Analysis of Information and Communication Technology Infrastructure (ICT) Vulnerabilities in Indian Context

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

ABSTRACT

The paper attempts to highlight the vulnerabilities of India's Information and Communication Technology (ICT) infrastructure to both natural and man made disasters and extrapolates its effect on national security. Using the existing organizational structures, a framework is recommended to facilitate cooperation of all stakeholders to address these vulnerabilities. By providing fail- safe and reliable communication links to all regions of the country, it would be possible to mitigate effects of these disasters by effective and timely relief operations, when needed. This acquired immunity of ICT assets to disasters would support long-term sustainable economic growth of India using twin vehicles of e-governance and e-commerce.

Keywords: Vulnerability of ICT infrastructure, disaster mitigation, economic growth, e-governance, e-commerce.

"The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable"

Sun Tzu Wu

1. Introduction

Computer technology is now deeply embedded in the process of telecommunications, which is best described as digital convergence phenomenon. Various value added services to the plain voice communication have resulted in the emergence of 'info-communication' industry (Yan, Pitt, 2002). Further low cost and reliable communication services have given boost to their widespread use in various walks of life. This has led to emergence of modern societies characterized by ubiquitous ICT infrastructure and our dependence thereon. Chain dependencies are created with consequent risks that need to be managed at national, regional and international levels. At the national level, need for coordinated action for prevention, preparation, response, and recovery from incidents by joint action of government authorities, the private sector and citizens emerges. At the regional and international level, cooperation and coordination amongst countries appears essential using a comprehensive approach. Framework for cyber security and critical information infrastructure protection would entail a national strategy and creation of legal frameworks to curb cyber crime. Regional work shop on frame works for cyber security and critical infrastructure

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

protection held at Hanoi in August 2007 under aegis of International Telecommunication Union (ITU 2007) has highlighted need for national frame works.

In this paper attempt is being made to highlight the vulnerabilities of India's Critical Information Infrastructure (CII) while it races forward to IT enable business and governance processes. By looking at India's problems with creative mind set, a synergetic approach is evolved to address its key concerns.

2. Vulnerabilities of ICT Infrastructure

Developed countries with evolved ICT infrastructure have experienced following vulnerabilities and initiated suitable counter measures.

(a) Prolonged disruption of electrical power during disaster leading to degradation/collapse of Information Infrastructure.
(b) Communication overload during Disaster leading to unacceptable delay or collapse of communication service.
(c) Vulnerable to use of Radio Frequency Weapons (RFW) by terrorists, other disgruntled persons.
(d) Vulnerable to Information Warfare and Cyber Terrorism through electronic media.
(e) Physical Damage by accidental, natural hazards or intentional sabotage.

A failure of the electricity infrastructure of more than a few hours, besides impacting law and order, would degrade critical services such as emergency medical services and the telecom network by depriving them of the needed power. Restoration of the electricity infrastructure, in turn, needs a working telecom system. Cyclone Katrina in USA during September 2005 (Rahman, 2006) and Orissa cyclone in 1999 (Srivasatva, Samarajiva, 2001), brought to light vulnerability of underlying electricity infrastructure to natural disasters and its cascading effect on information infrastructure. Effect of overload on ICT assets during September 11, 2001 attack on twin towers from available reports was alarming (Campen, 2002). Public Switched Network (PSN), cellular telephones, wireless networks and the Internet were not prime targets; still the cascading consequence of collateral damage to communication systems was significant. Vulnerability of ICT to electromagnetic radio frequency (RF) has been an area of concern since inception of these technologies. RF emitters are common in everyday life (TSWG, 2005). They work by sending invisible electromagnetic energy into the air or down a wire. RF emitters are used in a variety of applications, including wireless communication, navigation (e.g., Global Positioning System), radar, etc. Some familiar examples of RF emitters include broadcast radio transmitter towers, cellular phones, two-way radios, microwave ovens, weather radars, police radars, cable television, and local area networks. It is possible for electromagnetic energy from an emitter to adversely affect electronic devices not designed to work with the emitter. This is called Electromagnetic Interference (EMI). Radio frequency weapons (RFW) are created by leveraging this property of electromagnetic waves with suitable amplification of their power.

According to research underway at Technical Support Working Group (TSWG, 2005), Dept of DRDO, USA, RFWs can damage electronics and/or cause them to malfunction, even in ways that compromise built-in, fail-safe mechanisms. The impact of the malfunction depends on what equipment is affected, how it is affected, when it is affected, and what function it is performing. If the affected electronics control critical processes, the impact may be significant, resulting in economic loss, reduced defenses, and infrastructure facility downtime. RFWs transmit electromagnetic energy in one of two ways: Radiation, which is the process of broadcasting a signal through the air using an antenna or Conduction, which is the process of transmitting electrical energy through a wire, such as a power line or a telephone line. In either case, the energy can be transmitted continuously over a long period of time or transmitted in a burst over a short period of time.

The vulnerability of ICT assets of all developed economies to tools of information warfare /cyber terrorism

has been well documented (Gupta, Kumar, Bhattacharya, 2004). Participants in a war game called "Digital Pearl Harbor" sponsored by Gartner and the U.S. Naval War College demonstrated that terrorists could use cyber attacks to hurt the U.S. economy and political will severely (Purchase, Caldwell, 2002).. The players were drawn primarily from Gartner's client base and included people who manage the IT systems that are part of the critical infrastructure, that is, systems that control or operate parts of the electrical power grid, telecommunications, financial services, and networking services and the Internet. The conclusions reached by the participants suggest that vulnerability stems from the vulnerability of software in use and from the availability of information on the Internet that terrorists need. Addressing the terrorist threat requires a comprehensive and collaborative approach. Network security has emerged as a major technology concern in India not just for the government websites but for the corporate sector as well

3. Critical Infrastructures and their Interdependencies

Even though there are differences about the details as to what constitutes the critical infrastructure, there is general agreement among industrialized countries as to its basic elements. Generally critical infrastructure elements include energy, transportation, water supply, information and communication services, emergency services, law enforcement, financial services, health care, food supply and high vulnerability industries as shown in figure 1 (Rahman, 2005). This figure also highlights the infrastructure interdependencies showing physical, cyber, and new economy linkages.

Critical Information Infrastructure

Critical information infrastructure (CII) is a subset of the critical infrastructure. At the same time, CII is a cross-cutting element that permeates all infrastructures and makes communication between them possible. Figure 2 shows how the information infrastructure links banking and finance, natural gas and oil services, transportation, telecommunications, the electric power, water and sewer, and emergency services. The CII is composed of telecommunication infrastructure along with computer networks and the underlying electric power system including backup generation that keeps the system functional (Rahman, 2005).

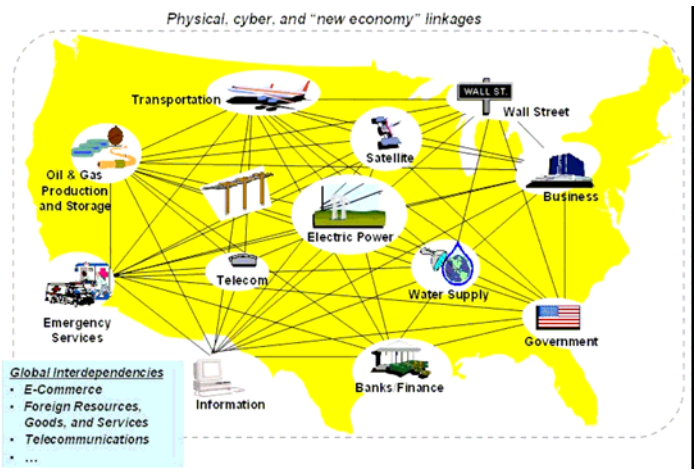

Figure 1: Critical infrastructure interdependencies elements on CII

Figure 2: Dependency of other critical

(Source : Rehman,2005)

High degree of ICT integration has made society increasingly dependent on the underlying infrastructures **(**Luiijf, Klaver, 2000).. The ICT-infrastructure has grown into a complex intertwined and interlinked mass of networks and services involving several distinct layers (see Figure3).

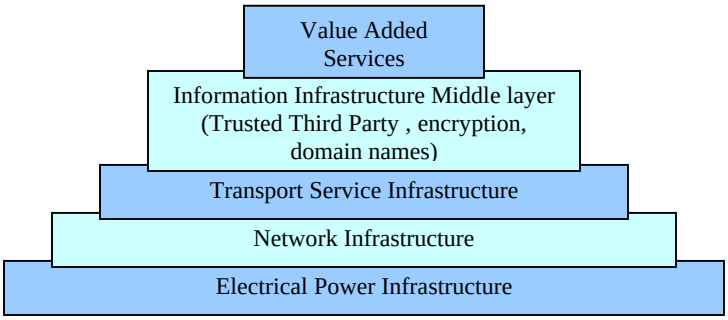

Figure 3: Model of vertically stacked infrastructures *(Source Luiijf, Klaver, 2000)*

4. India's Challenge

Post liberalization, 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 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 telecommunication 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 need for growth of our communication infrastructure, does not specifically address vulnerabilities and action plan. National Disaster Management Authority has highlighted need for reliable and robust communication support for disaster management and expected performance objectives are being firmed up (NDMA, 2007). Objectives enunciated on official web site of India's Department of Telecommunication (DOT, 2002) 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. India has been vulnerable to various natural disasters like earthquakes, floods, cyclones and draughts. Recent trends of terror as preferred weapon by various state and non-state actors has only compounded the challenge. The complexity of the disaster management can be gauged by looking at various blocks of the Figure 4. Survivable ICT infrastructure to support synergetic working of these subsystems is critical.

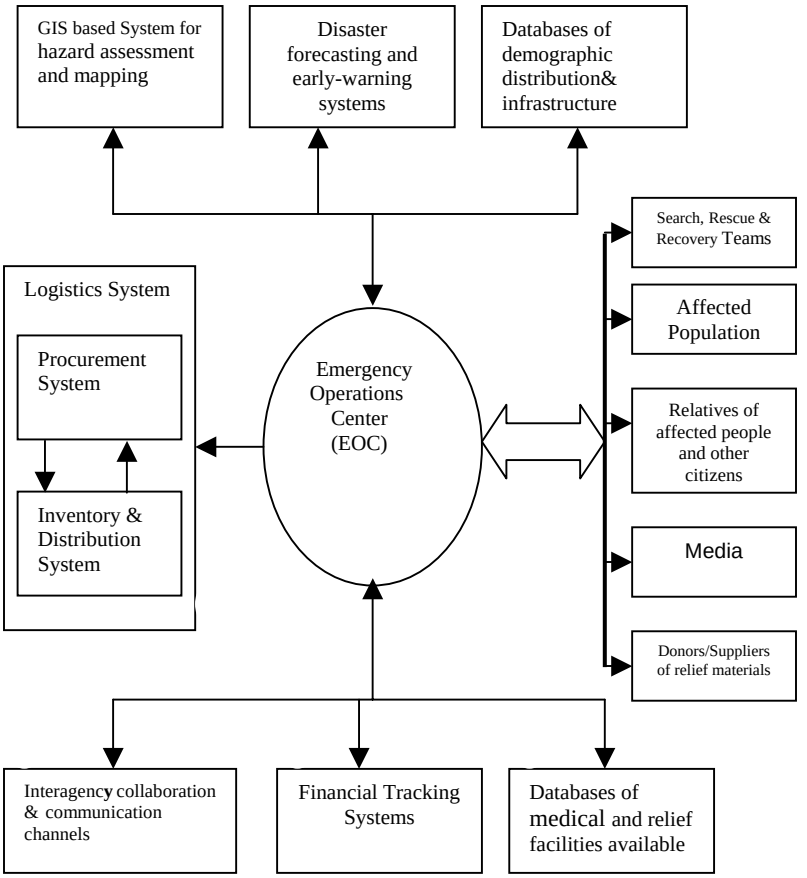

Figure 4: Disaster Management Subsystems *(Source: Gupta, Kumar, Bhattacharya, 2004b)*

The dramatic impact of the Tsunami on the shores of the Indian Ocean demonstrates the crucial importance of effective, all-embracing communication systems. Many people could have saved their lives, if they had received a timely warning, via telephone, email or radio… (Correljé, 2003), Many shores were not flooded until hours after the earth quake took place. In the next stage of disaster management, widespread malfunctioning of networks and connections for fixed and mobile telephone, local radio systems and other communication facilities delayed immediate emergency responses to take-off. Communication infrastructures are heavily dependant on public policy frameworks and economic regulation. A study by Srivastava and Samarajiva (2001) deals with the impact of regulation on the degree of disaster preparedness of network operators and the recovery of the infrastructure after a disaster has hit. Their analysis draws on two case studies, namely, the impact of a cyclone on the power supply system of the Indian state of Orissa and the consequences of bombings on the restructured Sri Lanka telephone system. The study identifies the main issues and suggests a set of solutions in respect of the regulatory design of systems. According to the study disaster management does not appear as a regulatory priority either in telecom or in energy. In regional context, when many countries around the Indian Ocean are confronted with the immediate need to react to similar disasters review of these issues and the conclusions presented may be of immense value to policy makers. Need for a regulatory framework that provides incentives to achieve the desired robustness of the system at reasonable cost, without infringing on the managerial autonomy of the operators is most essential in the liberalized systems.

Disaster preparedness should be part of the license conditions of service providers. Long-term regulatory framework for disaster mitigation and management should highlight risk before new investors enter the market, so that incentives are properly aligned. The investor has to bear some part of the costs of recovery, to act as incentive to build and maintain robust systems. Government, consumers of the service and the general population has an interest in prompt restoration of vital services, therefore it is also reasonable to allocate part of the risk to these stakeholders. Government should inform potential investors of its expectations, including specified levels of disaster preparedness and recovery capabilities.

5. Looking for a model

Government Emergency Telecommunications Service (NCS, 2007) functioning in USA under National Communication System (NCS) can provide a conceptual model while evolving India's emergency telecommunication and IT infrastructure.

The Government Emergency Telecommunication System Concept

The Government Emergency Telecommunications Service (GETS) is a White House-directed emergency phone service provided by the National Communications System (NCS) in the Cyber Security & Communications Division, National Protection and Programs of the Department of Homeland Security. GETS supports federal, state, local, and tribal government, industry, and non-governmental organization (NGO) personnel, in performing their National Security and Emergency Preparedness (NS/EP) missions. GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN). It is intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased.

GETS Eligibility Criteria

There are five broad categories that serve as guidelines for determining who may qualify as a potential GETS user. These users may be in federal, state, local, or tribal government, critical infrastructure sectors in industry, or non-profit organizations that perform critical National Security and Emergency Preparedness (NS/EP) functions. Typical GETS users are responsible for the command and control functions critical to management of and response to national security and emergency situations, particularly during the first 24 to 72 hours following an event.

i) *National Security Leadership*

This user performs NS/EP functions essential to national survival when nuclear attacks threatens or occurs. In addition, this user provides support to critical order wire and control services necessary to ensure the rapid and efficient provisioning or restoration of other NS/EP services. These user functions may include the following:

- Critical order wire or control service supporting other NS/EP functions
- Presidential support critical to continuity of Government and national security leadership.
- National Command Authority support for military command and control critical to national survival.
- Intelligence critical to warning of potentially catastrophic attack
- Support for the conduct of diplomatic negotiations critical to arresting or limiting hostilities.

ii) *National Security Posture and US Population Attack Warning*

This user type performs additional NS/EP functions essential to maintaining an optimum defense, diplomatic, or continuity of government posture before, during, and after crisis situations. Such situations are those ranging from national emergencies to international crises, including nuclear attack. These user functions may include the following:

- Threat assessment and attack warning
- Conduct of diplomacy
- Collection, processing, and dissemination of intelligence
- Command and control of military forces
- Military mobilization
- Continuity of Federal Government before, during, and after crisis situations
- Continuity of state and local government functions supporting the Federal Government during and after national emergencies
- Recovery of critical national functions after crisis situations
- National space operations

iii) *Public Health, Safety, and Maintenance of Law and Order*
The user type performs NS/EP functions necessary for giving civil alert to the US population by maintaining law and order and the health and safety of the US population in times of national, regional, or serious local emergency. These user functions may include the following:

- Population warning (other than attack warning)
- Law enforcement
- Continuity of critical state and local government functions (other than support of the Federal Government during and after national emergencies)
- Hospitals and distribution of medical supplies
- Critical logistic functions and public utility services
- Civil air traffic control
- Military assistance to civil authorities
- Defense and protection of critical industrial facilities
- Critical weather services
- Transportation to accomplish foregoing NS/EP functions

iv) *Public Welfare and Maintenance of National Economic Posture*
This user type performs NS/EP functions necessary for maintaining the public welfare and national economic posture during any national or regional emergency. These user functions may include the following:

- Distribution of food and other essential supplies
- Maintenance of national monetary, credit, and financial systems
- Maintenance of price, wage, rent, and salary stabilization, and consumer rationing programs
- Control of production and distribution of strategic materials and energy supplies
- Prevention and control of environmental hazards or damage
- Transportation to accomplish the foregoing NS/EP functions

v) *Disaster Recovery*
This user type performs NS/EP functions of managing a variety of recovery operations after the initial response has been accomplished. These user functions may include the following:

- Managing medical resources such as supplies, personnel, or patients in medical facilities
- Other activities such as coordination to establish and stock shelters, to obtain detailed damage assessments, or to support key disaster field office personnel may be included.
- Examples of those eligible include:
  - Medical recovery operations leadership
  - Detailed damage assessment leadership
  - Disaster shelter coordination and management

- Critical Disaster Field Office support personnel

6. Analyzing the vulnerabilities of India's ICT Infrastructure

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 communication network should support diverse social objectives of empowering our rural masses, E-Governance, E-Commerce and disaster warning/relief. Vulnerabilities of India's Information and Communication Technology (ICT) infrastructure are analyzed as below:

Prevailing situation	Main Players	Processes involved
• Our Communication infrastructure is the substrate on which new economy is to grow in coming years. • This communication infrastructure lacks survivability features against known threats. • Our communication infrastructure is still to evolve and we can take advantage of 'last mover' to learn from the experience of other developed countries. • Our need to minimize 'digital divide' can be aligned with compulsion to provide telecommunication infrastructure for national disaster mitigation. • Telecom Regulatory Authority (TRAI) can act as facilitator and regulator for creation of infrastructure that can survive or degrade gracefully in the event of full spectrum of anticipated emergency situations. • National Disaster Management Authority (NDMA) under of Ministry of Home Affairs is responsible to coordinate disaster management at national level. • The stakeholders both Government and commercial establishment can share the cost of adding survivability features after TRAI mediated consensus. • India, with a large base of educated, underemployed/unemployed youth, can effectively tap the possibility of increasing share in emerging BPO/KPO segments using substrate of a robust communication infrastructure. • The size of the infrastructure that needs to be put in place offers a very lucrative market for indigenous industry to invest in. FDI with suitable safeguards and partnership with Indian origin business houses would provide large initial investments.	• Indian Government. • Emergency Services under NDMA coordinated perations centers at State/District /Taluk levels • Military and Para Military Organizations • ITU-T at international level • Department of Telecommunication. • TRAI as Indian telecom regulator • Telecommunication service providers both incumbent BSNL/MTNL and private service providers. • Electrical Power Sector Regulator • Electrical Power Sector Service Providers • Banking and Finance including critical E-Commerce functions. • Gas and Oil Sector • Transportation Sector • Water Supply Systems • Telecom Equipment manufacturers • Existing & potential Corporate and Individual Telecommunication subscribers. • Human Resource Development ministry	• Consultation at International and national level to facilitate consensus and creation of right environment to encourage investment for steering our ICT infrastructure on a sustainable and safe trajectory. • Indian government is working towards ' Bharat Nirman' with aim to reduce digital divide to 5:1 by 2015 from current 25:1. Various incentives and subsidies from Universal Service Obligation (USO) funds being used. The USO fund could be innovatively used to support investments towards increasing survivability of Communication and Electricity infrastructure. • Consultation process at international and national level for migration to Next Generation Networks (NGN) is on the anvil. Suitable survivability features can be incorporated while firming up specifications. • Semiconductor policy announced in June 2007 to facilitate foreign investments in telecom manufacturing sector to leverage the telecom boom and liberalized economic environment of India.

Lessons Derived

- International and national policy for survivable communication and electricity infrastructure needs to be articulated.
- Regulatory Framework yet to be articulated which would lead to fair competition and spur investments towards survivability of critical infrastructure.
- Rural areas penetration of telecommunication far from satisfactory. 'Digital Divide' needs to be reduced and empowerment of rural India using telecom as part of 'Bharat Nirman' initiative needs thrust.
- Telecom equipment manufacturing sector very nascent and investments in R&D to absorb and innovate in emerging telecom technology very minimal. The industry has to gear up for indigenous equipments with survivability features.

Suggestions

- National Disaster Management Authority (NDMA) under of Ministry of Home Affairs could coordinate creation of the qualitative requirements (QRs) of the communication and IT support system and update the QRs at periodic intervals to ensure that resilience of the network to future threats is maintained. Such an exercise should have participation from representatives from all stake holders, relevant R& D organizations and academia to generate a comprehensive blue print.
- The US approach to support ' National Security and Emergency Preparedness' function is based on providing GETS which is exclusive and in addition to other communication infrastructure in use by government, business and common men. Though it uses segments of the national communication infrastructure it is purported to have higher reliability, survivability and overload avoidance features by incorporation of 'priority access' features. We would do well to have a slightly different approach. As we have advantage of 'last mover' with very minimal investments in legacy networks compared to developed countries, we should invest in survivability features by providing redundancy, radiation hardening and physical protection for all new communication infrastructure being created.
- Emergency telecommunication and IT system for disaster management being evolved under aegis of National Disaster Management Authority (NDMA, 2007) should follow after suitable adaptation the USA's GETS model. Operational details of classified nature may be obtained by interfacing at appropriate level of government.
- This infrastructure under operational control of NDMA, should be used for socially relevant roles like e-governance, distance education and information/ disaster warning dissemination to village level in absence of actual disaster situation. This would ensure cost effective utilization of nation's investment and ensure training of users at village level. Long term disuse by reserving it for only disaster warning and coordination can lead to poor maintenance and availability in hour of need.
- Telecom Regulatory Authority of India (TRAI) being the nodal agency to regulate the telecom infrastructure growth in our country may be considered by Indian government to evolve fund sharing norms between Government and commercial users of this network.
- The network should evolve in phases. However, the over all blue print should be in place after necessary consultation and brainstorming process. The operational availability and maintenance of this network is recommended to be the responsibility of NDMA as this is a nodal organization for disaster management.
- While foreign investments to tap the emerging market would certainly flow, it is imperative that Indian business houses move across the value chain by investing through joint ventures in hardware and software segments of this Industry, besides the Service Providers role presently being played by them.
- A more holistic view and initiative at Government level is necessary to invest in survivability features by providing redundancy, radiation hardening and physical protection for all new

communication infrastructures being evolved. A public private partnership to synergize the resources is called for.

Expected Performance

- Development of sustainable competitive advantage through core competence building in the telecom sector.
- Spread of telecom to rural India would facilitate economic growth and reach of education by e- governance and e-education respectively.
- The fair competition in the regulated environment would lead to investments both in manufacturing and service provision. This would create innovative telecom services to subscribers both corporate and individual. E-commerce would give fillip to our economy.
- Dependence on imported technology would reduce and our trade balance would become healthy.
- The next generation networks using best technical practices would provide more reliable communication which is a must for our disaster mitigation and management efforts.

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 provide emergency telecommunication and IT system, while planning and implementing India's ICT infrastructure. Natural or insurgency/terrorist induced disaster increases pressure on available telecommunication 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 telecommunication 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 communication systems. The expert group should find and recommend suitable mix of redundancies in the critical communication networks 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. It should rather be the right synergy of People, Process and Technology that should spearhead the metamorphosis from the "taken-for-a-ride by disasters" community to a well-prepared disaster resistant one. The establishment of Emergency Operation Centers and their charted-out implementations by the respective governments and concerned agencies worldwide can be considered as a stepping stone to success in combating the deadly disasters and their after effects that continue to haunt generations to come. 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. Campen Alan. D. (2002), paper on 'Information Assurance' Retrieved August, 2002 from http://www.infowar.com.
2. Correljé Aad (2003), The Missing Link: Review of regulatory design for disaster preparedness and recovery by infrastructure providers: South Asian Experience by L. Srivastava, R. Samarajiva, in: *Critical infrastructures: State of the art in research and application*, eds. W. A. H. Thissen & P. M. Herder, pp. 103-120. Boston: Kluwer Academic Publishers, 2003. Section Economics of Infrastructure, Faculty Technology, Policy and Management, Delft University of Technology, Postbus 5015, 2600 GA Delft, NL
3. DOT (2007), Retrieved August, 2007 from http://www.dot.gov.in
4. Purchase Eric , Caldwell French,(2002), Digital pearl harbor: a case study in industry vulnerability to cyber attack, http://www.gartner.com/2_events/audioconferences/dph/dph.html

5. Gupta, M.P., Kumar, P., & Bhattacharya, J,(2004a), *Government online: Opportunities and Challenges*, TMH, New Delhi.,421
6. Gupta, M.P., Kumar, P.,& Bhattacharya, J,(2004b), *Government online: Opportunities and Challenges*, TMH, New Delhi.,532
7. Luiijf. H.A.M. , . Klaver, M.H.A (Mrs),(2000), ISSUE PAPER, IN BITS AND PIECES ,Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society, Retrieved September 22, 2007 from http://www.iwar.org.uk/cip/resources/tno/cip-netherlands.pdf
8. NCS (2007), Retrieved May 19, 2007 from http://www.ncs.org
9. NDMA (2007), Retrieved August 7, 2007 from http://www.ndma.gov.in
10. NTP (1999), Retrieved August 7, 2007 from http://www.dot.gov.in
11. TSWG (2005) ,Retrieved August 20, 2007 from http://www. Tswg.org
12. Rahman, Saifur (2006), ICT-Integrated Energy Infrastructure, 4th EAPC/PfP Workshop on Critical Infrastructure Protection & Civil Emergency Planning: Building Bridges Between Stakeholders to Mitigate Disasters,Zurich, Switzerland,24-26 August 2006, www.ari.vt.edu
13. 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
14. Sushil, (2001) *Global Journal of Flexible Systems Management* 2001,Vol 2,1,pp51-55
15. Xu Yan,D.Pitt,(2002),*Chinese Telecommunication Policy*, Artech House, Boston & London,1

About The Authors

MM 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.