mission-mode approach involving a number of initiatives with the help of various institutions operating at national, state and local levels. The central ministries, states and other stakeholders have been involved in the participatory and consultative process of evolving policies and guidelines.

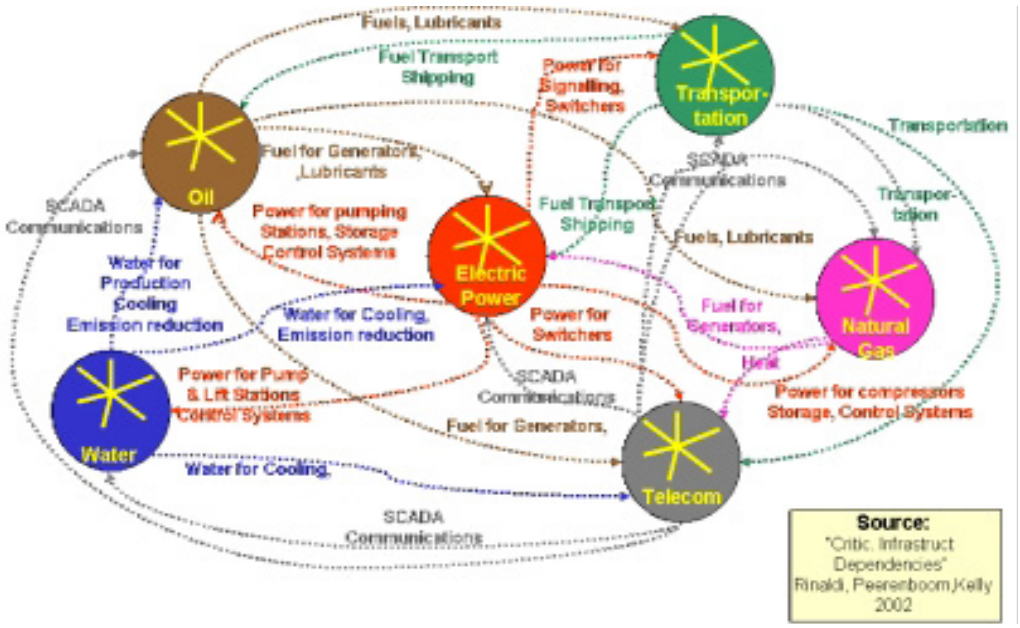
This Policy framework is also in conformity with the International Strategy for Disaster Reduction, the Rio Declaration, the Millennium Development Goals and the Hyogo Framework 2005-2015. The themes underpinning this policy are:

- Community-based disaster management, including last mile integration of the policy, plans and execution.
- Capacity development in all related areas.
- Consolidation of past initiatives and best practices.
- Cooperation with agencies at national, regional and international levels.
- Compliance and coordination to generate a multi-sectoral synergy.
- From the national vision and aforementioned theme, the objectives guiding the policy formulation have evolved to include:
- Promoting a culture of prevention and preparedness – by centre-staging DM as an overriding priority at all levels and at all times.
- Encouraging mitigation measures based on state-of-the-art technology and environmental sustainability.

- Mainstreaming DM concerns into the development planning process.
- Putting in place a streamlined institutional techno-legal framework in order to create and preserve the integrity of an enabling regulatory environment and a compliance regime.
- Developing contemporary forecasting and early warning systems backed by responsive and fail-safe communications and Information Technology (IT) support.
- Promoting a productive partnership with the Media, NGOs and the Corporate Sector in the areas of awareness generation and capacity development.
- Ensuring efficient response and relief with a caring humane approach towards the vulnerable sections of the society.
- Making reconstruction an opportunity to build back better and construct disaster-resilient structures and habitats.

A quick tour of the NDMA's portal gives a feeling that unless NDMA is unwilling to share its plans with public, a lot needs to be done to achieve same coherence as being practiced by most of the developed world with USA being just an illustrative case. There seems to be no division equivalent to the National Cyber Security Division (NCSD) under DHS in USA. NCSD like organization would formalize our steps towards holistic cyber security.

The *transparency of the national system* for the protection of a state's own critical infrastructures is viewed as vitally important. It is essential to the attainment of adequate critical infrastructure protection that proper awareness of the problem is created at all levels of industry, state and society.
The process of securing our critical infrastructures is a daunting task (Schmitz, 2003).As indicated in figure 9 below, the interdependencies of critical infrastructures suggest a holistic approach to address their vulnerabilities.



(Source: Schmitz Walter,2003)
Figure 9: Interdependencies of Critical Infrastructures

The NDMA plans to have a holistic approach to disaster management. Figure 10 from NDMA website

summarizes the concept of Disaster Management Continuum.

(Source : NDMA ,2008)

Figure 10: Disaster Management Continuum

To achieve incremental gains in securing our cyber space open debate between all stakeholders viz government, private industry and common citizen is imperative. As can be seen from experience of USA that it is not a trivial issue and requires very dedicated and structured approach at the highest level in our government. Regular monitoring using an agreed metric for the achievements is need of the hour. The preparatory work undertaken by NDMA towards this objective can be shared with other stakeholders after suitable action to create declassified versions of the reports. What is more important is to have an overall blue print with operational details being shared on 'need to know' basis.

The cyber security effort in Indian context seems to be fragmented and shrouded in mystery .The cyber security measures taken by NIC, NDMA and other government agencies are not available in public domain and , therefore, seem to lack a plausible oversight mechanism at national level. The Indian Industry's effort as coordinated by NASSCOM and Data Security Council of India emphasize " self regulation" and are driven by the need for IT companies to project right image for outsourcing of IT projects from West/USA. As our experience with recent financial meltdown has highlighted that self regulation driven by market forces is not best model to follow.

Prima facie, the sub prime crisis can be attributed to the greed of unchecked expansion by the banking sector of the US economy which was helped to a great extent by the pro-capitalistic policies of the US governments during the past two decades. Many of the regulations that kept the US banking in check were slowly but surely ripped apart, giving rise to a view which promoted that the US financial sector was now too large and complex to be regulated from the outside, what needed was self-regulation. The results are bare open now for all to see (Chandrashekar, 2008). Government oversight and regulation is essential to protect our critical infrastructures against cyber threats

It is recommended that laudable adoption by Indian IT industry of various cyber security standards to survive in international competition should be nurtured by Indian government backed regulatory initiatives. Creation of NDMA under ministry of Home is a very prudent step to achieve synergy in making Indian

critical infrastructures resilient. In today's world compartmentalization is not an option and we need to evolve from this nucleus created by Indian government. Any half measures would be very risky for us when our dream to be an IT super power seems to be within our reach. A system of oversight to audit progress made towards stated objectives and corrective steps is unavoidable.

7. Concluding Remarks

As our investments in ICT infrastructure grow our vulnerability to damage by natural disasters or through attacks by insurgents/terrorists with objective to immobilize and paralyze day-to-day activities of the nation is becoming real. Such damage would cause short and long term setback to economy. We have many lessons from US initiative to secure our cyber system, while planning and implementing India's ICT infrastructure. Natural or insurgency/terrorist induced disaster increases pressure on available ICT systems exponentially to facilitate coordination between various agencies like fire brigade, medical services, police, media and civil administration. It is proposed that the existing and planned ICT infrastructure of the nation, both in public and private domain be analyzed by a group of experts under aegis of NDMA to suggest suitable operational arrangements to minimize their vulnerability to perceived attacks by inimical elements and natural disasters. This would entail rigorous technical analysis of current and emerging wireless and wired ICT systems. The expert group should find and recommend suitable mix of redundancies in the critical ICT systems supporting the governance structure of the nation. The focused analysis of the vulnerabilities and their protection, would lead to recommendations that would avoid duplication of effort and, therefore, economical at national level. The notion that disasters can be completely brought under control by technological and scientific capabilities alone would be too presumptuous. The most sacrosanct component in any such venture is participation from all stakeholders to ensure an appropriate solution for the welfare of humanity

References

1. Bush, George. W. (2002), Executive order on critical infrastructure protection, *Proceedings of the 12th annual conference on Computers, freedom and privacy*. San Francisco, California, ACM.
2. Chandrashekar ,C.P.(2008) ,"In Search of Causes", Frontline, Vol. 2, 25th October-7th November 2008
3. Chaturvedi M.M.,Gupta M.P., Bhattacharya J.(2007),"Analysis of Information and Communication Technology Infrastructure vulnerabilities in Indian context" In J. Bhattacharya(Ed),*Towards next generation E- government*(PP 192-202) India: Gift Publishing.
4. DHS(2008),Department of Homeland Security website, www.dhs.gov/nipp, Retrieved October 7, 2008.
5. DOT(2008), Retrieved August, 2008 from http://www.dot.gov.in
6. Dunn Myriam(2005), "A Comparative Analysis of Cyber security Initiatives Worldwide", Center for Security Studies, Swiss Federal Institute of Technology (ETH Zurich) for the WSIS Thematic Meeting at ITU on Cyber security.
7. Eeten, M.J.G. van, Roe, E.M., Schulman, P , Bruijne, M.L.C. de,(2006), "The Enemy Within: System Complexity and Organizational Surprises", in M. Dunn and V. Mayer (eds), *International CIIP Handbook* 2006. Vol. II: Analyzing Issues, Challenges, and Prospects, Zurich, Center for Security Studies at ETH Zurich, at <www.crn.ethz.ch/publications/crn_team/detail.cfm?id=16157>, pp. 89–109. Retrieved October 7, 2008
8. ITU (2007), Retrieved September 22, 2007 from http://www.itu.int/ITU-D/cyb/events/2007/hanoi
9. ITU/WSIS(2002), World Summit on the Information Society,www.itu.int/wsis/INDEX.HTML retrieved on 05 Oct 2008.
10. Masera M., Wilikens M. (2000), Interdependencies with the information infrastructure: dependability and complexity issues, Research Institute for Systems, Informatics and Safety, Joint Centre, European Commission T.P.210, Ispra (VA), Italy
11. Mayer, Heymans, Matulevičius (2006), "Design of a Modeling Language for Information System Security Risk Management", Technical Report October 2006, Henri Tudor – CITI, 29 Av. John F. Kennedy, L-1855 Luxembourg, Kirchberg
12. MIT(2008),Ministry of Information and Communication Technology, http://mit.gov.in/default.aspx
13. Nain et al (2007), "An Emerging Landscape:Global Initiatives to Secure Cyberspace",Georgia Institute of

Technology,Center for International Strategy, Technology and Policy,Atlanta,Georgia, USA, http://www.cistp.gatech.edu/catalog/
14. NDMA (2008), Retrieved August, 2008 from http://www.ndma.gov.in
15. NIC(2008), Retrieved August 7, 2008 from http://www.dot.gov.in
16. NTP(1999), Retrieved August 7, 2008 from http://www.dot.gov.in
17. OIG(2007),"Challenges Remain in Securing the Nation's Cyber Infrastructure", Office of Inspector General (OIG) Department of home land security, www.dhs.gov/oig.
18. Saravade, Nandkumar,(2007), "Cyber Security Initiatives in India", paper presented at ITU conference at Hanoi in August 2007.Director, Cyber Security and Compliance,NASSCOM.
19. Schmitz Walter(2003),"Modeling and Simulation for Analysis of Critical Infrastructures", Critical Infrastructure Protection (CIP) Workshop (Frankfurt a.M., 29-30 Sept. 2003) - Paper 2.3, Page: 1
20. Srivastava Leena, Samarajiva Rohan , (2001), Regulatory design for disaster preparedness and recovery by infrastructure providers: South Asian experience, Paper presented at Economics of Infrastructures Section, TBM Faculty, TU Delft, Jaffalaan 5, 2628 BX Delft, Netherlands, www.delft2001.tudelft.nl/paper%20files/paper2055.doc
21. TRAI(2008),NGN Report, Retrieved August 7, 2008 from www.trai.gov.in
22. UNGIS (2007,United Nations Global Alliance for ICT and Development." United Nations. 2007 (available online athttp://www.un-gaid.org/, accessed on 5 Oct.2008)
23. WSIS(2006), World Summit on the Information Society, www.itu.int/**wsis**/goldenbook/, retrieved on 05 Oct 2008
24. Yadav,N, Priyadarshini,T (2008)Adequately Protected in India ?The Need For A Separate Legislation , Mainstream, Vol XLVI No 30,16 July 2008.

About the Authors

M M Chaturvedi is an Indian Air Force officer pursuing PhD at IIT Delhi. An alumnus of National Defense College, New Delhi, he has held various appointments dealing with telecommunication policy issues. An engineer by profession his current interests include vulnerability analysis of evolving ICT infrastructure.

M. P. Gupta is Chair-Information Systems Group & Coordinator-Center for Excellence in E-gov at the Department of Management Studies, Indian Institute of Technology (IIT Delhi). His research interests lies in the areas of IS/ IT planning and E-government. Prof.. Gupta has authored acclaimed book "Government Online" and edited two others entitled "Towards E-Government" and "Promise of E-Government", published by McGraw Hill, 2005. His research papers have appeared in National and International Journals/Conference Proceedings. He was the recipient of the prestigious Humanities & Social Sciences (HSS) fellowship of Shastri Indo Canadian Institute, Calgary (Canada) and a Visiting Fellow at the University of Manitoba. He supervised e-government portal "Gram Prabhat" which won the IBM Great Mind Challenge Award for the year 2003. He has steered several seminars and also founded the International Conference on E-governance (ICEG) in 2003 which is running into sixth year. He is on the jury of Computer Society of India (CSI) E-gov Awards and also a member of Program Committee of several International Conferences. He is life member of Global Institute of Flexible Systems Management (GIFT), Systems Society of India (SSI) and Computer Society of India (CSI).

Jaijit Bhattacharya is Country Director, Government Strategy at Sun Microsystems and also an Adjunct Faculty at IIT Delhi. He is responsible for the creation of the next generation of solutions for the governments, based on open standards. Dr. Bhattacharya also advises governments on e-governance strategies. He is an e-Governance advisor to Government of Sri Lanka and has been conducting trainings for ADB institute in Tokyo on Public Expenditure Management as well as helping the World Bank develop curriculum for their e-Leadership program. Dr. Bhattacharya has been involved in developing technologies for e-governance and in implementation of very large systems in over nine countries. He has also developed business models and strategies for leading companies in the IT, media and computer hardware industries. He has numerous research papers to his credit in leading journals and conferences. He is also the editor of the book "Technology in Government" and has also co-authored 'Government On-line – Opportunities and Challenges', published by Tata McGraw Hill which was released by the Honourable President of India, Shri Abdul Kalam. Dr. Bhattacharya did his PhD from Department of Computer Science and Engineering IIT Delhi, prior to which he did his B. Tech in Electrical engineering from Indian Institute of Technology, Kanpur and MBA from Indian Institute of Management, Calcutta. He is a member of IEEE and ACM. He is also a polyglot and speaks French and Bahasa Indonesia besides English, Hindi and Bangla.