

**CRITICAL ISSUES IN ENGINEERING THE NATIONAL
INFORMATION INFRASTRUCTURE - BUILDING
INFORMATION WARFARE CAPABILITY**

THESIS

Submitted in partial fulfillment
of the requirements for the degree of
DOCTOR OF PHILOSOPHY

By

PREM CHAND

Under the Supervision of

Dr. Mukul Sinha

**BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE
PILANI (RAJASTHAN) INDIA
2003**

DEDICATION

This thesis is dedicated to my family - my parents, wife and children. Firstly to both my parents, who would be so happy at seeing me submit a Ph.D. thesis at the age of 55, despite job pressures of a Corporate Head. The sense of caring, values and hard work of my parents continue to inspire our entire family. To my wife and children who will hopefully live in a cyber world where peace and tranquility will be so omnipresent that one would not even have to talk about the Information Warfare - it would be a given, not a pleasant hope as it is today.

ACKNOWLEDGEMENT

Working towards my Ph.D. and producing this thesis has been a very enjoyable experience for me. While evolving Navy's Information Warfare strategy, the thought of scaling up the program to national dimensions always engaged my mind. However the state of Information and Communication Technology (ICT) penetration in the country, the constraints of inter-agency dialogue on security sensitive subjects and the pressures of time bound project schedules kept me confined to the Armed Forces. It was my friends of long time and gurus in software areas like Dr. Raja Ram and Dr. Mukul Sinha who saw potential in my work and prodded me to look beyond the Armed Forces. Their guidance led me to join Ph.D. at BITS at 50th year of my age. Later as member of the National Task Force on IT and Software Development, I saw real value in their advice and looked at e-Security in the national and global context. When I nearly completed my thesis addressing concerns of the National Information Infrastructure (NII), in particular the NII security, the same very gurus virtually reset the clock, by asking me to leave classical NII security to its owners and operators and the market forces. They insisted that, I should concentrate on the military dimension of the Information Warfare involving EMP and RF energy weapons with deterrence potential near equivalent to nuclear capability. I realized the wisdom in their concern for national interest and reworked on the thesis.

The Navy gave me an excellent environment to develop my research bearings. My 14 years at WESEE enabled me to foresee, prospect, plan, think and research many areas of Information Warfare, and consolidate them into a 10 volume document titled "Program Complexities of India's Information Infrastructure Security and Information Warfare Program for the Year 2000 and Beyond". I must thank the Navy for this opportunity. This work helped me tremendously to create the world class Information Assurance Framework and Methodologies for getting new insights and applying academic rigor to the problems faced by the ICT community. It also gave me an opportunity to examine threats and vulnerabilities of the emerging cyber space, which have direct bearing on our survival and sustenance in social, economic, political and military terms in the foreseeable future.

Who does one thank for this thesis work? I think that the Ph.D. process itself at BITS Pilani has to be thanked for this. It provides an excellent opportunity for students to bring about industry insights to academic work and the vice versa. The cheerful and positive attitude of Dean, RCD and DAC members puts an external student immediately at ease. I wish to express my sincere thanks to Prof Ravi Prakash, Prof. Rahul Banerjee, Prof. S Balasubramanian, Prof. Sanjay Shrivastava, Dr. Sanjay Pohekar and the office staff lead by Sh. Raghubir Singh for their guidance and help.

The concept of Guru has been central to our culture all through the ages. In Dr. Mukul Sinha, I found that concept truly realized. I was indeed fortunate to have him as my Guru. Not only did he inspire me to do my Ph.D. at a time when my focus was to build my corporate image, he was always at my side to guide me, exhort me, even scold me, to ensure that I did not falter in my

academic pursuits. I remember with fondness the innumerable brain storming sessions that I used to have with him and how he used to bring focus and clarity to the problems we were faced with. He always said that a Ph.D. has to be earned, not merely received. I hope I have not belied his expectations. I cannot thank him enough for all that he has done for me.

I worked with several organizations helping some of them to evolve security overlay for their information infrastructure including ISO 17799 compliance for Information Security Management System (ISMS). Their support and co-operation helped me in my research. I would especially like to thank the senior management and CIO's of the following corporates for this: MBT Mumbai, M&M Mumbai, VeriSign, USA, BT, UK, GSIT, Indore and MCTE, MHOW. There are many other agencies, which I have not listed but which have been very helpful during my research.

I would also like to thank my friends at KPMG - Parag Deodhar, Microsoft - Homi Bardha, Deloitte & Touche: Shashikant Shirhatti, ICICI - Haridas Raigaga, MBT - John Helleur, Kiran Deshpande, Avinash Marthe, Andy Ranveera, Lucius Lobo, Chetan Varde, Mahesh Joshi and Rahul Agarwal & Ranjeet., WESEE - Arun Saxena, Anurag Dave and Kinhuk De, DRDO - K. Santhanam, MCIT- B. K. Gairola, IITK - Maninder Agarwal, MCTE - RL Magotra and M G Datar. Avinash Marthe has specially inspired and encouraged me. Many of the thoughts expressed in this thesis are the result of a common understanding that we came to as a result of discussions with them.

The Internet has indeed revolutionalised exchange and sharing of information across the globe. I have benefited immensely from it. I wish to thank the entire research community whose papers have benefited me, without in anyway staking claim or credit for any of such work in the thesis. At individual level Carlo Kopp's work has been very inspiring. At Organisation level my gratitude goes to US agencies engaged with IT and IW.

My heartfelt thanks to Gurpreet, Ranjeet, Rahul, Akhilesh and Harsh who provided excellent support in producing this thesis. It was they who had to bear the burnt of my disorderly ways and decipher my scribbles written on bumpy flights back to Delhi (from wherever). They relieved me of the burden of the "production aspects" of the thesis.

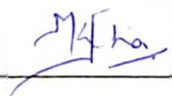
On the personal front, this thesis would not have been possible without the continued encouragement and support that I received from my entire family. Special thanks to my children, daughter Neeti and her husband Sunil, son Anirudh and daughter Srishti who have been such a beneficial influence in my life, and to my wife Kirti who kept me always focused on the task ahead ever since we came together and has been the lynch-pin of my professional and personal life. Her support (and hot cups of tea) was invaluable throughout my Ph. D work.

CERTIFICATE

This is to certify that the thesis entitled CRITICAL ISSUES IN ENGINEERING THE NATIONAL INFORMATION INFRASTRUCTURE – BUILDING INFORMATION WARFARE CAPABILITY and submitted by PREM CHAND ID.No. 1997 PHXF 403

For award of Ph.D. Degree of the Institute, embodies original work done by him under my supervision.

Signature in full of
The Supervisor



Name in capital block
Letters

DR. MUKUL SINHA

Date May 19, 2003

Designation

MANAGING DIRECTOR
Expert Software Consultants Ltd

ABBREVIATIONS

ACTS	Advanced Communication Technologies
ADO	Air Defence Operation
ADP	Automatic Data Processing
AFRL	Air Force Research Laboratory
AHFID	Allied High Frequency Interoperability Directory.
AICTE	All India Council of Technical Education
AIS	Automated Information System
ALH	Advanced Light Helicopter
ARDA	Accelerator Research Department A
ASMD	Air Surveillance for Missile Defence
ASP	Air Craft Self Protection
ATM	Asynchronous Transfer Mode
AWACS	Airborne Warning and Control Systems
B-IDSN	Broadband - Integrated Service Digital Network
BITS	Birla Institute of Technology & Science
C 2	Command & Control
C2W	Command-and-control warfare.
C4	Command, Control, Communications, and computers.
C4I	Command, control, Communications, Computers, and Intelligence
C⁴ISR	Computerized Command Control Communications Surveillance and Recommence
CDACT	Center for Advanced Computing Technologies
CEC	Cooperation Engagement Capability

CERT	Computer Emergency Response Team
CFO	Cross - Field Oscillator
CII	Corporate Infrastructure Protection
CIP	Critical Infrastructure Protection
CNI	Critical National Infrastructure
CNII	Critical National Information Infrastructure
COMSEC	Communications Security
COTS	Commercial off-The-Shelf
CSWS	Cylindrical Shock Wave Source
CVCM	Counter Virus Counter Measure
Cyberwar	A Synonym for Information Warfare.
DAE	Department of Atomic Energy
DARPA	Defense Advanced Research Project Agency
DBK	Dominant Battlefield Knowledge
DD	Dumpster Diving
DDA	Data Driven Attack
DES	Data Encryption Standard
DEW	Directed Energy Weapons
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure.
DISA	Defense Information Security Administration
DISN	Defense Information Systems Network
DNS	Domain Name Service
DoD	Department of Defense
DRDO	Defence Research and Development Organisation

DSWA	Defense Special Weapons Agency
ECO	Electronic Combat Operations
EDI	Electronic Data Interchange
EKMS	Electronic Key Management System
ELINT	Electronic intelligence
ELS	Emitter Locator Systems
EMEC	Emissions Security.
EMGF	Explosive Magnetic Generator of Frequency
EMI	Electromagnetic interference.
EMP	Electro Magnetic Pulse
EPS	Electronic Protection System
ERNET	Educational Research Network
ESD	Electro Static Discharge
ESPRIT	European Strategic Program for R&D in Information Technology
EW	Electronic Warfare.
FCC	Federal Communication Commission
FCG	Flux Compression Generators
FDI	Foreign Direct Investment
FMGF	Ferromagnetic Generator of Frequency
FSU	Former Soviet Union
GCCS	Global Command and Control System
GCSS	Global Combat Support
GHz	Gigahertz
GIE	Global Information Environment.
GII	Global Information Infrastructure

GPS	Global Positioning System
GW	Gigawatt
HEMP	High Altitude EMP
HERF	High Energy Radio Frequency
HPM	High Power Microwave
HPM-D	High Power Microwave Device
HTML	Hyper Text Markup Language
HTTP	Hyper Texts Transfer Protocol
IBM	International Business Machines
IBO	Information Based Operations
IBW	Intelligence Based Warfare
ICAO	International Civil Aviation Organization
ICT	Information and Communication Technology
IDA	Information Decision Action
IGMDP	Integrated Guided Missile Development Program
IIT	Indian Institute of Technology
IMGF	Implosive Magnetic Generator of Frequency
INFOSEC	Information Security
IPMO	INFOSEC Program Management Office.
IPR	Intellectual Property Rights
ISAE	Information Assurance Support Environment.
ISR	Intelligence Surveillance Reconnaissance
ISRO	Indian Space Research Organization
ISSO	Information Systems Security Organization.

ISTC	International Science and Technology Center
ISW	Information System Warfare
IVIS	Inter-Vehicular Information Systems
IW	Information Warfare
IW-D	Information Warfare-Defense
JEC	Joint Economic Committee
JLF	Joint Live Fire
KV	Kilovolt
LCA	Light Combat Aircraft
LII	Local Information Infrastructure
MBT	Main Battle Tank
MCG	Magneto Cumulative Generator
MCIT	Ministry of Communication and Information Technology
MEMS	Micro Electro Mechanical Systems
MHDFG	Magneto hydrodynamic Generator of Frequency
MHRD	Ministry of Human Resource Development
MHz	Megahertz
MILO	Magnetically Insulated Linear Oscillator
MURI	Multi University Research Initiative
MW	Megawatt
NCST	National Center for Software Technology
NIAP	National Information Assurance Program
NII	National Information Infrastructure
NIITF	National Information Infrastructure Task Force
NIPC	National Infrastructure Protection Center.

N-ISDN	Narrowband - Integrated Service Digital Network
NISER	National Institute for Advances in Educational Research
NNEMP	Non-Nuclear EMP
NRO	National Reconnaissance Office.
NSA	National Security Agency.
NSSRM	National Security Space Road Map
NSTL	Naval Scientific and Technological Laboratory
OLB	Operations in Land Battle
OODA	Observe - Orient - Decide - Act
OOTW	Operations Other Than War.
OSI	Open Systems Interconnection
PCCIP	President's Commission on Critical Infrastructure Protection
PEGF	Piezoelectric Generator of Frequency
PGM	Precision Guided Munitions
PHREAKING	"Hacking" the public phone network.
PIC	Particle-in-Cell
PII	Personal Information Infrastructure
PKI	Public Key Infrastructure
PSYOPS	Psychological Operations
PTN	Public Telecommunications Network
RACE	R&D in Advanced Communications Engineering
RD&D	Research Design & Development
REC	Radio Electronic Combat
RF	Radio Frequency
RFM	Radio Frequency Munitions

RMA	Revolution in Military Affairs.
RSTA	Reconnaissance, Surveillance and Target Acquisition
SAAO	Strategic Air Attack Operations
SAM	Surface to Air Missile
SCRBG	Super Conducting Ring Burst Generator
SCSI	Commercial Satellite Communications Initiative
SEAD	Suppression of Enemy Air Defence
SFMFSW	Super Conductive Former of Magnetic Field Shock Wave
SIGINT	The interception and analysis of electromagnetic signals
SMEs	Small and Medium Enterprises
SONET	Synchronous Optical Network
STCU	Science & Technology Center Ukraine
STPI	Software Technology Parks of India
STQC	Software Technology Quality Control
TCP / IP	Transport Control Protocol / Internet Protocol
TED	Transient Electromagnetic Detection
TOC	Tactical Operations Center
TWC	Information Warfare Center
TWEM	Transient Wave Electromagnetic Source
UAV	Unmanned Aerial Vehicles
UWB	Ultra Wide Band
WESSEE	Weapons and Electronics System Engineering Establishment.
WMED	Weapons of Mass Electrical Destruction

Table of Contents

PART- I UNDERSTANDING THE CRITICAL ISSUES	1
1 CHAPTER 1 RESEARCH OVERVIEW & LITERATURE SURVEY.....	2
1.1 Introduction	2
1.2 National Information Infrastructure Perspective.....	2
1.3 Security Threats to NII.....	4
1.4 Information Warfare Threat to NII.....	5
1.5 Formulation of Research Problem.....	8
1.6 Research Methodology & Approach.....	9
1.7 Literature Survey.....	18
1.8 Developing EM Weapons Capability: Justification for Research.....	20
1.9 Research Objectives & My Contribution	21
1.10 Structure of the Thesis Document.....	26
1.11 Conclusion.....	28
2 CHAPTER 2: NATIONAL INFORMATION INFRASTRUCTURE PERSPECTIVE .	30
2.1 Introduction	30
2.2 India's IT Vision - 2010: Action Plan	30
2.3 National IT Objectives	31
2.4 NII Perspective.....	33
2.5 The Promise of the NII.....	34
2.6 Building Blocks of NII.....	34
2.7 Global NII Initiatives	36
2.8 India's NII Initiatives	38
2.9 Critical Issues in Design and Development of the NII.....	42
2.10 Change Management Through Collaboration.....	46
2.11 Conclusion.....	47
3 CHAPTER 3 NII SECURITY PERSPECTIVE AND ISSUES	48
3.1 Introduction	48
3.2 Security of Information Operations.....	48
3.3 National Information Infrastructure and its Security	49
3.4 The Global Information Infrastructure (GII) and its Security.....	50
3.5 Role of NII in Critical National Foundations.....	52
3.6 Threats and Vulnerabilities of NII	53
3.7 Information Component – The Critical Common Threads	54
3.8 Interdependencies Cause Serious National Security Risks	55
3.9 The Changing Nature of Critical Infrastructure Protection.....	56
3.10 Survey of Critical Infrastructure Protection Initiatives Across the Globe	60
3.11 Infrastructure Assurance Issues.....	67
3.12 NII Architecture from Security Point of View.....	68
3.13 Volume and Complexity of NII & GII Security	69
3.14 Security Overlay for NII	70
3.15 Conclusion.....	72
PART- II INFORMATION WARFARE AND EMERGING SERIOUS THREAT TO NII.....	74
4 CHAPTER 4 INFORMATION AGE WARFARE.....	75
4.1 Introduction	75
4.2 Information Warfare Perception.....	75

4.3	Evolution of IT Based Warfare	76
4.4	Information Based operations (IBO).....	78
4.5	Impact of IT on Warfare.....	84
4.6	Analysis of the - Cyber Warfare, Netwar and Information Warfare Paradigms.....	92
4.7	Role of IT in IW	97
4.8	IW Survivability.....	99
4.9	IW Risk Management Strategies.....	100
4.10	Conclusion.....	102
5	CHAPTER 5 INFORMATION WARFARE THREAT ASSESSMENT.....	104
5.1	Introduction	104
5.2	Impact of ICT Penetration: Emerging Cyber Environment	104
5.3	Impact of IW in the Emerging Cyber Environment.....	105
5.4	IW Threat Scenario	107
5.5	Source and Diversity of IW Threats.....	107
5.6	Analysis and Perception of IW Attacks	108
5.7	Impact of IW Attacks	109
5.8	China and Russia's Electromagnetic Weapons	113
5.9	Survey of IW Capability of Different Nations.....	114
5.10	Different Perspectives & Views of IW	115
5.11	Systems Vulnerable to IW.....	116
5.12	Range of Threats & Vulnerabilities	117
5.13	IW Attack Tools: Cyberwar vis-à-vis EMP or RF Energy Weapons	118
5.14	IW –Offensive and Defensive Operations	119
5.15	Levels of Vulnerability and Threat	120
5.16	Approach for Assessment of IW Threats	124
5.17	IW Objectives.....	126
5.18	IW Threat Spectrum & National Security.....	126
5.19	Developing IW Capability for India.....	127
5.20	IW Threats Perception for India.....	128
5.21	Proposition for a National IW Framework for India.....	129
5.22	Conclusion.....	131
	PART- III EMP AND HPM ENERGY WEAPONS - A NEW INFORMATION AGE	
	DETERNCE.....	134
6	CHAPTER 6 EFFECTS AND VULNERABILITIES OF EM ENERGY.....	135
6.1	Introduction	135
6.2	EMP, RF and Microwave Energy	135
6.3	Historical Background.....	135
6.4	Effects of Nuclear Detonations: Radiating Fields.....	136
6.5	Characteristics of Radiating Fields [NUEFSHIP].....	138
6.6	Nuclear–EMP Effects on Electronic Devices (Effects of Neutrons)	140
6.7	Effects of Microwave Energy on Electronics, Materials and Personnel.....	142
6.8	Weaponisation of Microwave Energy.....	144
6.9	Categorization and Frequency Ranges for EM Weapons	146
6.10	Propagation of RF Energy as a Weapon	148
6.11	Potential of EM Weapons to Damage NII	148
6.12	Evaluation of Electromagnetic -Pulse as Weapon of Choice.....	149

6.13	Evaluation of HPM as Weapon of Choice	151
6.14	Potential Applications of EM Weapons	153
6.15	Conclusion.....	156
7	CHAPTER 7 TECHNOLOGY ASSESSMENT FOR DEVELOPMENT OF EM WEAPONS.....	157
7.1	Introduction	157
7.2	Historical Background.....	157
7.3	Evolution of High Power Microwave Devices	158
7.4	Profile of EM Weapons Programs USA	159
7.5	Events in Other Countries	162
7.6	Development of Building Blocks for RF Weapons	164
7.7	Live Testing.....	168
7.8	Damage Potential of RF / Microwaves Weapons	168
7.9	Emerging Directions	169
7.10	Conclusion.....	171
PART- IV	DEVELOPMENT OF IW CAPABILITY AROUND EMP & HPM ENERGY WEAPONS.....	173
8	CHAPTER 8 DEVELOPMENT OF EM WEAPONS	174
8.1	Introduction	174
8.2	Threat Perception	174
8.3	Scoping of the Solution Strategy.....	175
8.4	Operational Requirements.....	176
8.5	Building Blocks and Technology Base for EMP and RF Energy Weapons	177
8.6	Construction of EM Weapons.....	177
8.7	Development Objectives & Time Frames.....	189
8.8	Scope of Basic Research and Technology Demonstration.....	189
8.9	Development Program.....	189
8.10	Protection and Assurance Program	193
8.11	Development of Alternative Technologies for Risk Mitigation Against EM Weapons [62,63,64]	194
8.12	Suggested Approach for India.....	198
8.13	Conclusion.....	200
9	CHAPTER 9 PACKAGING INDUCTION AND DEPLOYMENT OF EM WEAPONS	203
9.1	Introduction	203
9.2	Identification of Targets.....	203
9.3	Delivery Systems for EM weapons.....	204
9.4	Lethality Assessment Issues.....	208
9.5	Enhancing Lethality of EM weapons.....	214
9.6	Doctrines for Use of EM Weapons	217
9.7	Defense Against EM Weapons	227
9.8	EM Weapons for IW-Defense.....	230
9.9	Defense Against Air Attacks.....	231
9.10	Enforcement of Technology Control Regime Using EM Weapons.....	231
9.11	Conclusions	231

10	CHAPTER 10 RESEARCH & DEVELOPMENT NEEDS OF THE EM WEAPONS PROGRAM	233
10.1	Introduction	233
10.2	Overview of Directed Energy Weapons (DEWs)	233
10.3	Research Design and Development (RD&D) Perspective	234
10.4	Survey of Global RD&D Initiatives in DEWs	235
10.5	Role of Simulation and Modeling: Foundation for Development of Next Generation EM Weapons	245
10.6	Research & Development Blue Print for India's EM Weapons Program	249
10.7	Indications for Future RD&D in EM Weapons	253
10.8	Conclusion.....	254
11	REFERENCES	256
12	PUBLICATIONS	273
13	INVITED TALKS	275
14	GLOSSARY	276

List of Figures

<i>Figure 1-1: National Security Threat and Deterrence Potential of IW Weapons</i>	7
<i>Figure 1-2 Basic Functions and Issues of NII Security</i>	10
<i>Figure 1.3 National Strategy to Secure the NII</i>	11
<i>Figure 1.4 : Threat Analysis & Warning</i>	11
<i>Figure 1.5 : Prevention & Protection</i>	12
<i>Figure 1.6 : Information & Knowledge Creation</i>	12
<i>Figure 1.7 : Response Management</i>	13
<i>Figure 1.8: Timeline for NIAP Activities</i>	13
<i>Figure 1.9: National Organisation for Critical Infrastructure Protection</i>	14
<i>Figure 1.10: NSTISSC Structure</i>	14
<i>Figure 1.11: A Complete IW Solution: Interlocking, Cooperative, Tailored and Includes Recovery)</i>	15
<i>Figure 1.12: US Defense Information Infrastructure Security Overlay</i>	15
<i>Figure 2.1: MCIT IT vision - 2010 Action Plan</i>	31
<i>Figure 2.2: Information Infrastructure Connectivity</i>	32
<i>Figure 2.3 : Sector wise Critical Infrastructure</i>	33
<i>Figure 2.4: Schematic Diagram of NII</i>	35
<i>Figure 2.5 : Survey of NII Initiatives across the Globe</i>	37
<i>Figure 3.1: National Infrastructure Dependencies</i>	49
<i>Figure 3.2: Analysis of Infrastructure Interdependencies</i>	50
<i>Figure 3.3: Critical NII Nodes</i>	52
<i>Figure 3.4: Infrastructures at Risk due to ICT Failures</i>	54
<i>Figure 3.5: Influences Across the Critical Infrastructures</i>	55
<i>Figure 3.6: Sector wise Vulnerability Assessment Plan</i>	58
<i>Figure 3.7: Activity wise USA spending on CIP for FY1998 - FY2001</i>	59
<i>Figure 3.8: Agency wise US spending on CIP for FY 1998 - FY 2001</i>	60
<i>Figure 3.9: 5 Level Threat & Vulnerability Model</i>	67
<i>Figure 3.10: NII Security Architecture</i>	69
<i>Figure 3.11: Integrated Information Infrastructure Security Overlay</i>	71
<i>Figure 3.12: Security Model</i>	72
<i>Figure 4.1: Three major Societal Transformations: Examples of Key Novelties</i>	77
<i>Figure 4.2: Three major Societal Transformations: Security Consequences</i>	78
<i>Figure 4.3 Information Operations Systemic Issues</i>	80
<i>Figure 4.4: Joint Vision 2020 of US, DOD</i>	82
<i>Figure 4.5 Components of Information Age Warfare</i>	84
<i>Figure 4.6 Impact of Information Based Operations</i>	85
<i>Figure 4.7: Logical Model of Network Centric Warfare</i>	88
<i>Figure 4.8: Components of Information Warfare</i>	95
<i>Figure 4.9 Component in Northrop Grumman Built Military systems</i>	97
<i>Figure 4.10 IW Survivability Summary</i>	100
<i>Figure 4.11: IW RMP for Weapons Systems</i>	101
<i>Figure 4.12: IW RMP for Distributed Information Systems</i>	102
<i>Figure 5.1 CNI targets of IW attacks</i>	109
<i>Figure: 5.2 Integrated Physical and IW Attack Scenario</i>	109
<i>Figure 5..3 Estimated number of attacks per hour as a function of time (UTC)</i>	110

Figure 5.4 Point of Attack.....	111
Figure 5.5 Financial Losses.....	112
Figure 5.6 Attack Sophistication vs. Intruder knowledge.....	112
Figure 5.7 IW capability of Different Nations	115
Figure 5.8 Interdependencies : Risk and Vulnerabilities.....	117
Figure 5.9 Attack Tools Vs Cost, Availability.....	119
Figure 5.10: IW Offense and Defence.....	120
Figure 5.11: CNI Vulnerabilities	121
Figure 5.12: CI Threat Layers	122
Figure 5.13: Typical Risk Assessment Model	123
Figure 5.14: Infrastructure Protection Process.....	123
Figure: 5.15 Scope of Useful But Unavailable Information.....	124
Figure 5.16 : Proposed Roles and Responsibilities for National Infrastructure Assurance	126
Figure 5.17: IW Threats Spectrum.....	127
Figure 5.18: IW as Viewed From Overall National Security Strategy.	128
Figure: 5.19 IW Threat to India.....	129
Figure: 5.20: National Security Threat and Deterrence Potential of IW Weapons	130
Figure 6.1: Nuclear Burst Effects Relative to Time.....	137
Figure 6.2: Typical Electromagnetic Pulse Shapes.....	137
Figure: 6.3 Energy Spectrum from Nuclear Detonation	138
Figure 6.4: Composite Effects of Nuclear Detonation at Different	139
Figure 6.5: EMP waveform Summary.....	140
Figure 6.6: Excitation of Electronics by EM field in a Shielded Facility.....	141
Figure 6.7: RF Effects on Electronics Equipment	142
Figure 6.8 EM Energy Interaction with Equipment and Cabling System.....	145
Figure 6.9: Categorization of Weapons.....	146
Figure 6.10: Electromagnetic Devices in Different Frequency Bands.....	147
Figure 6.11: Wave Length vis-a-vis Ranges of Energy.....	147
Figure 6.12: Categories of EMP & RF Energy Weapons	156
Fig 7.1: Evolution of High Power Microwaves	159
Figure 7.2: Summary of RD & D Projects, usable in EM Weapon Programs	162
Figure 7.3: High Power Microwave Beam Weapon Carried by Sead Platform (C. Kopp, 95/96)	163
Figure 7.4: Microwave Seismic Sensor Carried by Rece Platform (C.KOPP 10/95).....	163
Figure: 7.5: HPM E-Bomb Warhead (MK. 84 Form Factor)	171
Figure 7.6: Comparison Of Standoff, Free-Fall And Glide Weapons.....	171
Figure 8.1: USAF Core Competencies and High Power Microwaves	177
Figure 8.2: Components of EM Weapons	178
Figure 8.3: Generation of High Power Pulse.....	179
Figure 8.4 : Pulsed Power Needs for DoD, USA.....	179
Figure 8.5: X-ray image of Flux Compression Generator	181
Figure 8.6: Constructional Details of FCG.....	181
Figure: 8.7 Components of a FCG	182
Figure 8.8: Sequence of Flux Compression.....	183
Figure 8.9 Electric model of Flux Compression Generator	184
Figure 8.10: Generator current output, measured and calculated.....	184

<i>Figure 8.11: Spectral Energy Density of Radiation.....</i>	<i>186</i>
<i>Figure 8.12. : Constructional Details of Axial Vircator.....</i>	<i>187</i>
<i>Figure 8.13: Current in the Coil of the EMGF.....</i>	<i>188</i>
<i>Figure 8.14: Suggested Development Roadmap.....</i>	<i>189</i>
<i>Figure 8.15: Shedding Topology Diagram for MX HSS (Peacetime Configuration).....</i>	<i>195</i>
<i>Figure 8.16 Behavior of the Digital Circuitry to the Excitation.....</i>	<i>197</i>
<i>Figure 8.17: Modeling for EM Vulnerability Analysis.</i>	<i>197</i>
<i>Figure 8.18: Infrastructure Framework for National Information Warfare Program.</i>	<i>200</i>
<i>Figure 9.1: Height of Detonation vis-à-vis Lethality.....</i>	<i>206</i>
<i>Figure 9.2: Mode Delivery vis-à-vis weapon CEP.....</i>	<i>206</i>
<i>Figure 9.3 : Delivery Profile of GPS Guided EM Weapon.....</i>	<i>207</i>
<i>Figure 9.4 Lethal Footprint of the Low Frequency E-bomb in Relation to Altitude.....</i>	<i>211</i>
<i>Figure. 9.5: Lethal Footprint of HIPM E-Bomb in Relation to Altitude.....</i>	<i>211</i>
<i>Figure:9.6: Damage Potential of HPM Weapon.....</i>	<i>213</i>
<i>Figure 9.7 FCG Based EM Weapon Payload.....</i>	<i>214</i>
<i>Figure 9.8: Packaging of HPM Vircator Based Device.</i>	<i>216</i>
<i>Figure 9.9: Low Frequency E-Bomb - General Arrangement for Packaging.....</i>	<i>216</i>
<i>Figure 9.10: Packaging Using Vircator and 2Stage Flux Compression Generator.....</i>	<i>217</i>
<i>Figure 9.11: Mapping Warden's Model into NII.....</i>	<i>218</i>
<i>Figure 9.12: Mapping warden Model for EMP Weapons.</i>	<i>219</i>
<i>Figure 9.13: Typical Hardening Arrangement.....</i>	<i>229</i>
<i>Figure 10.1: Differing Characteristics of Laser and HPM Weapons.....</i>	<i>234</i>
<i>Figure 10.2 : DE Technology Program of DoD, USA.....</i>	<i>235</i>
<i>Figure 10.3: Manning Pattern for USAF DEW Directorate.....</i>	<i>236</i>
<i>Figure 10.4: USAF DEW Program Funding FY 2000.....</i>	<i>236</i>
<i>Figure 10.5: Developments in Pulsed Power Supplies.....</i>	<i>240</i>
<i>Figure 10.6: Project Groups and their Profiles at Stanford Linear Accelerator Center, USA.....</i>	<i>243</i>
<i>Figure 10.7: RD&D Collaboration by AFOSR under MURI program.....</i>	<i>244</i>

ABSTRACT

Introduction

The world today stands on the crossroads of challenges dictated by the Information Technology (IT). The survival and sustenance of human race in social, political, economic and military terms has never been so closely and tightly controlled by any technology as is being done by the IT. India is also sensitized to this reality and our resolve to become IT Super Power by the year 2008 justifies this intent. This resolve has its roots in a secure and credible National Information Infrastructure (NII), which must become the bedrock of our main stream IT activities.

The thesis examines the scope and promise of the NII, identifies critical issues in its design, engineering, creation and operations. The thesis signifies that security, safety and all time availability of the NII can be jeopardised by the on set of Information Warfare (IW). The IW relates to waging a war on target nations using information related principles, whereby the information systems are disabled, denied, damaged or destroyed using informational weapons such as Electromagnetic Pulse (EMP) and High Power Microwave (HPM) devices. These weapons have deterrence value near equivalent to nuclear arsenal, except the collateral damage.

The thesis examines the IW threat, assesses EMP and HPM device technologies under development and their impact on the NII survival and sustenance as Weapons of Mass Electrical Destruction (WMED). The thesis signifies that no such devastating weapons have ever been developed on this earth and a programmed war can take the civilization 200 years back to non-industrial ages. Thus EM weapons will have a direct bearing on our national security posture. Therefore India has no option but to develop contemporary IW capability around the EM weapons. A framework and blue print to develop this capability has been presented.

National Information Infrastructure Perspective

The Ministry of Communications and Information Technology (MCIT) in its India IT Vision - 2010 Action Plan, seeks to promote use of IT in all areas of the national economy and security. This plan would be founded on a world-class physical, institutional, and regulatory infrastructure, which will embrace the growing convergence of telecommunications, computers, consumer electronics, and the media infrastructure. This National Information Infrastructure would be the sum total of the Local Information Infrastructure (LII), Defense Information Infrastructure (DII), Government National Information Infrastructure (GNII), Corporate Information Infrastructure (CII) etc. It would be suitably integrated with the Global Information Infrastructure (GII).

Promise of NII: The societal promise of NII would be aimed to provide universal online connectivity to every Indian; be it a student, soldier, businessman, scientist, engineer, or doctor, without regards to geography, distance, resources, or disability. The NII would be a single thread traversing through, and, underpin every national infrastructure in energy, transport, finance, banking, healthcare, defense, business, industry, education and the government. Therefore NII would signify more than the physical facilities used to collect,

collate, transmit, store, process and display voice, data, text, and images. It would encompass ever-expanding range of equipment including cameras, scanners, keyboards, telephones, fax machines, computers, switches, compact discs, video and audio tapes, cable, wire, satellites, fiber optics transmission lines, microwave links, switches, televisions, printers, monitors etc. The NII would interconnect and integrate these physical components in a technologically neutral manner. The NII would encompass content in the form of video programming, scientific or business databases, images, sound recordings in laboratories, studios, publishing houses, government etc. The NII applications software would allow end users to access, manipulate, organize and digest the mass of information. The NII by itself will be under pinned by a framework of standards and specifications to facilitate connectivity, interoperability, security, reliability and availability. The people would form the most significant component of NII who will create information, develop applications and services, construct facilities and train others to tap its potential. The people would exist as owners, vendors, operators, service providers etc.

Critical Issues in Engineering the NII: The development, operations and support of NII would be the most difficult and challenging task of this century for all the nations including India. The critical issues in its engineering will encompass a NII framework with clearly defined objectives, goals, policies and roadmap, collaborative, requiring significant policy changes, communications reforms, regulatory framework for universal access for cable TV, phone, revision of tax policies, security etc. The NII would be a "Network of Networks" and a "System of Systems" seeking information exchange over disparate networks easily, accurately and securely. It would be sufficiently open and interactive to evolve new communications facilitating collaborative learning, work, play and participation. The NII would need to ensure collection, collation, processing, storage and distribution of a large variety of information quickly at affordable cost.

Security Concerns of NII: The most critical issue would be to embed safety, security, confidentiality, integrity and availability of the Critical National Information Infrastructures (CNII). This will ensure protection at all levels, for all times, against the impending IW threat from EMP and HPM weapons.

Security Threats to NII: Threats and vulnerabilities to NII at individual, agency, state and national level have been identified in terms of gaps or weakness in protection policy, processes, and regulatory framework. These have been further amplified in terms of safety, security, confidentiality, availability, integrity, non-repudiation and time sensitivity. A scalable security framework in terms of architecture, policy, people and technology has been outlined. A security model addressing information, databases, computing resources, networking components, communications, personnel and physical environment has been examined.

The threats and vulnerabilities to NII arising out of Counter Virus Counter Measures (CVCM) as a part of Information Warfare (IW) have been examined. War Quality Viruses are becoming a part of military effort under formal IW programs. Development and integration of CVCM into military operations is a critical issue of national security. This

aspect has been examined and creation of a military capability from a national security perspective has been addressed.

Threat to NII from nuclear and non-nuclear EMP and HPM energy weapons has been examined. The EMP/ HPM weapons are a new class of weapons, under development by many countries. These weapons can be used by the Armed Forces and / or terrorist groups to deny, disable, disrupt, damage or destroy electronics and electrical systems. These weapons have the potential to detonate instantaneously, cause damage at the speed of light, operate in all weathers from air, surface or underwater platforms, and cover very large areas. These weapons do not require precise knowledge of target systems, don't cause collateral damage to buildings and don't kill human beings. They can target NII components of both civil and military establishments. Their deterrence and damage potential is near equivalent to nuclear weapons. Besides, they can enable a nation to win a war without causing human casualties. Therefore IW capability is emerging as a critical necessity for every nation to protect its NII against EMP and HPM weapons and at the same time to build a deterrence posture. Considering the national importance of this issue, "**Building IW Capability through Development of EM Energy Weapons**" has been identified as a focus of research in this thesis.

Information Warfare Threat to NII

The security of NII is the most critical issue, since NII underpins all the Critical National Infrastructures such as governance, defense, finance, banking, transport, trade, industry, energy etc. Within *NII Security*, the **Information Warfare** is a new digital age threat. In Information Warfare, a nation can disable, damage, deny and / or destroy enemy Information Infrastructure using Information Based techniques, while defending its own information assets. The power of Information Warfare is being perceived as follows:-

"Information Warfare attacks on the NII can be launched through viruses, network penetration attacks, denial of service attacks and EMP or HPM Energy weapons. These weapons can completely and irrevocably neutralize, incapacitate and isolate a most powerful nation in social, political, economic and military terms without firing a single shot using any conventional weapons".

The potential of EMP and HPM Energy weapons is being viewed as:-

"The EMP & HPM weapons are a totally new development of unprecedented complexities which possess damage & deterrence potential equivalent to nuclear weapons, and are not amenable to import". The quotes and statements presented below signify this

- *"The Threat to our Military and Commercial Information Systems poses a significant risk to National Security and must be addressed"*, William J Clinton, *National Security Strategy*, 1995.
- *"Our United States and our allies ought to develop the capacity to address the true threats of the 21st century. The true threats are Biological and Informational Warfare"*, George W. Bush, *IOWA speech*, 8th Jan, 2001

"The danger posed by International hack Attacks against critical US networks in some ways comparable to the threat Soviet nuclear warheads posed during the cold war" Secretary of State, USA, Condoleezza Rice, Mar 22, 2001

"Information in all its forms, Information Protection, and the increasingly prominent position of Information in the Attack have become central features in determining the outcome of modern and future conflicts.", General John M Shalikashvili, Chairman, JCOS, Memo, IW Status, 10th Oct. 1995.

Formulation of Research Problem

The research effort has been focused on the investigation of nuclear and non nuclear EMP generation, HPM energy generation, the frequency spectrum of EM waves, control of EM spectrum linked to military dominance, effects of EMP on solid state electronics which in turn constitute the foundation of all computers, networking components, communication systems and electrical power generation and distribution systems. Investigations have also been focused on the range and type of efforts for development of EM weapons technologies, EM effect studies, protection techniques, weaponising of EM devices, role and relevance of virtual simulation, building blocks of EM weapons, their lethality and deployment doctrines. These investigations have been mapped into program specific Research Design and Development (RD&D) needs of India and their integration into Integrated Guided Missile Development Program (IGMDP), Advanced Light Helicopter (ALH), Light Combat Aircraft (LCA) and Main Battle Tank (MBT) programs.

Research Methodology & Approach

The methodology to undertake this research work involved search and study of multiple sources of data and concepts, create a system to harvest ideas, converse with diverse peoples, continuous review, selection and integration of data flows and cross talk on virtual and actual communication nets. It created a self-servicing, rapidly adapting system for learning and knowing. The combination of people from industry & government and reference to case studies of work underway in USA under the National Information Assurance Program (NIAP), Vision 2020, Air Force 2025, Defense Area Plan - Weapons, Information Systems Assurance Services Office, Department of Defense, Critical Infrastructure Protection Initiatives of Department of Energy, Multi University Research Invitation (MURI) etc. encouraged a maverick thinking in me. It was a powerful means to envision future shape of things in IW.

IW Threat Forecasting and Assessment Methodology: A number of future forecasting methodologies were examined. A methodology based on of selection of alternate future, operations analysis, value focused modeling as identified by the DoD, USA for its Air Force 2025 has been adapted. This methodology gave rise to guiding factors viz. economic interest, technology dominance, low intensity threat, regional dominance, economic parity etc. The resultant assessments narrowed down to the necessity and relevance to create IW Capability with outlines of major national programs already underway in defense, food, technology, infrastructure etc in our country.

Methodology for IW Framework & Blue Print: Another methodology from Mitre Systems presented by Robert J Clerman, has been adapted for mapping national IW

Strategy in to threat analysis & warning, prevention & protection, response management, information sharing & knowledge creation.

Study of IW Initiatives Overseas: USA, Australia, and Europe have taken lead in underpinning CNIs with credible and secure NIIs. Following initiatives of USA have been examined.

- Steps and timeline for NIAP activities
- National level organizations for Critical Infrastructure Protection in terms of Presidential directive
- National security committees and working groups
- IW solution components
- Defense Information Infrastructure Security Overlay including EMP and HPM energy weapons and the protection strategies.
- Research initiatives

Approach to Analysis: The analysis of NII under pinning critical national infrastructures, vulnerabilities of NII to IW attacks, strengths and weaknesses of informational weapons, vulnerabilities of microelectronics to EMP and HPM energy, relating EM energy to a weapon like role, conceiving these devices as Weapons of Electrical Mass Destruction, their reaction times comparable to speed of light etc. have been undertaken through systematic examination of comparable events around the globe. These have been supported by data and references. No formal tools for data processing have been used. The gist of analysis is as follows:-

- India's NII and the IT penetration in CNIs is still at a very nascent stage and very scantily documented. IW threats & vulnerabilities are not obvious to, and, understood by the planners and decision makers. Therefore many inputs to evolve IW framework are not available in the country.
- EMP and HPM research is highly classified, therefore reliance has been on open sources of literature.
- NII, NIAP & IW programs of USA, Australia & European nations have been examined for guidance.
- Results of the EMP from nuclear tests, research efforts on electro magnets to generate Non-Nuclear EMP, and the effects of EMP and HPM energy on microelectronics have been examined.
- Analysis of dependencies of NII underpinning CNIs, vulnerability of NII to IW attacks using HPM and EMP energy weapons, relating EMP and HPM devices to a weapon's role, conceptualizing HPM as WMED, preparing wish list for national, IW capability, technology development, production, doctrine, combat model, deployment, future course of research etc. have been examined in detail.
- Presentation of Work involving collection, collation, analysis, inferences and conclusions has been referenced and each phase of the research work has been documented chapter wise.

Research Inputs : Following steps have been followed for research inputs.

- Research Inputs include literature survey, interaction with experts, personal know-how & experience, personnel involvement in RD&D programs. The inputs from

DRDO, DAE, ISRO & Armed Forces on research, technology, budgets, tie-ups, induction plans etc. have been very limited.

- Interaction with experts based on personal involvement as author of Navy and National C4ISR concept, program manager, Navy's Command & Control Systems program director, Navy's IW Initiatives, member- Prime Minister's National IT Task Force, member, Defense IT Task Force, member, Working Group on National RD&D in IT and the founder of Information Assurance Laboratory at MBT Mumbai has provided immensely useful inputs.
- Some of the details personally known to me are classified and therefore have not been referenced.
- EMP / HPM weapons research is highly classified, therefore inputs through personal interaction have been taken from US Universities (CMU, Stanford, Texas, Michigan, Perdue), information security related associations (SANS Security Training Institute, Washington, USA, Association of Fraud Examiners (ACFE), International Information System Security Consultancy Consortium (ISC2), Disaster Recovery Institute International (DRII), Washington, USA, Information Security Audit and Control Association (ISACA), USA.) and, societies / Labs (JAWS Technologies, Canada)).
- Methodology has been benchmarked with national awareness initiatives of the NII underpinning CNIs, IW framework & Blue Print of Western countries, RD & D needs of EMP & HPM Weapons Program of USA, Russia and China, technology development & system engineering life cycles for major infrastructure and production, induction, deployment & support life cycles of major military programs.
- Program level references within and outside India included Integrated Guided Missile Development Program, India, Advanced Technology Vehicle Project (ATVP), India, National Information Assurance Program (NIAP), USA, Directed Energy Weapons Program (DEW), USA, National Information Infrastructure Initiatives, USA, Australia and India.

Research Objectives & My Contribution:

The objective of this research effort has been to provide **“Thought Leadership to the country for a potential multi-billion rupees RD&D program, aimed at early leadership role for India amongst the proponents of Information Warfare, possession of deterrence status by India as an IW weapon power, immense earning potential through export of EM weapons and cross fertilization of expertise across a wide spectrum of scientific and technological fields in civil sector to leverage spin-offs of these technologies.** I have been able to make following concrete and credible contributions.

- **Identification of IW Threat to National Security:-** This included identification of critical National Infrastructures (CNIs) sustaining our social, political, economic, military operations and governance, identification of interdependencies amongst themselves, NII components (including CII, DII, GNII) underpinning CNIs, NII threats & vulnerabilities from Info War, Netwar and Cyberwar, assessment of potential of EMP and HPM as Weapons of Electrical Mass Destruction (WEMD) & Deterrence, study of comparable NII, NIAP, IW-D, DEW initiatives of USA, Russia & China.

- **National IW Capability:** Framework and Blue Print has been suggested. An organizational structure for research, and development has been proposed.
- **IW Program Needs:** These have been defined in terms of the, know-how, basic research, technology development, system development & engineering, tests & evaluation , production and deployment
- **IW Operation:** These have been conceptualized in terms of .Armed Forces needs, operational doctrines, combat model, integration with conventional weapons, protection strategies & civil defense
- **Research, Design and Development foot print:** Following has been presented
 - Basic research in Pulsed Power, Storage, Shaping, Transmission, Measurements, Accelerator Structure, Advanced Beam Concepts, Collective Effects, HPM, Vircators, Wave Oscillators, Fast Wave Gyros, Plasma Filled Devices.
 - Technology development for HPM sources (MHz - GHz frequency, MW - GW power), compact high power modules, high gain, UWB antennae systems, compact, efficient, high, pulsed power drives.
 - Assessment of HPM effects & lethality pertaining to RF testing of crucial military assets counter measure techniques, biological effects, civil, defense issues.
 - Integration with military programs such as IGMDP, NC4ISR, UAVs.
 - Protection program comprising of EMP hardening, susceptibilities studies, components, systems and platform protection.
 - Development of EM weapons based military posture encompassing surveillance & defence, counter proliferation, counter - munitions.
 - Integrated follow-on efforts for technology demonstration, system level developments, testing & evaluation, tactics and doctrines, combat modeling.

Potential End Users of this Research: The thesis have the potential for use as follows:-

- Reference framework for Ministry of Communication and Information Technology to evolve and implement National Information Assurance Program for protection of critical NII.
- Blue Print for development of Information Warfare capability built around EMP and HPM energy weapons. This would concern National Security Council, ministries of home affairs, finance, defense and the industry.
- Compiled information resource for institutions, DRDO, DAE, Armed Forces and the research community in general.

Structure of the Thesis Document: The thesis has been organized in 4 sections under chapters 1 to 10 as follows

- **Understanding the Critical Issues of Engineering the NII**
 - Research Overview and Literature Survey
 - National Information Infrastructure
 - NII Security Perspective & Issues
- **Information Warfare: An Emerging Threat to NII**
 - Information Age Warfare
 - IW Threat Assessment

- **EMP & RF Energy Weapons: A New Information Age Deterrence**
 - Effects & Vulnerabilities of EM Energy
 - Technology Assessment for Development of EMP & RF Energy Weapons.
- **Development of IW Capability Around EMP & RF Energy Weapons.**
 - Development of EM Weapons
 - Packaging, Induction & Deployment
 - Research Needs of EM Weapons Program

Conclusion

This research addresses the development of EM energy weapons as a non-lethal IW capability in offensive and defensive role. The following conclusions emerge from this research effort.

- NII is synonymous with, and central to India's survival and sustenance in social, political, economic and, military terms.
- NII is extremely prone to disability, damage, denial of service and destruction by the IW weapons.
- IW is emerging as a new dimension of "Warfare in the Digital Age".
- The IW threat in the form of Net War, Cyber War and Info Warfare exists in three categories viz., "National Security Threat", "Shared Threat to Civil and Military Establishments", and "Local Threat affecting social, political, economic and military interests".
- EMP and HPM energy as Weapons of Electrical Mass Destruction, can inflict unprecedented damage to microelectronics embedded in every system on the earth, and is thus extremely threatening for the civilized world
- Building IW capability around EMP & HPM weapons for India is inevitable and unavoidable. It befits India's 21st century security needs and deterrence posture blending with nuclear capability.
- India possesses critical mass of basic know-how, technology, software based simulation to develop IW capability around EMP and HPM energy weapons.
- A framework and blue print to develop this IW capability has been evolved and presented in this thesis.
- The proposed IW program is crucial for self-reliance, it and will free India from technology control regime imposed by the West.
- This capability will position India in "Power Projection League" with "Deterrence" equated to Nuclear Capability.
- The IW program will enable cross-fertilization in expertise and would result in numerous technology spin-offs.
- The program multi-billion dollars export potential.
- Proposed framework and blue print are "**Robust and Risk Free**".

This thesis meets the stated objective of :

"Providing thought leadership to create research, design and development footprint for national security agencies, research community and industry to build Electromagnetic Pulse / High Power Microwave weapons as a principal component of India's Information Warfare capability"

The proposed framework and blue print compares with other national level initiatives of the past viz.

- Atomic Energy Program
- Indian Space Program
- Integrated Missile Program
- National Food Program

PART- I
UNDERSTANDING THE CRITICAL ISSUES

CHAPTER 1: RESEARCH OVERVIEW AND LITERATURE SURVEY

**CHAPTER 2: NATIONAL INFORMATION INFRASTRUCTURE
PERSPECTIVE**

CHAPTER 3: NII SECURITY PERSPECTIVE AND ISSUES

CHAPTER 1

RESEARCH OVERVIEW & LITERATURE SURVEY

1.1 Introduction

The world today stands on the crossroads of challenges dictated by the Information Technology (IT). The survival and sustenance of human race in social, political, economic and military terms has never been so closely and tightly controlled by any technology as is being done by the IT. India is also sensitized to this reality at the level of individuals, citizens, society, corporate sector, and the government. Our resolve to become IT Super Power by the year 2008 justifies this intent. This resolve has its roots in a secure and credible National Information Infrastructure (NII), which must become the bedrock of our main stream IT activities.

The thesis examines the scope and promise of the NII, identifies critical issues in its design, engineering, creation and operations. The thesis signifies that security, safety and all time availability of the NII can be jeopardised by the on set of Information Warfare (IW). The IW relates to waging a war on target nations using information related principles, whereby the information systems are disabled, denied, damaged or destroyed using informational weapons such as Electromagnetic Pulse (EMP) and High Power Microwave (HPM) devices. These weapons have deterrence value near equivalent to nuclear arsenal, except the collateral damage.

The thesis examines the IW threat, assess EMP and HPM device technologies under development and their impact on the NII survival and sustenance as Weapons of Mass Electrical Destruction (WMED). The thesis signifies that in the foreseeable future, EM weapons will have a direct bearing on our national security posture. Therefore India needs to develop contemporary IW capability around the EM weapons. A framework and blue print to develop this capability has been presented.

This chapter describes research objectives, focus areas, approach and the methodology adopted in this thesis to prepare and present a framework for development of IW capability around EMP and HPM energy weapons. It also presents literature survey underpinning the research effort and the structure of thesis document. In order to illustrate the volume and complexity and seriousness of the IW issues, it presents an overview of the national and global NII initiatives, their security concerns and the programs underway in India and overseas for protection of Critical National Infrastructures (CNI) across the globe against IW attacks.

1.2 National Information Infrastructure Perspective

The Ministry of Communications and Information Technology (MCIT) in its India IT vision - 2010 Action Plan, seeks to promote use of IT in all areas of the national economy viz. agriculture, industry, trade, services etc. as a critical input in making India a global economic power. This plan would be founded on a world-class physical, institutional, and

regulatory infrastructure, which will embrace the growing convergence of telecommunications, computers, consumer electronics, and the media infrastructure (minus its contents). This National Information Infrastructure would be the sum total of the Local Information Infrastructure (LII), Defense Information Infrastructure (DII), Government National Information Infrastructure (GNII), Corporate Information Infrastructure (CII) etc. It would be suitably integrated with the Global Information Infrastructure (GII) [53, 103, 104, 105].

1.2.1 Promise of NII

The societal promise of NII would therefore be aimed to provide universal online connectivity to every Indian; be it a student, soldier, businessman, scientist, engineer, or doctor, without regards to geography, distance, resources, or disability. The NII would be a single thread traversing through, and, underpin every national infrastructure in energy, transport, finance, banking, healthcare, defence, business, industry, education and the government. Therefore NII would signify more than the physical facilities used to collect, collate, transmit, store, process and display voice, data, text, and images. It would encompass ever-expanding range of equipment including cameras, scanners, keyboards, telephones, fax machines, computers, switches, compact discs, video and audio tapes, cable, wire, satellites, fiber optics transmission lines, microwave links, switches, televisions, printers, monitors etc. The NII would interconnect and integrate these physical components in technologically neutral manner. The NII would encompass content in the form of video programming, scientific or business databases, images, sound recordings in laboratories, studios, publishing houses, government etc. The NII applications software would allow end users to access, manipulate, organize and digest the mass of information. The NII by itself will be under pinned by a framework of standards and specifications to facilitate connectivity, interoperability, security, reliability and availability. The people would form the most significant component of NII who will create information, develop applications and services, construct facilities and train others to tap its potential. The people would exist as owners, vendors, operators, service providers etc. [99, 182].

1.2.2 Critical Issues in Engineering the NII

The development, operations and support of NII would be the most difficult and challenging task of this century for all the nations including India. The critical issues in its engineering will encompass a NII framework with clearly defined objectives, goals, policies and roadmap. The building of NII would be a collaborative task seeking private investment and involvement, requiring significant policy changes, communications reforms, regulatory framework for universal access for cable TV, phone, revision of tax policies etc. The NII will also need to create universal service concept to ensure affordable access to advanced communications and information services, regardless of income, disability or location of all the citizens. The creation of basic information technologies in computing, networking and electronics will require massive and unprecedented technological innovations and new applications particularly in healthcare, government online services, education in rural areas, defense etc. The NII would be a "Network of Networks" and a "System of Systems" seeking information exchange over disparate networks easily, accurately and securely. It would be sufficiently open and interactive to evolve new communications facilitating collaborative learning, work, play and participation. The NII would need to ensure collection, collation,

processing, storage and distribution of a large variety of information quickly at affordable cost [85, 86, 99, 100].

1.2.3 Security Concerns of NII

The most critical issue would be to embed safety, security, confidentiality, integrity and availability of the Critical National Information Infrastructures (CNII). This will ensure protection at all levels, for all times, against the impending IW threat from EMP and HPM weapons. Many dramatic changes expected from development of NII will grow out of advances in wireless technologies. Therefore access to NII resources by anyone, at anytime from anywhere will have direct bearing on the control and management of Radio Frequency (RF) spectrum and its security issues [84,106].

In this thesis NII security has been examined with respect to internal and cross border, natural or man made threats, arising out of economic competition, political and social mismatch and military dominance through Information Warfare Weapons. The security has been examined in terms of intrinsic or built up vulnerabilities during design, operation and support of NII, arising out of technology, processes and environmental limitations. The threats and vulnerabilities to the NII have been mapped as risks, which can be mitigated or minimized through a set of cost-benefit trade-offs

1.3 Security Threats to NII

Threats and vulnerabilities to NII at individual, agency, state and national level have been identified in terms of gaps or weakness in protection policy, processes, and regulatory framework. These have been further amplified in terms of safety, security, confidentiality, availability, integrity, non-repudiation and time sensitivity. A scalable security framework in terms of architecture, policy, people and technology has been outlined. A security model addressing information, databases, computing resources, networking components, communications, personnel and physical environment has been examined. A preparatory framework to support this initiative in terms of technology, people and processes has been articulated. It emerges that this component of NII security is being addressed globally by all nations whereby people and technology can now be resourced at reasonable effort and expense. Therefore this area has not been researched further [76, 133, 175].

The threats and vulnerabilities to NII arising out of Counter Virus Counter Measures (CVCM) as a part of Information Warfare (IW) have been examined. The development of malicious code management framework and technology is a need-based effort and is universally shared by the IT community. No investigation therefore has been carried out in this area. However War Quality Viruses are becoming a part of military effort under formal IW programs. Development and integration of CVCM into military operations is a critical issue of national security. This aspect has been examined and creation of a military capability from a national security perspective has been addressed

Threat to NII from nuclear and non-nuclear Electromagnetic Pulse (EMP) and Radio Frequency (RF) weapons has been examined. The EMP/RF weapons are a new class of weapons, under development by many countries. These can be used by the Armed Forces and/or terrorist groups to deny, disable, disrupt, damage or destroy electronics and electrical

systems, which form the basic building blocks of NII. These weapons have the potential to detonate instantaneously, cause damage at the speed of light, operate in all weathers from air, surface or underwater platforms, and cover very large areas. These weapons do not require precise knowledge of target systems, don't cause collateral damage to buildings and don't kill human beings. They can target NII components of both civil and military establishments. Their deterrence and damage potential is near equivalent to nuclear weapons. Besides, they can enable a nation to win a war without causing human casualties. Therefore IW capability is emerging as a critical necessity for every nation to protect its NII against EMP and RF Weapons and at the same time to build a deterrence posture. Considering the national importance of this issue, "Building IW Capability Through Development of EM Energy Weapons" has been identified as a focus of research in this thesis. The research work has been organized as follows:

- **Understanding the Critical Issues of Engineering the NII**
 - National Information Infrastructure
 - NII Security Perspective & Issues
- **Information Warfare: An Emerging Threat to NII**
 - Information Age Warfare
 - IW Threat Assessment
- **EMP & RF Energy Weapons: A New Information Age Deterrence**
 - Effects & Vulnerabilities of EM Energy
 - Technology Assessment for Development of EMP & RF Energy Weapons.
- **Development of IW Capability Around EMP & RF Energy Weapons.**
 - Development of EM Weapons
 - Packaging, Induction & Deployment
 - Research Needs of EM Weapons Program

1.4 Information Warfare Threat to NII

The security of NII is the most critical issue, since NII underpins all the Critical National Infrastructures such as governance, defense, finance & banking, transport, trade, industry, energy etc. Within "*NII Security*", the Information Warfare is a new digital age threat. In Information Warfare, a nation can disable, damage, deny and / or destroy enemy Information Infrastructure using Information Based techniques, while defending its own information assets. The power of Information Warfare is being perceived as, "*Information Warfare attacks on the NII can be launched through viruses, network penetration attacks, denial of service attacks and EMP or HPM Energy weapons. These weapons can completely and irrevocably neutralize, incapacitate and isolate a most powerful nation in social, political, economic and military terms without firing a single shot using any conventional weapons*". The potential of EMP and HPM Energy weapons is being viewed as, "*This is a new class of weapons of unprecedented complexities which possess damage & deterrence potential equivalent to nuclear weapons, and are not amenable to import*".

1.4.1 Targets of IW Attacks

The spectrum of targets for IW attack can be very large and diverse and can range from GPS jamming to corrupting of missions, exploitation of emissions, damage, disability or destruction of electronics, corruption of real time data, munitions that can be armed or

made inert etc. A consistent IW attack can totally paralyze and incapacitate even a well-formed military force. With large scale computerization and dependence on data banks, the other risk areas where tampering or misinformation can be planted are the medical facilities, logistics, personnel data, cargo, transport, space, finance, trade, general administration, industry etc., categorised as follows.

The physical and information technology facilities, networks and assets whose disruption or destruction would have serious impact on the health, safety, security, economic well-being of the citizen or on the effective functioning of government in the country are also given below [95, 108, 110, 185].

- Government: Essential government services/ activities not included elsewhere.
- Energy and Utilities: Electrical power, water purification, sewage treatment, natural gas industry, oil industry.
- Services: Health care, food industry, postal/courier, meteorological, financial services, customs, immigration.
- Transportation: Aviation, surface, rail, marine.
- Safety: Nuclear, Hazardous material, prisons, flood control, environment, search and rescue, emergency services, building systems.
- Communication: Telecommunications, television industry, satellite systems, radio industry, cable television industry, mobile phones etc.

1.4.2 Intensity and Dimension of IW Threats

The IW Threat from EMP and HPM weapons is unprecedented and most threatening of all the weapons ever produced on the face of the earth. The quotes and statements presented in the figure 1.1 signify the seriousness of threat from Information Warfare, in particular from the use of EM weapons.

QUOTED BY	STATEMENT
William J Clinton US President National Security Strategy, 1995.	<i>"The Threat to our Military and Commercial Information Systems poses a significant risk to National Security and must be addressed"</i>
President George W. Bush IOWA speech 8th Jan, 2001	<i>"Our United States and our allies ought to develop the capacity to address the true threats of the 21st century. The true threats are Biological and Informational Warfare".</i>
Secretary of State, USA, Condoleeza Rice, Mar 22, 2001	<i>"The danger posed by International hack Attacks against critical US networks in some ways comparable to the threat Soviet nuclear warheads posed during the cold war".</i>
General John M Shalikashvili Chairman, JCOS Memo, IW Status, 10th Oct. 1995.	<i>"Information in all its forms, Information Protection, and the increasingly prominent position of Information in the Attack have become central features in determining the outcome of modern and future conflicts."</i>
Joseph S. Nye Jr. 7 Admiral William Owens "America's	<i>"Knowledge more than ever before is power. The one country that can best lead the information revolution will</i>

<p>Information Edge", 1996</p> <p>http://www.iwar.org.uk/cyberterror/index.htm</p> <p>Statement of Bronius Cikotas to US Congress on the The Progression of Terrorism and the Use of Nuclear And Non Nuclear EMP.</p>	<p><i>be more powerful than the other".</i></p> <p><i>"As long as nuclear warheads and the means to deliver them exist, the EMP threat still exists! Intent to use can change in a week or a month, and it takes us years of effort to harden our systems to EMP. This possibility for change of intent was implied in a meeting in Vienna between our Congressional delegation, which included Congressmen Curt Weldon and Roscoe Bartlett and their counterparts from the Russian Duma over tensions between U.S. and Russia with regard to our conflict in Kosovo. In summary, the message was – do not push Russia around, we have a responsible government now, but there are factions that could surface and push for an EMP attack against the U.S. that would shut your country down without directly causing physical damage or death. The vulnerability of our infrastructure and our society has increased with the increased use and dependence on electronics".</i></p>
<p>Defence Science Board, USA, Report (AP 237 STC 97, Sep. 1997)</p>	<p><i>"Unlike an attacker in conventional war, an attacker using the tools of information warfare can strike at critical civil functions and processes such as telecommunications, electric power, banking, or transportation and other centers of gravity or even at the social structure, without first engaging the military. Such a strategic information warfare attack can occur without forewarning or escalation of other events. In addition, attacks on the civil infrastructure could impede the actions of the military as much as a direct attack on the military's force generation processes or command and control".</i></p>
<p>New MAX.com 26th Jan, 2002</p>	<p><i>"In 1999-2001, the PLA was engaged in developing a "shell-less gun" (electromagnetic gun, or EMG). Present efforts are concentrated on developing an anti-tank EMG and an anti-aircraft EMG".</i></p>
<p>NEWSMAX.com 26th Jan 2002</p>	<p><i>"In Oct 2001, Chinese executives from Rosoboronexport made presentations at Lankagwi Int. Maritime & Aerospace 2001 exhibition in Malaysia about Ranets E (a mobile RF defence system against high-precision weapons) and Rosa-E(system designed to break enemy radar systems and ground based military installations)"</i></p>
<p>Office of the Director Defence Research & Engineering, USA, Memo Jun 28, 2002.</p>	<p><i>"HPC Challenge Project Sr. No. 1 FY 2003 "Directed High Power RF Energy: foundation of Next Generation Air Force Weapons - Air Force Research Laboratory - Keith Cartwright".</i></p>
<p>Figure 1-1: National Security Threat and Deterrence Potential of IW Weapons</p>	

1.4.3 Developments in IW Attack Tools: Cyber War vis-à-vis EM weapons

The IW attacks on infrastructures at national scale can be conducted through a series of hacker attacks, synchronized in time, combined with physical attacks. The most common choice for physical attacks would be switching stations, communication antennas, pipelines transformers, pumping stations and the cabling systems. The attacks on the information infrastructure can be through network penetration viz. virus attack, spamming etc. These attacks can also be launched through EMP and HPM energy weapons to disrupt, disable, damage or destroy the electronics embedded in the IT systems [35.80.150].

The research, design and development of all types of IW weapons such as "malicious code", "network penetration" and "EMP and HPM energy weapons" is necessary to create national level IW-Defense and IW Offense capability. As brought out above there is a global awakening and concern about malicious code and network penetration attacks and the national level Information Assurance Programs are being conceived and launched by USA, Australia, China and many European countries to safe guard their NIIs. The global IT and Communication industry is supporting these initiatives and considerable know-how, technology and industry support is available in this area. However the development of EMP and RF energy weapons is localized to few nations viz. USA, Russia, France, UK, Israel, Ukraine, China etc. These weapons are also called "Weapons of Mass Electrical Destruction" due to their potential to disable or damage any solid state electronic devices embedded in computers and communication systems.

The developments in the area of EMP and RF energy weapons are also shrouded in secrecy and confined to defense establishments. Very limited open source literature is available except initial investigative research emanating from nuclear EMP tests in 60s & 70's. The very high value IW capability programs involving military are underway across the globe. Also considering the controversies regarding use of nuclear weapons, most countries in the future will prepare deterrence posture around EMP and RF energy weapons and keep hard kill nuclear weapons as a last option.

1.5 Formulation of Research Problem

The research effort has been focused on the investigation of nuclear and non nuclear EMP generation, HPM energy generation, the frequency spectrum of EM waves, control of EM spectrum linked to military dominance, effects of EMP on solid state electronics which in turn constitute the foundation of all computers, networking components, communication systems and electrical power generation and distribution systems. Investigations have also been focused on the range and type of efforts for development of EM weapons technologies, EM effect studies, protection techniques, designing weapons with EM devices, role and relevance of virtual simulation, building blocks of EM weapons, their lethality, combat modeling and deployment doctrines. These investigations have been mapped into program specific Research Design and Development (RD&D) needs of India and their integration into Integrated Guided Missile Development Program (IGMDP), Advanced Light Helicopter (ALH), Light Combat Aircraft (LCA), Main Battle Tank (MBT) and Unmanned Aerial Vehicles (UAV) programs.

Therefore while the broad area of research pertains to Critical Issues in Engineering the NII, the research bearings are on the security of NII in the emerging information age and

Information Warfare as a serious concern for NII security. The specific research area is focused on building of Information Warfare Capability around the Electromagnetic Pulse and High Power Microwave weapons.

1.6 Research Methodology & Approach

The methodology to undertake this research work involved search and study of multiple sources of data and concepts, creation of a system to harvest ideas, converse with diverse players, continuous review, selection and integration of data flows and exchange of views on virtual and actual communication nets. It created a self-serving, rapidly adapting system for learning and knowing. The combination of inputs from government personnel, people from industry and reference to case studies of work underway in USA under the National Information Assurance Program (NIAP), Vision 2020, Air Force 2025, Defense Area Plan 1998-Weapons, Information Systems Assurance Services Office, Department of Defense, DII protection strategies, Critical Infrastructure Protection Initiatives of Department of Energy, Multi University Research Initiative (MURI) etc. encouraged a maverick thinking in me. It was a powerful means to envision future shape of things in IW.

The study does not compare existing systems with hypothetical ones because of the difficulties in comparing real with paper plans. The future segments have been based on emerging technologies and the perceived world of 2025. The study has avoided "Out-of-the-box" solutions. The emphasis has been to help create capability to maintain vigilant edge over land, sea and air space of the country in the area of IW in a manner that would benefit India's political, economic and military role in the foreseeable 25 years.

1.6.1 IW Threat Foreseeing and Assessment Methodology

A number of future forecasting methodologies were examined. A methodology based on of selection of alternate future, operations analysis, value focused modeling as identified by the DoD, USA for its Air Force 2025 was considered suitable. These techniques were earlier tested on Space Cast 2020 project by the US Air Force. The factors which underpin this methodology are the "*India's World View*", "*American World View*", "*ΔTek*" and the "*World Power Grid*". These are the driving vectors for decisions on programs of this magnitude. The underlining meanings of these terms are as follows [4,5,11,12,13].

- "*India's World View*" is its perspective of the world and its willingness and capability to interact, and will range from domestic to global.
- "*American World View*" is the perspective on the world and its intent and capability to interact globally and ranges from domestic to global. However in practical terms "*India's World View*" is a subset of "*American World View*" in range, scale and depth. This is the reason for applying the US Air Force 2025 methodology in this research.
- "*ΔTek*" is the differential in the rate of economic growth and proliferation of technology, ranging from constrained to exponential.
- "*World Power Grid*" is the generation, distribution and control of political, economic and military power across the globe, which ranges between concentrated and dispersed.

This methodology gave rise to guiding factors viz. economic interest, technology dominance, low intensity threat, regional dominance, economic parity etc. The resultant assessments narrowed down to the necessity and relevance to create IW Capability with outlines of major national programs already underway in defense, food, technology, infrastructure etc in our country.

1.6.2 Methodology for IW Framework & Blue Print

Another methodology from the Mitretek Systems presented by Robert J Clerman [80], was examined and adopted. The steps followed to undertake research in consonance with this methodology for evolving the national IW Framework and Blue Print are as follows:

- Basic Functions and Issues of NII Security, figure 1.2

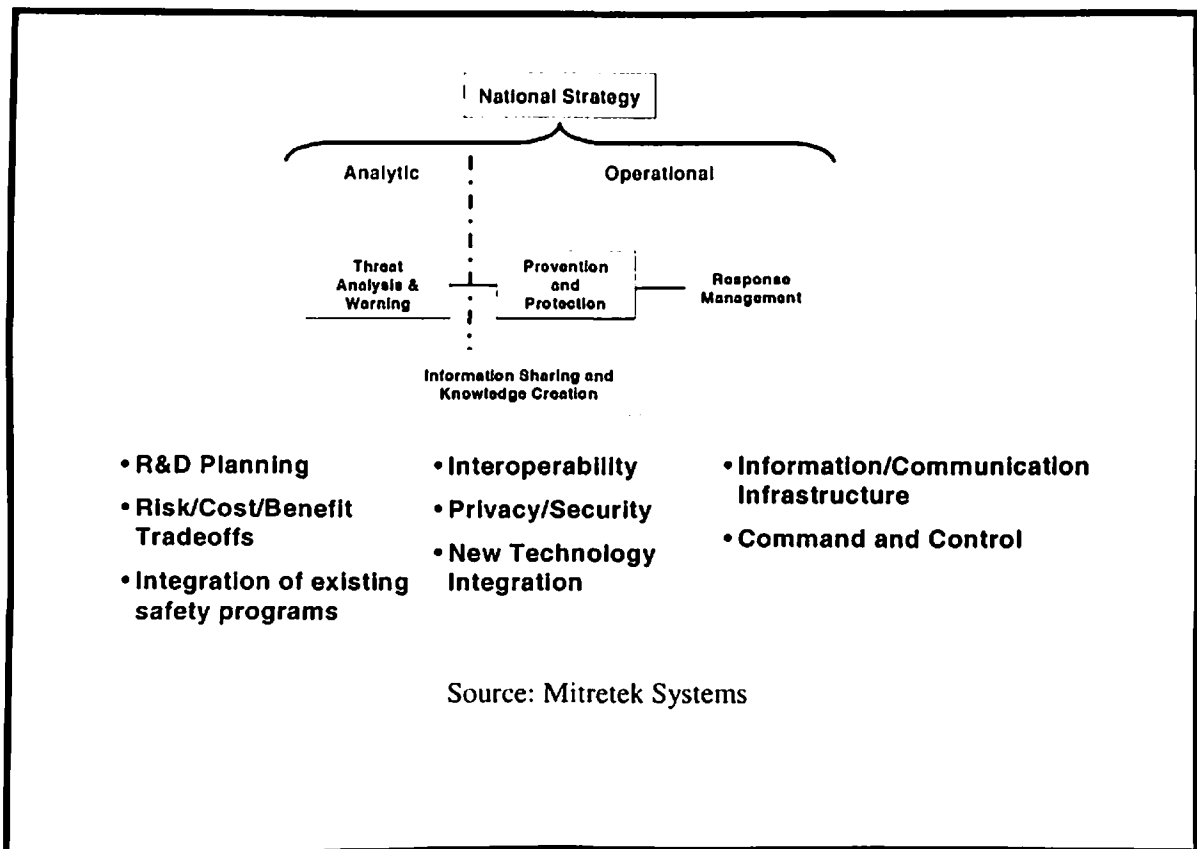


Figure 1-2 Basic Functions and Issues of NII Security

- National Strategy to Secure the NII, figure 1.3

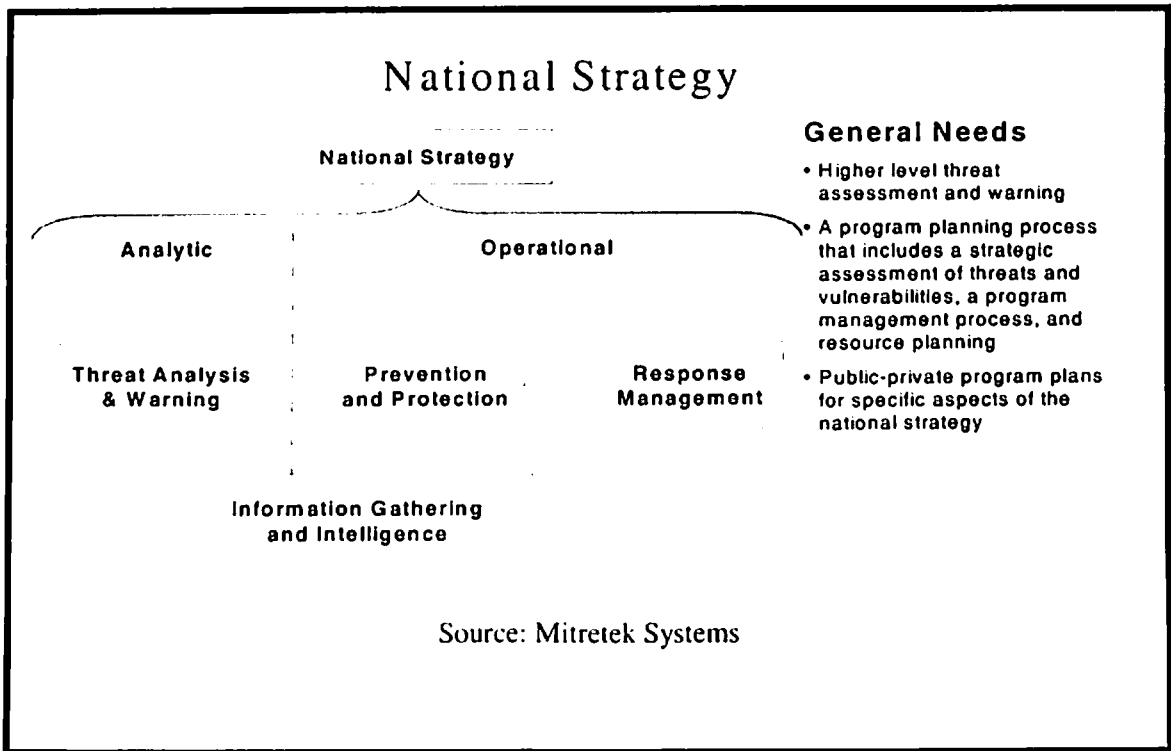


Figure 1.3 National Strategy to Secure the NII

- Threat Analysis and Warning, figure 1.4.

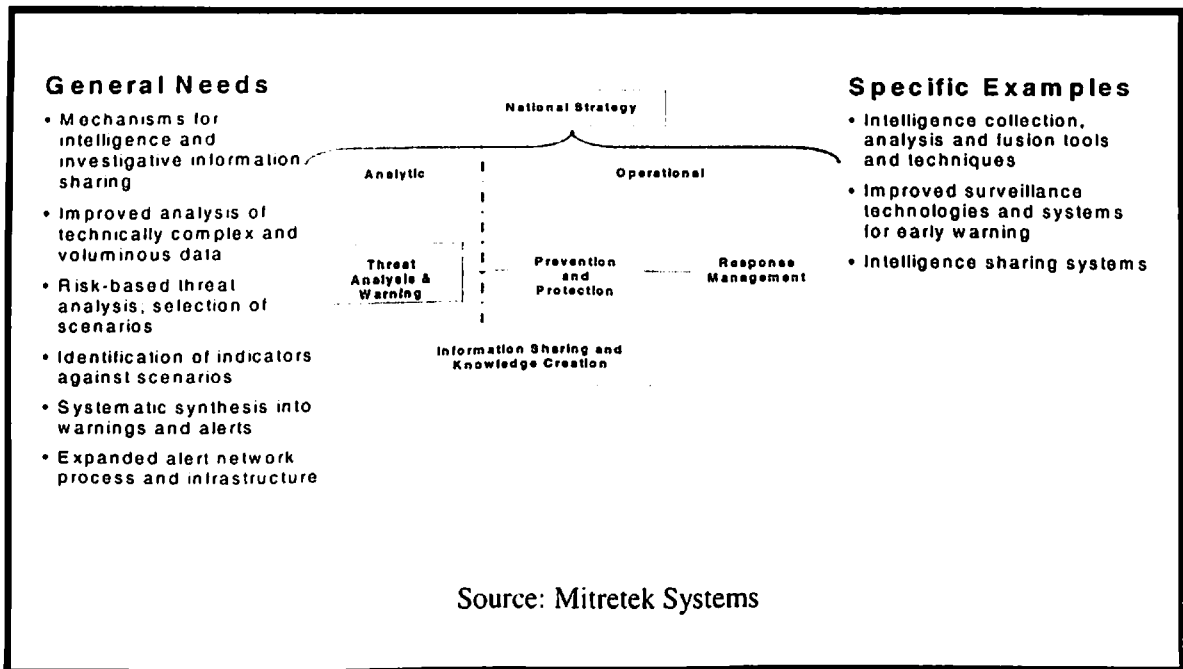


Figure 1.4 : Threat Analysis & Warning

- Prevention and protection techniques, technology and methods, Figure 1.5.

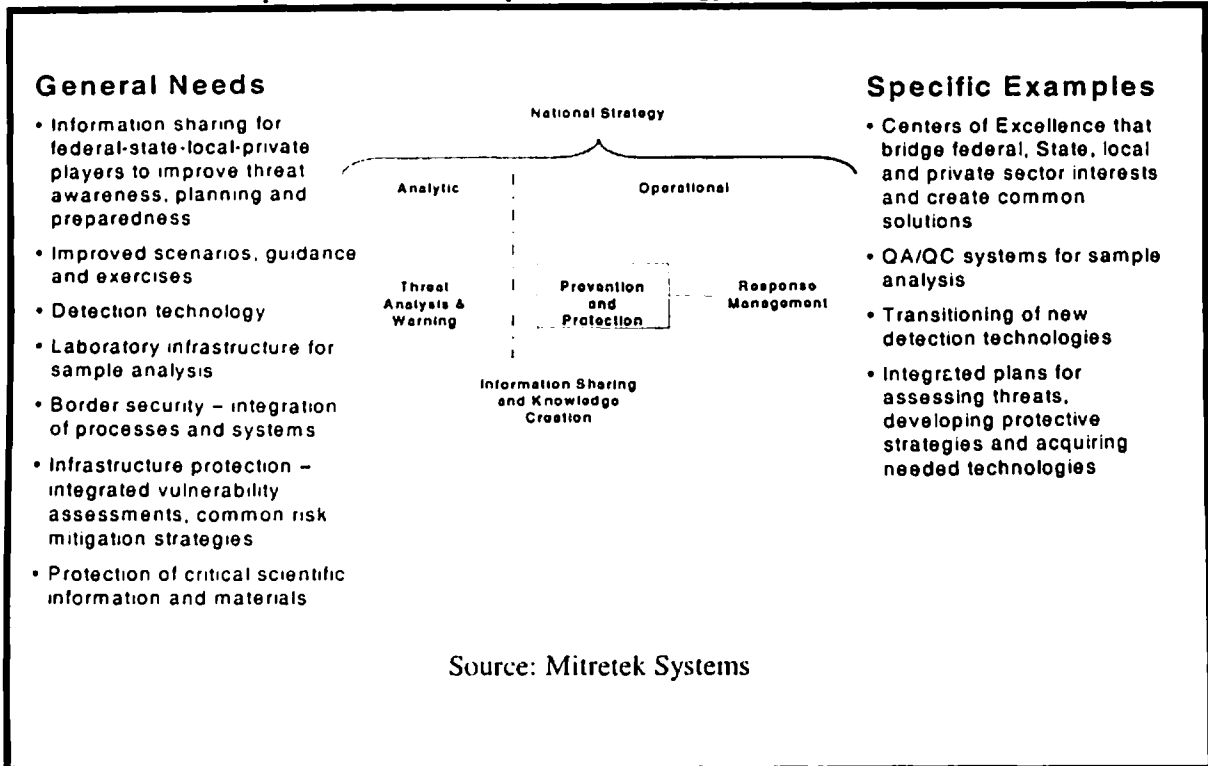


Figure 1.5 : Prevention & Protection

- Steps for Information Sharing and knowledge creation, figure 1.6.

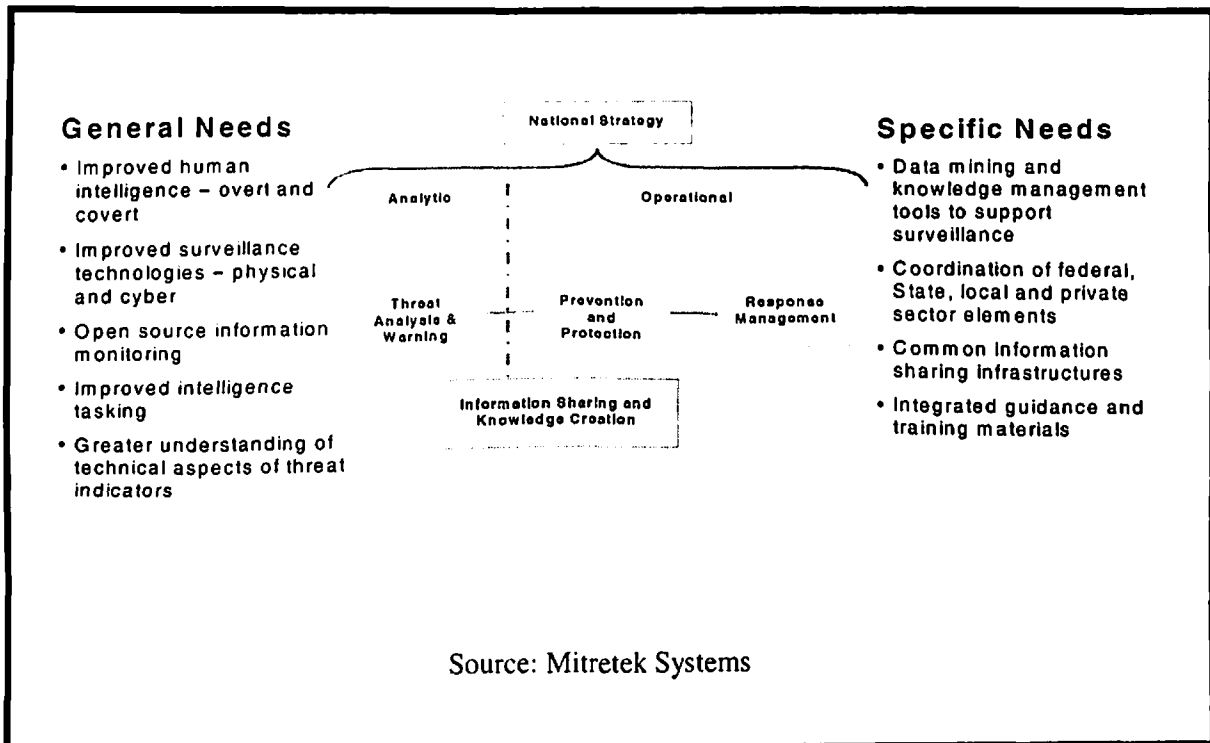


Figure 1.6 : Information & Knowledge Creation

- Response Monitoring and Management, figure 1.7.

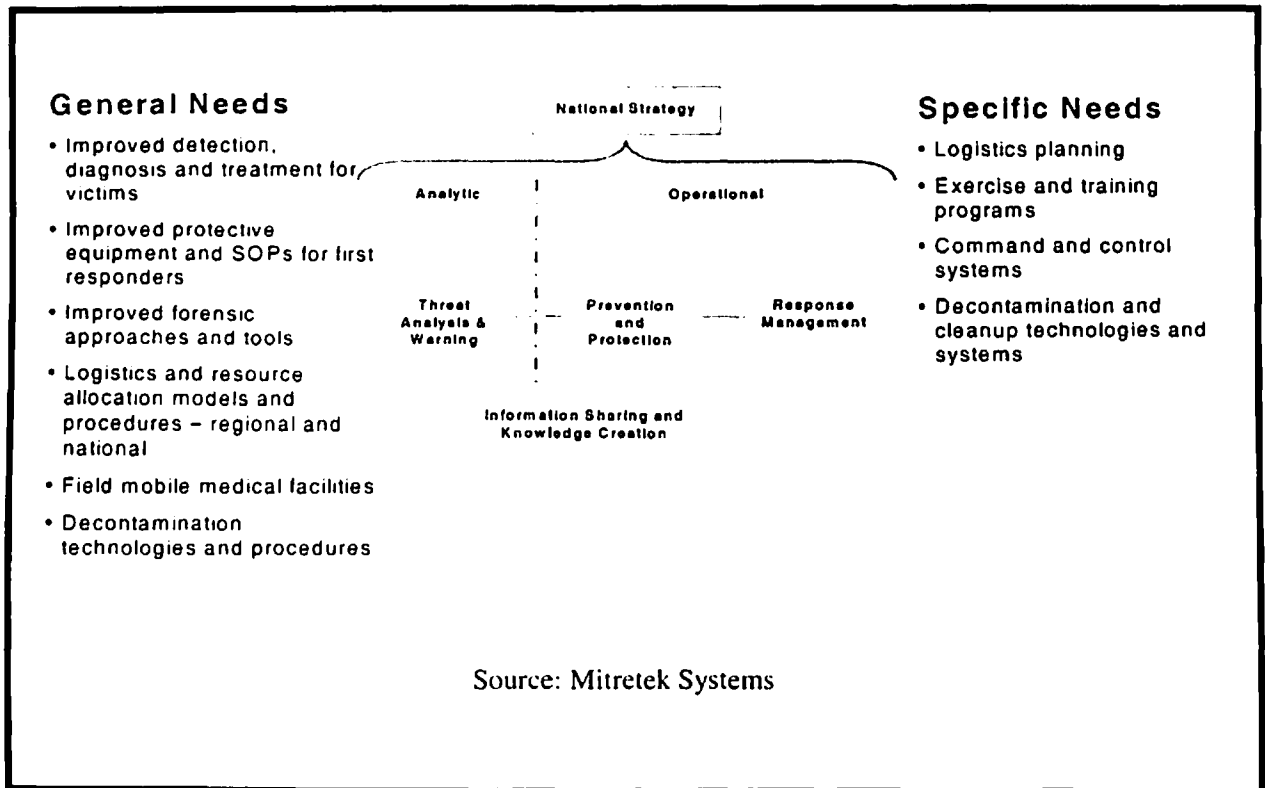


Figure 1.7: Response Management

1.6.3 Study of IW Initiatives Overseas:

USA, Australia, and Europe have taken lead in underpinning CNIs with credible and secure NIIs. Following initiatives of USA have been examined.

- Steps and Timeline for NIAP activities, Figure 1.8 [46].

June 2002	Homeland Security Act introduced PCCIP established
July 1997	Stanford/LLNL Workshop: Setting the Agenda
Oct 1997	PCCIP Report Issued
Feb 1998	Stanford/LLNL Workshop: Next Steps National Infrastructure Protection Center (NIPC) established within the FBI
May 1998	Presidential Decision Directive 63 (PDD-63) establishes the Critical Infrastructure Assurance Office (CIAO) within Department of Commerce
Sept 2001	Terrorist attacks on WTC, Pentagon
Oct 2001	White House Office of Homeland Security

Source:alderd@stanford.edu

- National level Organization for Critical Infrastructure Protection interns of Presidential directive DDD63, figure 1.9 [52].

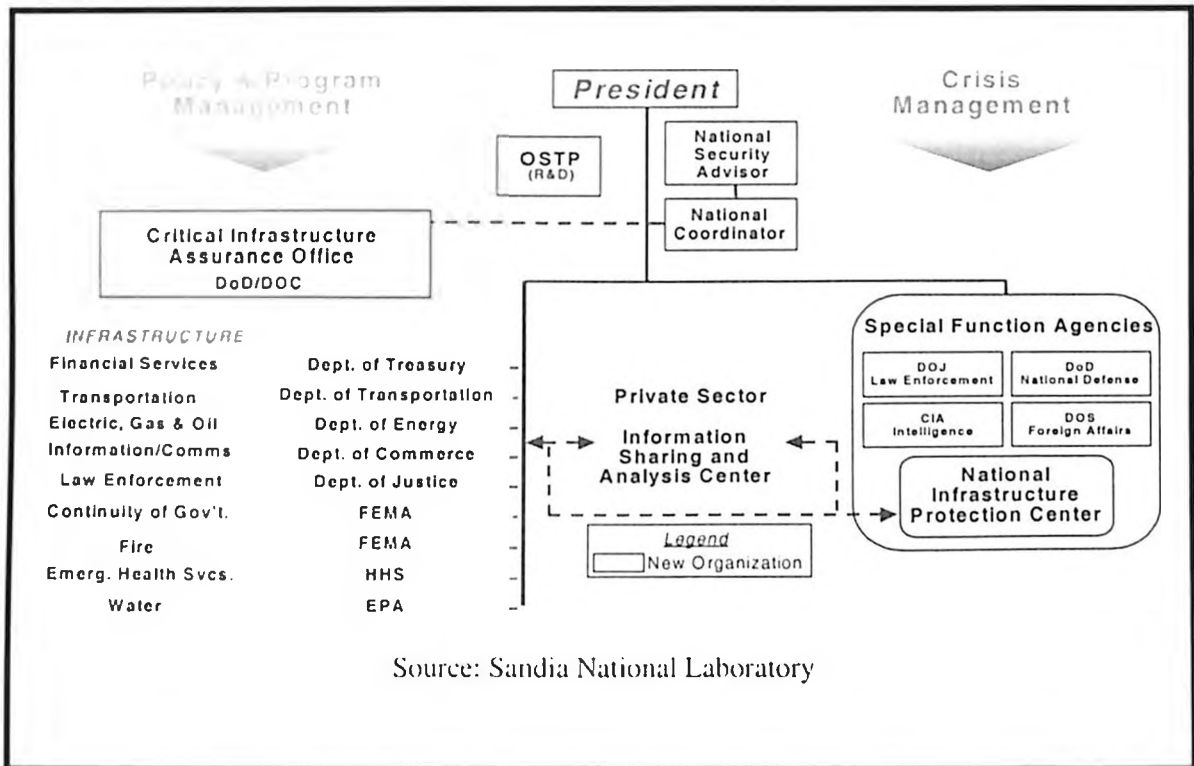


Figure 1.9: National Organisation for Critical Infrastructure Protection.

- National Security Committees and Working Groups figure, 1.10 [152].

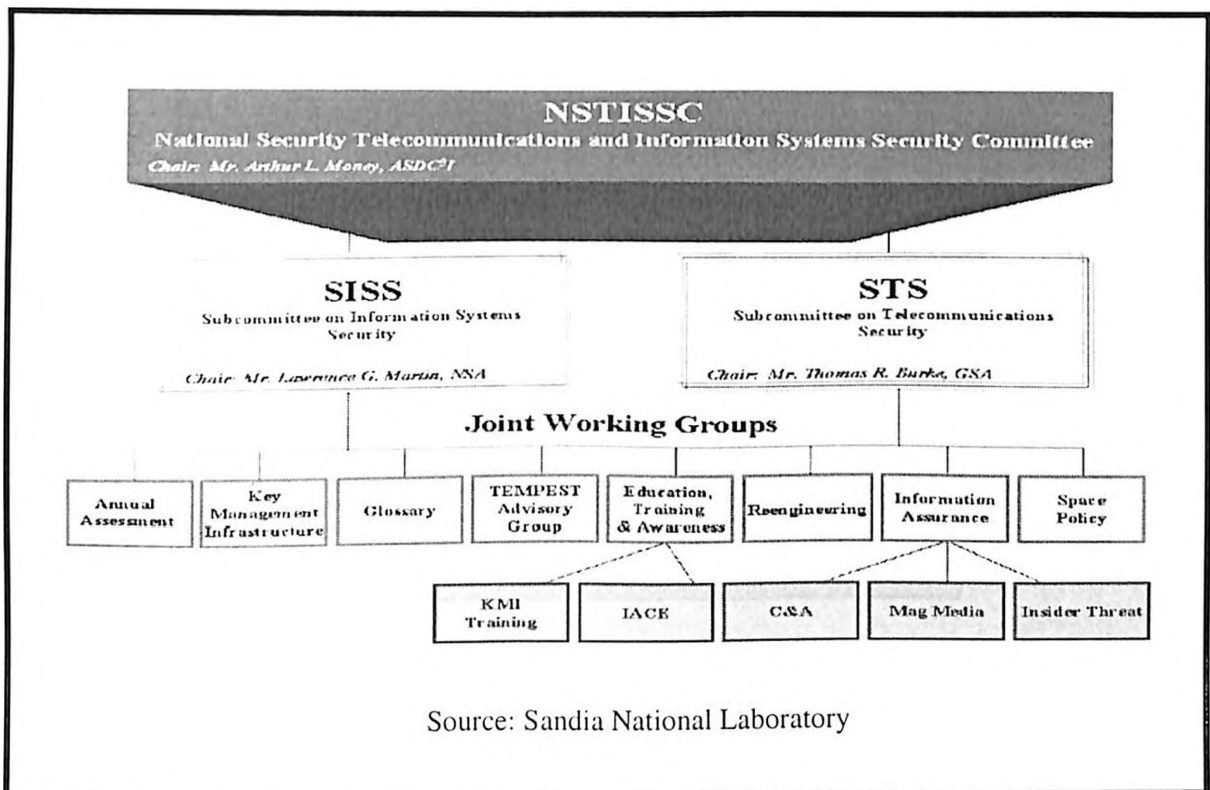


Figure 1.10: NSTISSC Structure

- IW Solution Components, figure 1.11 [98]

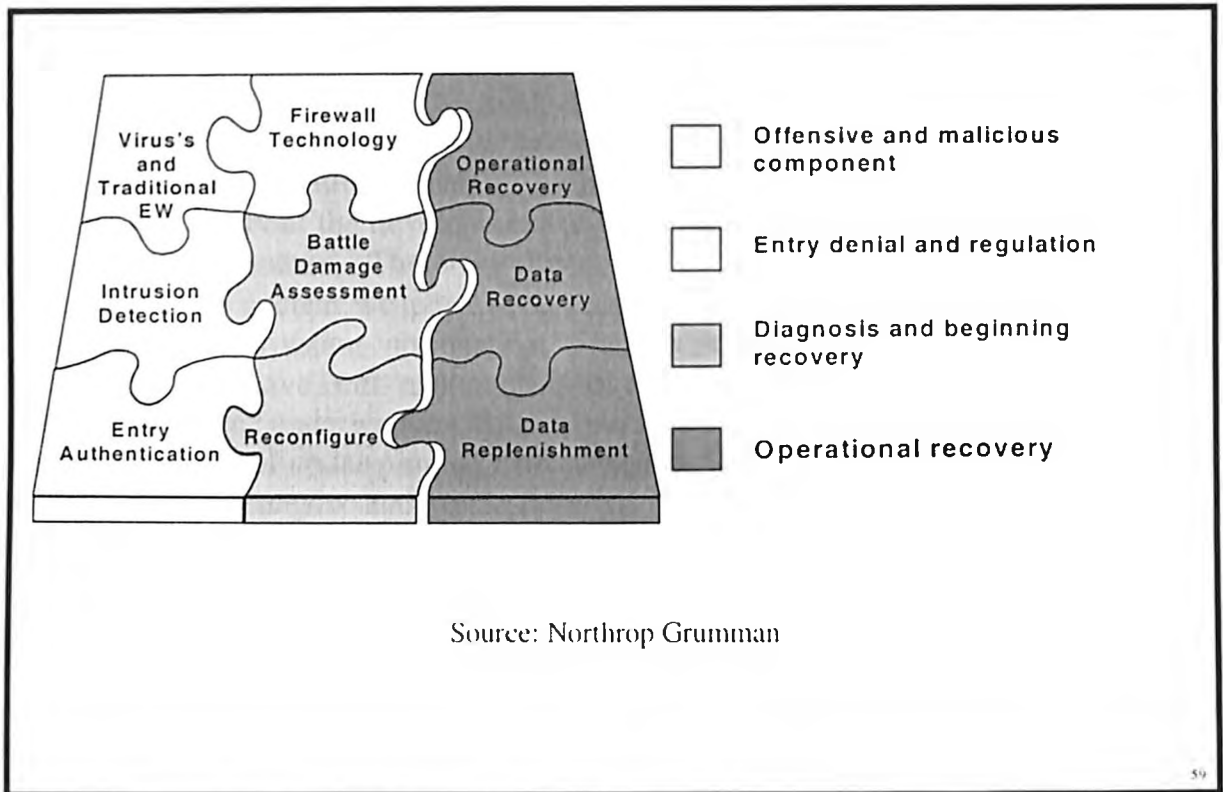


Figure 1.11: A Complete IW Solution: Interlocking, Cooperative, Tailored and Includes Recovery)

- Defense Information Infrastructure Security Overlay, figure 1.12, [125].

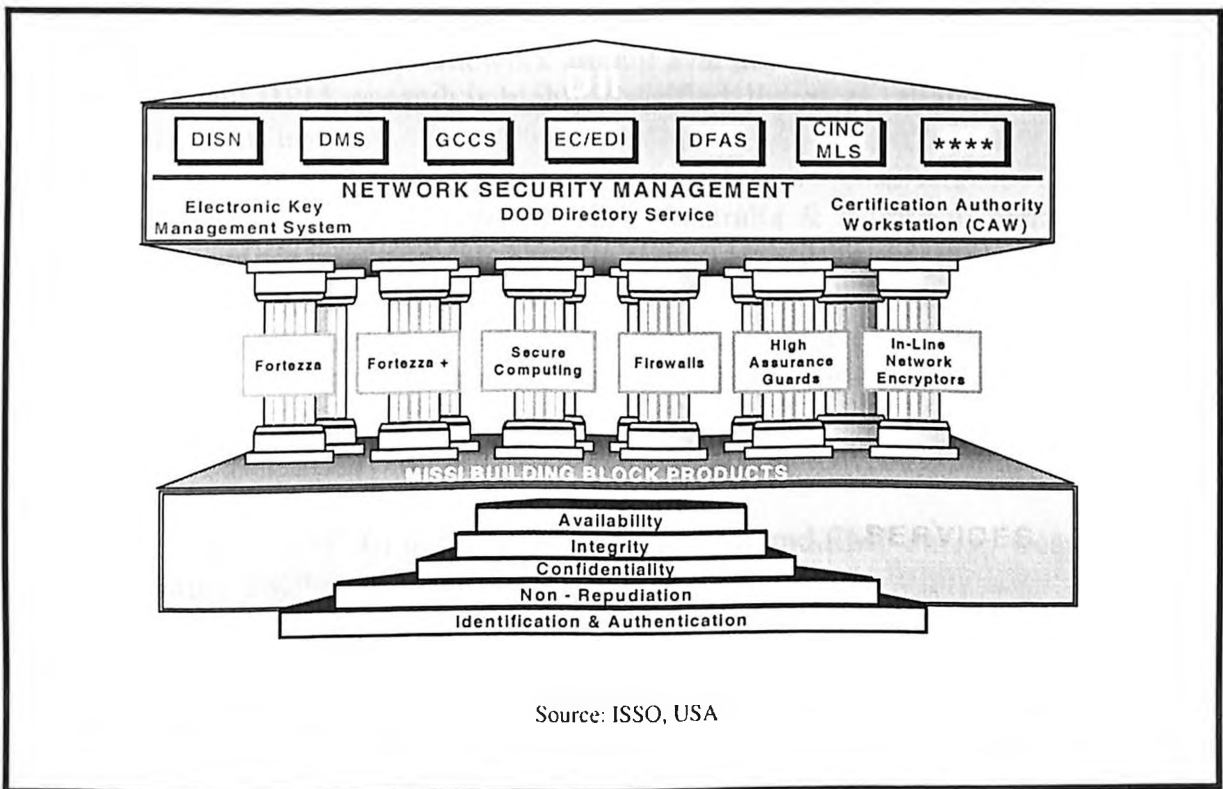


Figure 1.12: US Defense Information Infrastructure Security Overlay

1.6.4 Approach to Analysis

The NII underpinning the critical infrastructures in India is at a nascent stage due to slow pace of IT penetration. The threats and vulnerabilities of IT in the context of NII are still not obvious and understood. Therefore NIIs of developed nations and their threats and vulnerabilities from IW perspective have been examined and related to the emerging national security threats to India in the context of IW. As brought out above, very few issues about the development of EMP and HPM energy weapons are described in the open literature. Therefore historical background of Electromagnetic Pulse generation from nuclear weapons tests, research efforts to develop electromagnetics for generation of equivalent non-nuclear EMP, effects of high power microwaves on microelectronics have been examined from a military perspective, with available inputs from IW programs underway in USA.

The analysis of NII under pinning critical national infrastructures, vulnerabilities of NII to IW attacks, strengths and weaknesses of informational weapons, vulnerabilities of microelectronics to EMP and HPM energy, relating EM energy to a weapon like role, conceiving these devices as Weapons of Electrical Mass Destruction, their reaction times comparable to speed of light etc. have been undertaken through systematic examination of comparable events around the globe. These have been supported by data and references. No formal tools for data processing have been used. The gist of analysis is as follows:-

- **Background**
 - India's NII, IT penetration in the CNIs is still at a very nascent stage and very scantily documented.
 - IW threats & vulnerabilities are not obvious to, and, understood by the planners and decision makers.
 - Inputs to evolve IW framework are not available in the country.
 - EMP and HPM research is highly classified, therefore reliance has been on open sources of literature.
- **Approach**
 - NII, NIAP & IW programs of USA, Australia & European nations have been examined for guidance
- **National Security & Military Perspective:** Following have been examined
 - EMP tests results from nuclear detonations conducted by the USA in 60s
 - Research efforts underway on Electromagnetics to generate non-nuclear EMP,
 - Effects of EMP and HPM Energy on micro-electronics
- **Analysis Undertaken**
 - Dependencies of NII underpinning CNIs,
 - Vulnerability of NII to IW attacks using HPM and EMP energy weapons,
 - Relating EMP and HPM devices to a weapon's role,
 - Conceptualizing HPM as WMED
 - Preparing wish list for national IW capability
 - Technology development, production, doctrine, combat model, deployment
 - Future course of research
- **Presentation of Work**
 - Collection, collation, analysis, inferences and conclusions have been referenced.
 - Each phase of the study/ research work has been documented chapter wise.

1.6.5 Research Inputs

In India the Defense Research is confined to laboratories of Defense Research and Development Organization (DRDO), Department of Atomic Energy (DAE), Indian Space Research Organization, Armed Forces, Defense Public Sector Units, few institutions viz. TIFR, IISc, IITs and a few industries in the private sector. These agencies are mostly owned by the government and seldom share details with outside research community. Specific requests for project details viz. technology, budgeting, overseas tie-ups, induction plans are also not entertained by these agencies under the pretext of classified information. Even their publications are restricted to internal circulation.

On the other hand, agencies in the Department of Defense, USA share unclassified information more openly through Internet and other means. However most details pertaining to EM weapons, which are the focal point of this research thesis, are highly classified and are not available even in USA. For the purposes of this research, most of the inputs have been gleaned from open literature, Internet, informal contacts with researchers and personal knowledge of the subject. References to classified documents have been avoided. However inputs and inferences, which have bearing on the development of technology, system engineering, protection approach, doctrines etc. have been presented based on a life cycle approach of major programs for national security. The life cycle approach has also been adopted keeping in view the social, economic, political and military considerations driven by the history, technology forecasting, assessment, conceptual framework, development, delivery and deployment. The EM weapons program will be comparable in volume, complexity and technology diversity to the Integrated Guided Missile Development Program (IGMDP) of India, under which 5 variants viz Naag, Akash, Trishul, Prithvi and Agni missiles are being developed. The methodology followed to conduct the research has been mapped to IGMDP type of initiatives. This involved investigation of ideas, origin of EMP, basic sciences applicable to Electromagnetics, development and integration of technologies, operational IW blue print in the foreseeable future, national strengths in software and robust industrial base for simulation and virtual prototyping etc. Following steps have been followed.

- **Research Inputs Types and Origin**
 - Literature survey
 - Interaction with experts
 - Personal know-how & experience
 - Involvement in RD&D programs
 - Research inputs of from DRDO, DAE, ISRO & Armed Forces on research, technology, budgets, tie-ups, induction plans etc. are very limited.
- **Interaction with experts based on personal involvement in the following.**
 - Author: Navy and National C4ISR Concept Definition Document.
 - Program Manager: Navy Command & Control Systems Development.
 - Program Director: Navy's IW Initiatives.
 - Member: Prime Minister's National IT Task Force.
 - Member: Defense-Industry IT Task Force.
 - Member: Working Group on National RD&D in IT.
 - Founder: Information Assurance Laboratory.

- **Some of the details personally known to me are classified and therefore have not been referenced.**
- **EMP / HPM weapons research is highly classified, therefore inputs through following personal interaction have been obtained.**
 - US universities visited: CMU, Stanford, Texas, Michigan, Perdue.
 - Information security related associations visited: Sans Security Training Institute. Washington, USA, Association of Fraud Examiners (ACFE), USA International Information System Security Consultancy Consortium (ISC2), USA Disaster Recovery Institute International (DRII) Washington, USA, Information Security Audit and Control Association (ISACA), USA.
 - Societies / Labs visited: JAWS Technologies, Canada.
- **Methodology Benchmarks**
 - National awareness of the NII underpinning CNIs.
 - IW framework & blue print of Western countries.
 - RD & D needs of EMP & HPM weapons program of USA, Russia and China.
 - Technology development & system engineering life cycles of major systems.
 - Production, induction, deployment & support life cycles of major military programs.
- **Literature Survey as described in the succeeding sections.**
- **Program level references within and outside India.**
 - Integrated Guided Missile Development Program, India
 - Advanced Technology Vehicle Project (ATVP), India
 - National Information Assurance Program (NIAP), USA
 - Directed Energy Weapons Program (DEW), USA
 - National Information Infrastructure Initiatives, USA, Australia and India.

1.7 Literature Survey

The IW threats have emerged and have been recognized only in 1980s. Most of the development work in EM weapons is underway in Russia, USA and some of the European countries. On the other hand the information and expertise pertaining to security technologies viz. identification, authentication and access control technologies, Public Key Infrastructure, firewalls, Intrusion detection, malicious code management etc. is available through internet, books and other open literature in the industry, and institutions. However information on EM energy weapons is highly classified and is not available in the open literature. This thesis work has been compiled from information available on the Internet, testimonies of senior scientists and functionaries before various committees, program plans of defense contractors in the USA etc. A brief overview of important references is as follows:

- **Literature Addressing NII Initiatives of India.**
 - India IT Vision 2010 : Action Plan, GoI Report, May 1998 [53].
 - Information Technology for Masses, GoI Report, Jul 2000 [100].
 - GoAP e-Governance IT Architecture, Specification, Aug 2001 [85].
 - IT Action Plan (Parts 1,2,3) - National IT Task Force, GoI Reports, Jul 1998-Apr 1999 [103,104,105].

- Conceptual and Architectural Framework for Networking Components, WESEE Report, Aug 1999 [N.A].
- Navy & National C⁴ISR Architecture, WESEE, Ministry of Defence Report, Aug 1996 [32].
- Asian Security in 21st century, Jasjit Singh, IDSA, Oct 1999 [110].
- Information Age & India, Akshay Joshi, NSC, Apr 2001 [15].
- Program complexities of India's Information Infrastructure Security and Information Warfare Initiatives for the year 2000 & Beyond, Arun Saxena & Prem Chand, WESEE, Ministry of Defense Report, Jan 2000 [150].
- **Literature Addressing NII Initiatives Across the Globe.**
 - Architectural Framework for the National Information Infrastructure, Cross Industry Working Team, Report, USA, Mar 1998 [16].
 - Critical Foundations - Report of US President on CNI, Oct 1997 [37].
 - Protecting the Home Land - Report of US Defense Science Board Task Force, March 2001 [152].
 - Security in the Information Age, Joint Economic Committee, US Congress, May 2002 [176].
 - National Strategy to Secure Cyber Space, White House, USA, Report, Feb 2003 [185].
 - Critical Infrastructure Protection and Information Warfare, 2000 [46].
- **Literature Addressing development of EMP & HPM Energy Weapons.**
 - Engineering & Design of Electromagnetic Pulse and Tempest Protection for Facilities, NIST, USA Report of US Defense Science Board on IW- Defense, Nov 1996 [70].
 - Directed High Power RF Energy : Foundation for Next Generation Air Force Weapons, 2002 [48].
 - EMP Bomb - WEMD etc., Carlo Kopp, 3 Publications [39,40,41].
 - High Power Microwaves: Strategic and Operational Implications, AWC, USA 200 [68].
 - Security Implications of High Power Microwave Technology, AE Pevler, IEE Symposium, 1997 [10].
 - Proc. of the 11th IEEE Int. Pulsed Power Conference, Baltimore, USA, 97 [179].
 - Proliferation and Significance of RF Weapons Technology, Statements of Scientists and Senior Functionaries to JEC, US Congress [33,39,193,189].
 - Multi University Research Initiative (MURI), Report on EM Weapons, USA 199 [87].
 - Test and Measurement Program and Facilities [172].
 - High Power RF Weapons [138].
 - Defense Technology Area Plan - Weapons, Air War College, USA, 1998 [45, 88]
 - Measures & Protection Against IW, 1998 [134, 135].
 - The Peoples Republic of China on IW Initiatives [187].
 - Targeting Human with Directed Energy Weapons [60].
 - Research Needs of CIP, 2001 [156].

- Research Efforts at Stanford University, Air Force Research Laboratory, Industry [28, 51,91,94].
- Simulation and Virtual Prototyping of EM Weapons [58,167].

1.8 Developing EM Weapons Capability: Justification for Research

Against the above background, the development of EM weapons as a deterrent capability along with a credible EM protection capability for NII is the most pressing need for India to survive and sustain in the cyber space of foreseeable 15 to 20 years. This is the most significant national security and economic concern, and, has therefore been identified as the primary focus of research. The factors in support of this decision are as follows:-

- India's NII is still at its blue print stage. Bolting down security and protection as an after thought is not a preferred way to address this issue. It needs to be built-in from foundation on ward.
- Concerns about Information Warfare, Non-Lethal Weapons, Cyber War and Cyber Space security are being discussed by various national agencies. However there is no formal National Information Assurance Program (NIAP) yet in place to address them.
- EM weapons can incapacitate that entire NII thereby bringing work in banks, industry, airlines, railways, shipping, defense, industry, hospitals etc. to a grinding halt. This damage potential of these weapons has not yet been recognized by the concerned agencies, primarily due to lack of exposure to this field.
- India is known to be nuclear capable. However there is no visible sign of evolving protection strategies for NII against EMP in the event of a nuclear exchange or accidental detonations. This inaction is also primarily due to lack of awareness.
- The country has an ambitious self-reliance program underway to develop military capability. However there is an inherent lag in its RD&D delivery capability as is evident from media reports about Light Combat Aircraft (LCA), Advanced Light Helicopter (ALH), Main Battle Tank (MBT), and Integrated Guided Missile Defense Program (IGMDP) programs. The EM weapons program is not yet even known to be on our blue print. In the past, this lag in our RD&D efforts has often compelled the Armed Forces to meet their operational needs through import at very high cost. In case of EM weapons, even if their import is sought, it is very unlikely that many countries will be keen to sell them to India due to their deterrence potential being equated to nuclear weapons. There is already a move amongst Russia and Western nations to control the proliferation of EM weapons technology on the lines of nuclear weapons. Therefore there is no option for us but to develop EM weapons capability indigenously with requisite external help.
- The serious development of EM weapons in the west commenced in 80s. They are likely to be inducted into operational service by USA, its allies and Russia in 5 to 7 years. With concerted efforts, India can catch up in the development of these weapons and avoid disparity as well as import at very high price under unreasonable restrictions.
- The physics of Electromagnetics is developed and well understood. The emergence of virtual simulation has made technology development comparatively easier. India has computing resources, scientific temper, and software expertise to support

development of EM capability. These strengths can also be leveraged to enter into strategic partnerships with friendly countries to collaborate in the EM weapons development program. This is one area in which the country has potential to develop and maintain parity with the world leaders and earn substantial foreign exchange.

1.9 Research Objectives & My Contribution

The terms "Information Warfare"; "Netwar", and "Cyberwar" appeared in literature in early 90s. The serious work in the EM weapons areas as a component of Information Warfare is still confined to USA, Russia, China, Ukraine and Israel. In India despite attempts amongst the DRDO and Armed Forces, no formal framework and blueprint for development of IW capability in the country has yet been evolved. The basic reason for this inability at national level efforts is due to the lack of precedence, lack of understanding and expertise at middle and senior level personnel of the complex and diverse basic sciences applicable to Electromagnetics, mathematical complexities of designing high power microwave systems, complexities of virtual prototyping and simulation, inability to relate operational objectives to directed energy weapons, system engineering, instrumentation and packaging technologies. In this context the IW weapons program in India has been a non-starter.

I have been involved in the definition and development of IT embedded real time systems for the Navy since 1978. During this period I have been directly responsible to evolve Navy and National C⁺ISR architecture, design of ship borne command & control systems, design of submarine combat systems and development of the security overlay for Navy's Information Infrastructure in terms of encryption devices, firewalls, intrusion detection systems etc. This involvement and continuity has helped me to understand the complexities of modern information infrastructures and their vulnerabilities to Information Warfare involving EM energy weapons.

My contribution therefore has been to provide **"Thought leadership to the Armed Force, research community and industry for a potential multi-billion rupees RD&D program, aimed at early leadership role for India amongst the proponents of Information Warfare, possession of deterrence status by India as an IW weapon power, immense earning potential through export of EM weapons and cross fertilization of expertise across a wide spectrum of scientific and technological fields in civil sector to leverage spin-offs of these technologies "**.

The EM weapons program of DOD, USA has roots in the development of Directed Energy Weapons as part of the Star Wars program of President Regan's era to neutralize Soviet missiles. On similar lines, the National Information Assurance Program (NIAP) of USA has roots in the protection of National Critical Infrastructures against cyber war attacks. In this thesis I have presented a layered and as integrated approach to build IW-Defense and IW-offence capability. The EM weapons component of the IW capability presents unprecedented scientific, technological, operational and management challenges. I have presented a blue print to address them keeping in view the strengths and weakness of our country. My contribution in specific terms is as follows:

- **Identification of IW Threat to National Security.**
 - Critical National Infrastructures (CNIs) sustaining our social, political, economic, military operations and governance have been identified.

- Their interdependencies amongst themselves have been identified and articulated.
- NII components (including CII, DII, GNII) underpinning CNIs have been identified.
- NII threats & vulnerabilities from Info War, Net War and Cyber War perspective have examined and mapped to National Security Needs of Digital Age India.
- Potential of EMP and HPM as Weapons of Electrical Mass Destruction & Deterrence has been examined.
- Comparable NII, NIAP, IW-D, DEW initiatives of USA, Russia & China have been examined.
- **National IW Framework and Blue Print has been suggested. An organizational structure for research, and development has been proposed.**
- **IW program needs in terms of the following have been defined.**
 - Know-how
 - Basic research
 - Technology development
 - System development & engineering
 - Tests & evaluation
 - Production & deployment
- **IW Operations in terms of the following have been conceptualized.**
 - Armed Forces needs
 - Operational doctrines
 - Combat model
 - Integration with conventional weapons
 - Protection strategies & civil defense
- **Following core Research Design and Development areas have been identified.**
 - Basic research in pulsed power, storage, shaping, transmission, measurements, accelerator structure, advanced beam concepts, collective effects, HPM, vircators, wave oscillators, fast wave gyros, plasma filled devices.
 - Technology development for HPM sources (MHz - GHz frequency, MW - GW power). compact high power modules, high gain, UWB antennae systems, compact, efficient, high pulsed power drives.
 - Assessment of HPM effects & lethality pertaining to RF testing of crucial military assets counter measure techniques, biological effects, civil, defense Issues.
 - Integration with military programs such as IGMDP, C⁴ISR, UAVs.
 - Protection Program comprising of EMP Hardening, Susceptibilities Studies, Components, Systems and Platform Protection.
 - Development of EM military posture encompassing surveillance & defense, counter proliferation, counter-munitions.
 - Integrated follow-on efforts for technology demonstration, system level developments, testing & evaluation, tactics and doctrines, combat modeling.

It is perceived that these issues have not yet been addressed in the country under any national level formal project or program.

1.9.1 Potential End Users of this Research

The thesis have the potential for use as follows:-

- Reference framework for Ministry of Communication and Information Technology to evolve and implement National Information Assurance Program for protection of critical NII.
- Blue Print for development of Information Warfare capability built around EMP and HPM energy weapons. This would concern National Security Council, Ministries of Home Affairs, Finance, Defense and MCIT and the industry.
- Compiled information resource for institutions, DRDO, DAE, Armed Forces and the research community in national institutions.

1.9.2 Globality of the Research

The objectives of the research have also been to bring the globality of security issues into focus. This is aimed to highlight that we would require collective will and wisdom of academia, industry, and government to address these issues comprehensively. The outlines of this work have been presented separately in the following papers, but not included in the thesis [150].

- Issues of Cyber Space Transition and Security.
- Development of NII Security Framework.
- Developing Information Warfare Troops.
- Research Needs for NII Security overlay.
- Protection of Critical Infrastructure: Need for National Initiatives

1.9.3 Motivation for the Research

The primary motivation to undertake this research came from the following factors.

- As Additional Director General, Weapons and Electronics System Engineering Establishment (WESEE), Ministry of Defense, I have been the Program Director responsible for development of Naval Computerized, Command, Control, Communications, Intelligence, Interoperability Recon science (C4I2SR) and Information Warfare Programs. I am also the co-author of "National C4I2SR Concept Definition, Architecture and Configuration" document. The involvement and understanding of this work had urged me to write a document titled, "Program Complexities of India's Information Infrastructure Security and Information Warfare Initiatives for the Year 2000 and Beyond", a 10 volume piece of work.
- As member of the Prime Minister's National Task Force on IT and Software Development, I had the opportunity to examine some of the technology and security issues concerning the NII security and their impact on the industry to enter into global IT business.
- The university research community, DRDO, MCIT and the Armed Forces are not yet addressing NII security issues of this nature in a coherent manner. This low-level interest and concern is primarily due to lack of exposure on the part of concerned agencies. The idea therefore is to consolidate all issues and document them under this research work. This thesis can then form a baseline for future work. The approach and strategy evolved in this thesis has the potential to create scientific,

technological and economic value, which usually are the driving vectors for high-end research programs at national level.

- The timely development of national capability in Information Warfare, with prime emphasis on EM weapons can place the country amongst the select few, who would own a deterrence capability in the most vulnerable emerging cyber space. Besides, it will save the country billions of rupees in foreign exchange needed for the import of IW weapons in the most stringently controlled market.
- The work is an effort to present to the concerned agencies, a window of opportunity for developing IW capability around EM energy weapons, for which most of the basic ingredients exist in the country.

The above issues have been the primary motivation to nucleate a research community in the country to address this extremely vital issue of national security and economy in this digital age.

1.9.4 Limitations of Research Work

A large part of the contents of the thesis have been gleaned from open literature. Their application to Indian context for program related decision making and investments would require far more deeper research into concepts, technologies, Indian ambience, geo-politics, national security perceptions and priorities, political, religious, regional, legal, system engineering, organizational interface within and out side the government as well as classical research inputs (in their native sense viz. behavior, culture, literacy, work ethics, attitudes, religious beliefs, privacy, socio-economic, techno-economic, legal, educational etc.), since some issues involve a paradigm shift in our national precepts.

Secure National Information Infrastructure, Information Warfare, sovereignty over our native efforts in IT development, its consequential economic benefits and military superiority, constitutional bearing on our emerging information society, compliance to IT Act 2000, national civil defense in electronics etc., are issues of enormous significance to our survivability and sustenance in native, national or global sense. They must be examined and addressed by suitable people in civil and the military at the highest level.

Following issues though closely linked to the NII security have not been examined in detail.

- Security in the information age is explicitly or implicitly interwoven with constitutional and sovereign rights and privileges of all citizens and the importance of addressing them as a part of building the NII security foundation. Linking and addressing these security issues, as part of NII security is an area of intensive research covering social, economic, political and military domains and requires national level focus and investment by all sections of the society. Thesis has only given a brief account of these issues.
- The emergence of microelectronics has led to design of high performance systems. The performance edge in terms of faster and accurate response emanates from embedded intelligence in these systems, which has proliferated into almost every facet of systems of civil and military significance. Therefore, technologically advanced nations have produced platforms, weapon systems, delivery systems,

command and control infrastructure which can provide them overwhelming superiority almost instantaneously in terms of detection of targets, location and targeting in any part of the globe, underwater, on surface or in space. This has been clearly demonstrated in the current war in Iraq. Amongst these, a new breed of systems is emerging under the name of "Non-Lethal Weapons" or "Disabling Systems". Classes of these non-lethal weapons with computers as their basic building blocks have also been termed as IW Weapons, which are aimed to disable, damage, destroy or render enemy systems ineffective through the use of Information Technology (IT). This area requires separate and far deeper research, and therefore has not been addressed in this thesis.

- There can be situations when some countries may not share common political, social, economic or military interests with India. They may utilize their overwhelming superiority in EM energy weapons against us to extract any advantage of political, regional or economic significance. Even the non-lethal use of these assets would assume "deterrence value" hitherto possible only with nuclear weapons. Today, we have virtually no defense against them. As the IW technology advances further, this gap is bound to become wider. Therefore this issue needs careful examination from the point of view of technology control and denial. This area has not been addressed in the thesis. Also as a nuclear weapons state, there is a need to research deeper as to what strategic national security objectives can be addressed through non-lethal EM energy weapons and where to use our nuclear options.
- The war objectives of our adversaries and their allies may not be emanating into World War type of destruction, but it would emerge into a different type of cold war on the strength of EM energy weapons. Considering the emerging geopolitical situation, we can become the target nation because of very large economic potential of this region. The level and potential of vulnerability of NII to EM energy weapons may not be yet very apparent because such "Disabling Techniques" are yet being evolved and have not become "Disabling Systems" as part of warfare establishment. This issue needs to be examined in the context of cyber terrorism and has not been addressed in the thesis.
- The research signifies the need for development of security framework for protection of NII, which would supplement the IW capability. These issues have been examined in the form of security framework objectives, NII security goals, gaps in existing security overlay, national information security policy, policy research in information operations, segment specific security solutions, professional practices, security products and services, security management system and training. Another framework for development and deployment of IW troops for Counter Virus Counter Measures (CVCM) has been outlined. This addresses the need for offensive and defensive capability and role, expertise and requirements in hacking the communication systems, cellular phones, smart/ credit cards, teller machines, radio devices, satellite systems etc. It also describes attack strategies, planning, training, organization and deployment of IW troops, their cost and constraints. However these are very complex issues and require separate thrust, which has not been covered in this thesis.

We as a nation appear to be pre-occupied with economic, industrial, social and internal problems. We have not yet recognized our vulnerability to EM energy weapons. The

details of high-end IW weapons are not yet available in the open literature and this limited research effort is unable to comprehend this type of danger. This area warrants wider and bigger research efforts, far beyond what has been addressed in this thesis.

1.10 Structure of the Thesis Document

The thesis has been organized in 10 sections including this chapter, under chapters 1 to 10.

Chapter 2 addresses the NII perspective, its role for national development, and, its promise to the citizens and society. It describes the building blocks of NII in terms of gadgets, content, applications, standards and people. It also examines the critical issues in engineering of NII such as framework of services, universal services concepts, technology, applications, user interface, collaboration, Radio Frequency spectrum management, IPR issues, interagency coordination, online services, information security and network reliability. Amongst the critical issues, "NII Security Perspective and Issues" have been further examined in detail in Chapter 3, so as to identify the areas for research. This chapter describes the Critical National Infrastructures (CNI), their interdependencies on NII, whose IT elements must operate and survive all natural and man made vulnerabilities and threats during peace and war. It also describes the changing role of Critical Infrastructure Protection (CIP), surveys global initiatives for CIP and its funding, surveys the National Information Assurance Program (NAIP) under way in USA, identifies the role and relevance of agencies to make the NII and GII secure, security architecture, inter-dependencies, security goals, security model and a possible security overlay.

It signifies that from an operational perspective, the NII offers a borderless cyber workspace at the level of an individual, an organization, a state, the nation and the globe, where we all as citizens would coexist. This is a paradigm shift from a centuries old well-perfected paper based work environment to an unseen paperless workspace. There are peculiarities of this cyber space, which are linked to security by way of information warfare and secure national information services. These issues are not directly relevant to the focal point of research, they nevertheless have a very strong bearing on the overall security and safety of NII and have been examined.

In chapter 4, the NII security has also been examined from "Information Age Warfare" perspective. It examines the potential of IT to turn into a war winning effort, what is "Cyber War", "Information Warfare", "Net War", maps them into Revolution in Military Affairs (RMA), dimensions of IW in the context of computer as a bare machine, internal and external communications, and, the role of technology in IW. The Chapter 3 examines IW as evolution of IT based warfare in the context of technology, institutions, cultural values, perceptions and methods through the era of industrial and network revolutions. It also examines Information Based Operations (IBO), Information-in-War and Information Age Warfare in the context of Joint vision-2020 of USA, " Network Centric and "System of Systems" approach to military operations, IW survivability and IW risk management strategies.

Chapter 5, titled "Information Warfare Threat Assessment" examines the emerging cyber environment and the impact of IW on it in the socio-political, techno-economic and military - strategic dimensions, the new world information order, its collaborative effect on military, politics, governance and foreign policy. It further examines the IW threat scenario, source and diversity of threats, threat perception and impact of IW in social, political, military and economic terms. It also signifies the emergence of RF and EMP weapons, IW development activity across the globe, range of threats and vulnerabilities, attack tools and their sophistication, their cost and availability. It presents measures to assess, minimize and mitigate threats through organized national efforts. This chapter also outlines possible IW objectives, threat spectrum vis-à-vis our national security and presents IW strategy for India.

The remaining part of the thesis has been devoted to the EM weapons. The chapter 6 titled, "Effects and Vulnerabilities of EM Weapons". It defines EMP, RF and microwave energy, signifies effects of nuclear detonations in terms of radiating fields, their characteristics, effects of EMP on electronic devices, effects of microwave energy on electronics, material and personnel, weaponisation of microwave energy, energy coupling schemes, categorization and frequency ranges of EM weapons and their damage potential, propagation of RF energy as a weapon, potential to damage NII, EM energy weapons for special force and terrorists, EM energy weapons for strategic and military use, evaluation of EMP and HPM energy as weapons of choice, their effectiveness, countermeasures and value as a deterrent.

The Chapter 7 titled "Technology Assessment for Development of EM Weapons", outlines historical background, evolution of high power microwave devices, development of building blocks of EM weapons viz electrically driven devices, explosive driven devices, profile of EM weapons program in USA and other countries, summary of research work, transient electromagnetic devices and their damage potential, live testing, damage potential of RF/Microwave weapons and the emerging directions for development of EM weapons.

Chapter 8 titled "Development of EM Weapons" presents IW threat perception, scope of the IW solution, operational requirements of EM energy weapons as applicable to our Armed Services, objectives, building blocks and technology base needed for EM weapons, construction aspects of power sources, HPM sources, antennae systems, their design and performance features, adaptation of Flux Compression and Magneto Hydrodynamic generators and HPM vircators for EM weapons. This chapter also presents the objectives, timeframes, technology development, NII assurance program for protection against EM weapons, alternate technologies, integration with current military programs in terms of basic research, development of technology, demonstration, test & evaluation, force modernization, weapon system engineering and protection strategy and program.

Chapter 9 titled "Packaging, Induction and Deployment of EM weapons", addresses identification of targets for EM energy weapons, packaging of EM weapons as missiles, bombs, delivery options viz. as cruise missiles, UAVs or aircraft delivered weapons. It

also examines lethality assessment issues interns of influencing factors, voltage levels, constructional limitations, assessment of lethal coverage, kill assessment and monitoring difficulties and surveys measures for lethality enhancement. This chapter also outlines doctrines for use of EM Weapons in electronic combat operations, strategic air attack operations, air defence operations, maritime operations and operations in land battle. It maps the warden's 5 Ring model into NII layers and presents an approach for use of EM weapons against an adversary, as well as protection of our own NII viz. apex nodes concerning national leadership, critical NII nodes for economy and governance, IT and telecom services, media and population. It also examines the enforcement of Technology Control Regime using EM weapons.

Chapter 10 is titled, "Research and Development Needs of the EM Weapons Program". It presents the research, design and development perspective for the EM weapons, surveys global RD&D efforts underway, ranging from basic research in electromagnetic microwave circuits and components, co-axial windows, mode converters, multiple beam devices, multiple beam devices, inductive output tubes, high frequency gyrators, high power switching materials, explosive power generation, breakdown in liquids and solids, electric space propulsion physics and insulators, super efficient high rating power supplies, flux compression generators, high power microwave devices, antenna systems and a large range of software, tools for simulation and virtual prototyping. It presents the volume and complexity of the collaborative programs underway in USA through Multi University Research Initiative (MURI) is collaboration with industry and defense agencies. The chapter signifies that there is a need for a similar national initiative for India to develop IW capability around EM energy weapons. It presents a blue print for India in terms of basic research, technology development and demonstration in immediate, medium and long terms study of HPM effects and lethality, integration with existing programs, tactics and doctrine development, force modernization, protection strategy and framework. It signifies the efforts needed on the part of academia, industry, defense agencies. It also stresses upon the need for entering into strategic tie-ups overseas with friendly nations engaged in similar programs for mutual benefits.

1.11 Conclusion

This research addresses the development of EM energy weapons as a non- lethal IW capability in offensive and defensive role. The following conclusions emerge from this research effort.

- NII is synonymous with, and central to India's survival and sustenance in social, political, economic and, military terms.
- NII is extremely prone to disability, damage, denial of service and destruction by the IW weapons.
- IW is emerging as a new dimension of "Warfare in the Digital Age".
- The IW threat in the form of Net War, Cyber War and Info Warfare exists in three categories viz., "National Security Threat", "Shared Threat to Civil and Military Establishments", and "Local Threat affecting Social, Political, Economic and Military Interests".
- Amongst the IW weapons, the EMP and HPM energy as Weapons of Electrical Mass Destruction, are extremely threatening.

- Building IW capability around EMP & HPM weapons for India is inevitable and unavoidable. It befits India's 21st century political, economic and military needs & posture.
- India possesses critical mass of basic know-how, technology, software based simulation to develop IW capability around EMP and HPM energy weapons.
- A framework and blue print to develop this IW capability has been evolved and presented in this thesis.
- The proposed IW program is crucial for self reliance and will free India from technology control by the West.
- This IW capability will position India in "Power Projection League" with "Deterrence" equated to Nuclear Capability.
- The IW program will enable cross-fertilization in expertise and would result in numerous technology spin-offs across numerous industry segments.
- The program has multi-billion rupees export potential.
- Proposed framework and blue print are "Robust and Risk Free".

This thesis meets the stated objective of:-

"Providing thought leadership to create research, design and development footprint for national security agencies, research community and industry to build Electromagnetic Pulse & High Power Microwave weapons as a principal component of India's Information Warfare capability"

The framework proposed in this thesis compares with other national level initiatives of the past viz.

- Atomic Energy Program
- Indian Space Program
- Integrated Missile Program
- National Food Program

CHAPTER 2: NATIONAL INFORMATION INFRASTRUCTURE PERSPECTIVE

2.1 Introduction

The world today stands focused on the challenges dictated by Information Technology (IT). The survival and sustenance of human race in economic, political, military and social terms has never been so tightly controlled by any technology as the IT. India is also sensitized to this reality. The opening up of the economy and consequent Information & Communications Technology (ICT) boom in the country has also brought global ICT industry players into India. The IT has assumed far more priority than any other area of economy and technology. The IT has been recognized as a vehicle for modernization and growth towards self-reliance by the higher level of management in the country.

Realization of these initiatives has roots in a secure and credible **National Information Infrastructure (NII)**. In this chapter, a policy framework, along with a blue print for the development of NII have been examined. The IT perspective of the country has been viewed in relation to NII, its security and integration with Global Information Infrastructure (GII). Issues of synergy and perceptions of a large number of national agencies, particularly whose products and services have direct bearing on the security of the NII, have been examined. The chapter signifies the scope and promise of the NII and the current status. It also identifies the critical issues, which must be addressed while engineering the NII.

2.2 India's IT Vision - 2010: Action Plan

The Ministry of Communications and Information Technology (MCIT) document "India IT Vision - 2010: Action Plan" has identified 25 thrust areas for implementation in 3 phases as shown in Figure 2.1 [53]. It identifies NII as a principal component for national development.

The national IT vision centers around IT enables, creation of digital society and software exports. The action plan identifies infrastructure, human resource development, e-commerce / e-Business, e-Governance and localization of software as the focus area. It envisages creation of NII for national development, it infrastructure in the government and private sectors, creation and promotion of national high speed backbone, Internet, software technology parks across the country and a Software Technology Net. In order to support this initiative, it focuses on National Software capability Enhancement Program, empowerment of people through IT, cyber laws. National Software Development Fund, national facility for manufacturing electronic components etc.

1	Infrastructure	NII for national development	Nation's High Speed backbone network, Internet	Alternate NII/ Internet Backbone beyond 1999
		IT Infrastructure	STPI Infrastructure & promotion activities	Software Technology Net
2	HRD Education Training	VLSI Design Manpower	National Institute for Advanced Software Education & Resources	Indian Institute of Information Technology
		IT Education in Schools	Distance Education & Telecommunication	National Software Capability Enhancement Program
3	Business/ Commerce	e-Commerce	National software development fund	IT initiatives for 21 st century
		Finance S/w industry	Tech. Information Marketing e'	IPR promotion
4	Governance	Electronic Governance	Empowering People through IT	Cyber laws
5	Industry	Mega-Fab	World class S/w Companies	Mfg. Low-cost PC
		Localization of S/w		

Source: India IT Vision 2010: Action Plan

Figure 2.1: MCIT IT vision - 2010 Action Plan

2.3 National IT Objectives

The objectives and the framework given to the Prime Minister's National Task Force on IT and Software Development are as follows [103,104,105]. The national IT objectives also signify the need and urgency for creation of NII including resource mobilization.

- Use of IT in all areas of national economy viz. agriculture, industry, trade, services etc. as a critical input in making India a global economic power.
- A world-class physical, institutional and regulatory IT infrastructure, which will embrace the growing convergence of telecommunications, computers, consumer electronics, and the media infrastructure (minus its contents).
- A National Information Infrastructure (NII) backbone bridging the Local Information Infrastructure (LII), Defence Information Infrastructure (DII), Government National Information Infrastructure (GNII), Corporate Information Infrastructure (CII), Private Information Infrastructure (PII) dovetailed with the Global Informatics Infrastructure (GII) as illustrated in Figure 2.2.
- Pooling together the existing resources of the various wings of the government such as the Department of Telecommunications, Prasar-Bharati, Railways, Power Grid Corporation etc. to construct NII.

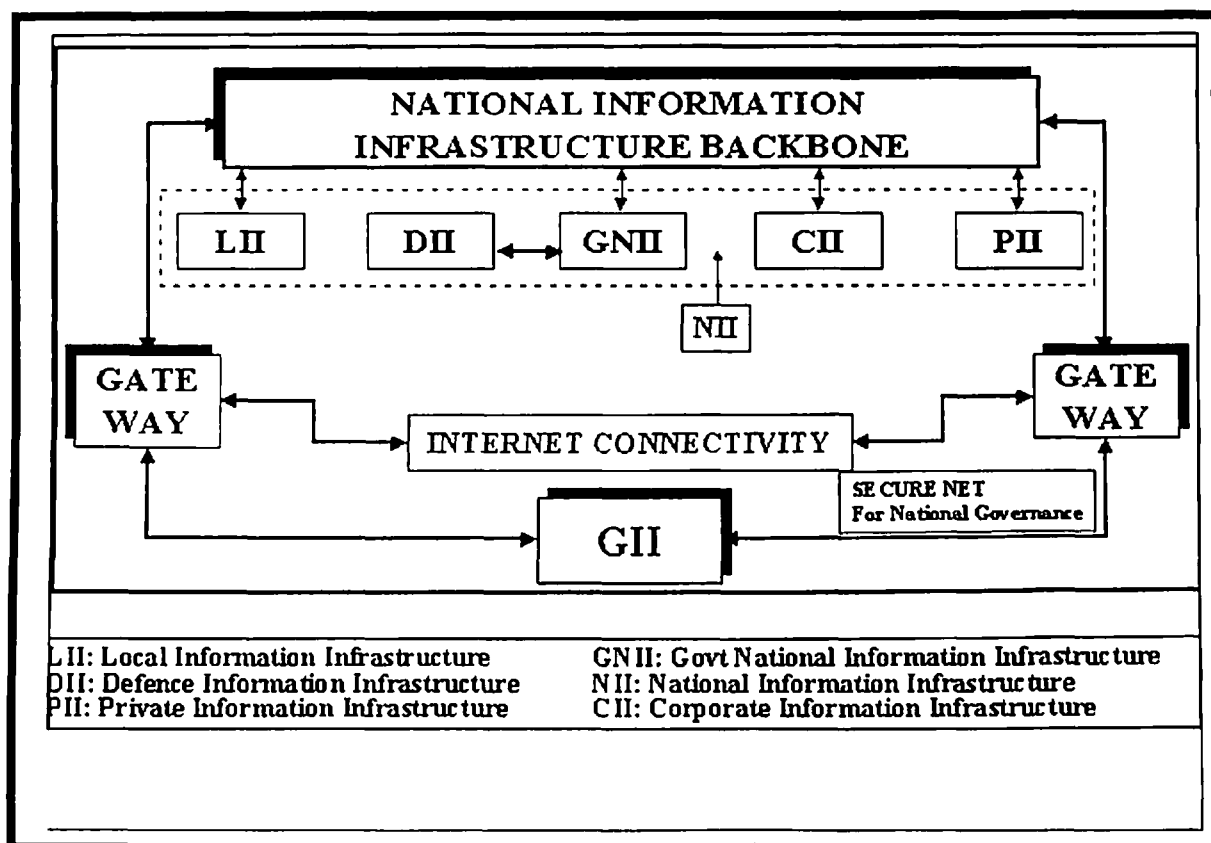


Figure 2.2: Information Infrastructure Connectivity

- Use of the Internet by all sections of society, especially in business and education, and development of Indian content for the Internet.
- A strategy for boosting the learning and use of IT in Indian languages to promote the development of software, especially educational and commercial software in Indian languages.
- A strategy for a twenty-fold increase in India's software and other IT services exports in ten years with focus on the development of world-class software products and brands that can quickly establish global dominance.
- Catalyze the growth of exports through the extensive use of e-Commerce and Electronic Data Interchange (EDI).
- Maximize the use of IT in the government at all levels; so as to make its functioning people-friendly, transparent and accountable.
- A strategy for dramatically increasing the PC density in the country and to that end, ensure that every household and commercial establishment that has a telephone also has a computer. Facilitate the availability of computer hardware, software and connectivity at the lowest possible cost.
- A strong and internationally competitive domestic manufacturing base for the computers, computer components and peripherals.
- A training and manpower development plan involving government agencies, private businesses, voluntary organizations, educational institutions and others to quadruple the number of IT professionals in the country in two years.

- A strategic plan to raise the necessary financial resources to realize the objectives of the NII.
- Legal framework for the creation of an IT-based society, with due focus on intellectual property rights (IPR), secrecy, security, and safety of information.
- Global competitiveness in IT and communications to play a prominent role in the development of IT in other countries.

2.4 NII Perspective

The NII is defined as a secure and seamless web of communication networks, computers, software, databases and consumer electronics enabling exchange of audio, text and video data by people across all sections of society covering entire landmass of the country with requisite gateways for global connectivity.

The NII as a common linkage establishes information exchange media amongst all national infrastructures, which constitute the critical foundations of the country for survival and sustenance in social, economic, political and military terms. The most critical amongst them as identified in a report of the United States President's Critical Infrastructure Protection Board, Sep 03 are the internal security, defence, energy, agriculture and environment as illustrated in figure 2.3 [185].

The NII therefore is viewed to be a key technology driver to enhance competitiveness in IT, telecommunications, software, entertainment, and other segments of business, industry education, healthcare etc which in turn support the critical infrastructure.

SECTORS	CRITICAL INFRASTRUCTURES
Core Infrastructure, Governance and Security	<ul style="list-style-type: none"> • Information and Telecommunications. • Transportation (aviation, rail, mass transit, waterborne commerce, pipelines and highways). • Postal and shipping. • Emergency Services. • Continuity of Government.
Treasury	<ul style="list-style-type: none"> • Banking and Finance.
Health and Human Services	<ul style="list-style-type: none"> • Public Health (including prevention, surveillance, laboratory services, and personal health services) • Food Processing.
Energy	<ul style="list-style-type: none"> • Energy (electric power, oil and gas production, and storage)
Environmental Protection	<ul style="list-style-type: none"> • Water • Chemical Industry and Hazardous Materials
Agriculture	<ul style="list-style-type: none"> • Agriculture • Food (meat, and poultry)
Defence	<ul style="list-style-type: none"> • Defence Industrial Base
<p>Source: Report of CNI Protection Board, USA. Figure 2.3 : Sector wise Critical Infrastructure</p>	

2.5 The Promise of the NII

The societal promise of NII would be to ensure that the best schools, teachers and courses would be available to all students, without regard to geography, distance, resources or disability. The vast national resources of art, literature and science would be available everywhere, in large and small institutions, libraries and museums [99,182].

The NII services will improve country's health care system and respond to other important social needs available on-line, without waiting in line. It would be possible to live in many places without foregoing opportunities for useful and fulfilling employment, by "telecommuting" to offices through an electronic highway instead of by automobile, bus or train. The small manufacturers would get orders from all over the world electronically with detailed specifications in a form that the machines can use to produce the necessary items. The NII would enable viewing latest movies, play the hottest video games or bank and shop from the comfort of a home. The government information would be accessible directly or through local organizations like libraries, apply for and receive government benefits electronically and get in touch with government officials easily. Individual government agencies, businesses and other entities would be able to exchange information amongst themselves electronically reducing paperwork and improving services.

Information is emerging as one of the nation's most critical economic resources for service industries, manufacturing, economic growth and national security. It is estimated that in the U.S.A two- third of its workers are in information-related jobs and the rest are in industries that rely heavily on information. A similar situation is expected to emerge in India.

In an era of global markets and global competition, the technologies to create, manipulate, manage and use information are of strategic significance. Those technologies will help businesses remain competitive and create challenging, high- paying jobs. They also will fuel economic growth, that in turn, will generate a steadily-increasing standard of living for all Indians.

Against this background there is a need to further consolidate the NII initiative and work with businesses, labour, academia, public interest groups, the central and state governments to ensure the development of a NII that enables all of us to access information and communicate with each other using voice, data, images or video at anytime, anywhere.

By encouraging private sector investment in the development of NII, and through government programs to improve access to essential services it would also be possible to promote competitiveness, job creation and solutions to the pressing social problems.

2.6 Building Blocks of NII

The NII is constituted by the physical facilities such as transmission fiber, switched backbone, nodes used to collect, collate, transmit, store, process, and display voice, data, text and images, gadgets, contents, software applications, framework of standards, specifications and people as shown in the figure 2.4 [85,86].

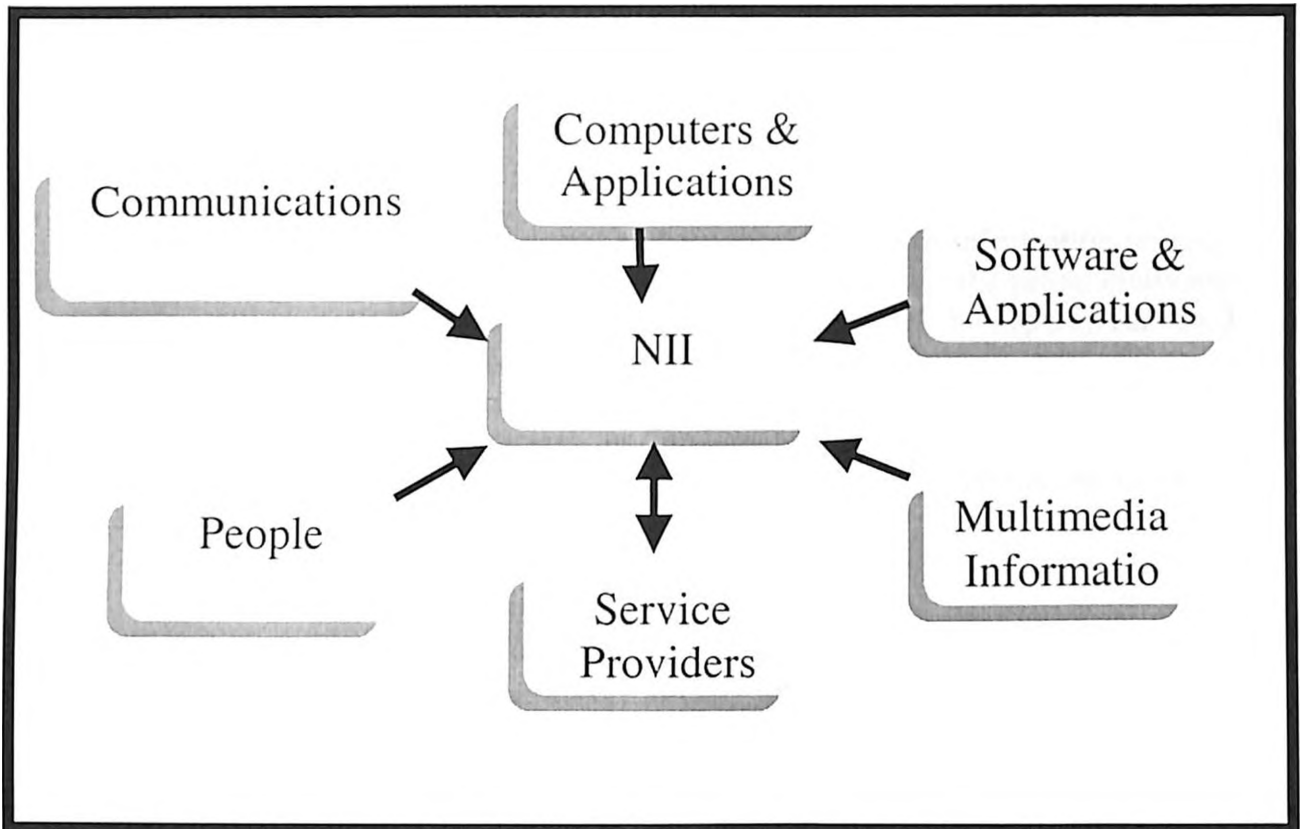


Figure 2.4: Schematic Diagram of NII

- **Gadgets:-** These include very wide and ever-expanding range of equipment including cameras, scanners, keyboards, telephones, fax machines, computers, switches, compact disks, video and audio tapes, cable, wire, satellites, optical fiber transmission lines, microwave nets, switches, televisions, monitors, printers etc. The NII would integrate and interconnect these physical components in a technologically neutral manner. The NII would require building foundations for living in the Information age and for making these gadgets useful to the public, businesses, and other non-governmental entities.
- **Contents:** The information itself may be in the form of video programming, scientific or business databases, images, sound recordings, library archives, and other media. This information may belong to government agencies, laboratories, studios, publishing houses and industry etc. A large volume of centuries old paper based data would make a very significant component of contents, which would have to be transitioned into a paperless media.
- **Applications:** Applications are the software that allow users to access, manipulate, organize and digest the proliferating mass of information, which the NII's facilities will deliver.
- **Standards & Specifications:** The network standards and transmission codes that facilitate interconnection and interoperation between networks would ensure the privacy of persons, the security of the information carried, as well as the security and reliability of the networks.

- **People:** The most significant component of the NII would be the people who create the information, develop applications and services, construct the facilities, and train others to tap its potential. Many of these people will be vendors, operators, and service providers working for private industry as well as in the government.

2.7 Global NII Initiatives

The NII is perceived as a techno-social and economic vision of information society of the 23 century. The focus and thrust towards an on-line economy is the prime motivation that dominates NII strategies in countries like USA, Australia, U.K, Singapore, Taiwan, Japan, Korea, Canada and several others. The key economic agenda is to create domestic jobs and global competitiveness through new information technologies. The NII programs of these nations are at various stages of implementation. The privatization needs and expectations from NII differ from country to country depending on the following key factors amongst others.

- The technological base already established
- The level of absorption of technology by the society
- The contribution of technology to develop mental issues
- Training and educational framework already set-up
- Economic level and quality of life

A summary of the NII initiatives in various countries is given in Figure 2.5. [53]. Following inference emerges from NII programs of these nations.

2.7.1 Strategies

The strategy adopted by each country is to develop NII with reference to their own circumstances and values. Although many features of a country's NII plans might be similar to the NII plans and experience of the other countries, they differ in their actual implementation in detail in the host country.

The NII plans in United States and Japan are aimed at national goals centering around mainly development of technology for computer hardware, software, switches, network technology, standards and developing protocols. For the most part, they are influenced by domestic and not outside considerations. In contrast, the NII plans of Singapore,

	France	Japan	Korea	Singapore	United States
Motivation	New economic growth and jobs: reaction to perceived US threat: lit telecom reform agenda set by European Union.	New economic growth and jobs: catch-up with US lead in PCs software and networking.	Desire for early participation in information revolution: reaction perceived Japanese competition and US. Asian leadership.	New economic growth and jobs: compete in region: attract Macs: reinforce role as business hub.	New economic growth and jobs: compete globally: maintain lead in computers (Communication and media)
Vision	Preserve French culture	Multimedia Information society	Establishment status among economic powers: provides transparency in government	Intelligent island: achieve balance between openness and communication ideology.	Information super highway empowerment citizens.
Strategy & Policy	Be a player in the industry through free market competition: be first mover among members of European Union.	Catch - up with the US through stimulus spending. Domestic trails, and participation in foreign trials, and in foreign trials.	Government to be leading NII user and to stimulate public demand. Expand private sector role in NII and stimulate private investment.	Adopt features of free markets but keep government as driver: be last follower of advanced nations but a first mover in the region.	Maintain lead through free market competition to stimulate investment and innovation: order without design through markets versus hierarchies.
Technology and Timing	Fiber optic backbone with copper wire to household by 2025.	Fiber optic broadband network to the home by 2005.	Fiber optic broad band network to the home by 2035	Fiber optic broadband to the office and residential block: coaxial cables to all homes by 1997: two-wires to each house by 2005.	Fiber optic broadband network to the home by 2025: last mile being reconsidered for copper wire (phone and Cable TV) and wireless
Implementation on plans (Telecommunications and media ownership, computing networks)	Liberalize telecom: corporate & privatize.	Liberalize telecoms somewhat; Nippon Telephone & Telegraph privatize and new common carriers created.	Promote market competition.	Promote competition in phone, cable broadcast and computing networks; deploy applications on networks; use govt.-linked enterprises for control.	Broadly liberalize telecoms. Long distance, local phone and Cable TV may enter each other's markets: cross-media ownership permitted up to 25% of market.
Institution and coordination	Ministry of Industry Post & Telecoms is coordinator at country level. Directorates in European Commission influence country decision.	Ministry of International Trade & Industry, Ministry of Finance. Ministry of posts & Telegraphs in government and Nippon Telephone & Telegraph plus National Computer Committee in industry.	Ministry of Information and Communication is govt. coordinator.	National Computer Board, Ministry of Information, National IT Committee. Telecommunication Authority of Singapore. Singapore International Media. Singapore Cable Vision, Internet Service Providers. Coordination by Govt. especially National IT Committee.	Congress, Federal Computer Committee. National Institute of Standard & Technology, State Public Utility Commissions. Coordination by the market. Govt. is the court of appeal.

Source: Action Plan 2020

Figure 2.5 : Survey of NII Initiatives across the Globe

France and Korea are all strongly influenced by outside considerations. Singapore plan is aimed at maintaining its position as a business hub in the Asia Pacific region and achieving a status of a developed nation. France's plan is influenced by decision of the European Union so that their domestic firms are well – positioned for economic competition. Korea, Thailand and Malaysia plans are influenced by their desire for recognition among the advanced nations of world and for leadership in the Asian sphere. [16,73,74,76]

2.7.2 Technologies

Implementation plans of all countries are essentially based on high speed, High Bandwidth (ranging from 622 Mbps to 2.5 Gbps) communication networks capable of two way voice, data and video communication connecting businesses and house hold. Most advanced countries have planed employment of advanced fiber optic Synchronous Optical Network (SONET) transmission system / Synchronous Digital Hierarchy (SDH) Network and Asynchronous Transfer Mode (ATM) switches in a single network or networks at the core of the new public access of transmission network. While USA is deploying SONET transmission system, Europe and Asia are deploying SDH transmission system. Evaluation of SDH deployment is part of Francs Telecom's global objective. Also in Japan, NTT (Nippon Telephone and Telegraph) has already deployed SDH. The phase I and phase II Plans are drawn by a few countries to upgrade the international and high speed domestic network bandwidth from 2.5 GB to 16 GB. The last mile to home is telephone and / or cable. The last mile network technology ranges from Broadband Integrated Services Digital Network (B-ISDN) to Narrowband Integrated Services Digital Network (N-ISDN). The need for high bandwidth into home is in order to receive high quality images, large databases, etc. Which can be downloaded to PCs or other appliances. Cellular, low orbiting satellites and video electronics are also being implemented by a number of counties.

2.7.3 Implementation Period

The plans generally call for a technology in place in 10 –15 years. Only France has a little longer horizon. The countries have made plans to implement NII in 2 to 3 phases. Each phase extends for 4 to 5 years. As mechanism to speed up implementation, country plans call for stimulus spending, government focussed promotion of societal applications and telecommunications reforms.

2.7.4 Policies

NII Plans and their implementation in all the countries are monitored by high power Committees / Boards headed at the level of Vice President / Prime Minister or such senior government functionaries. The applications, Research & Development etc. are planned and monitored by the high power committees.

2.8 India's NII Initiatives

In order to respond to the needs of digital economy as perceived in its vision- 2010: Action Plan, the MCIT has formulated a number of nationally coordinated initiatives which are under various stages of implementation. These include [53]:

- National Information Infrastructure for National Development: NII 2000 Action Plan
- National Software Capability Enhancement Program (Project: SoftCap)
- STPI Vision 2000: Expand High Speed Datacom Facilities to enhance Software Exports
- IPR Promotion Program
- Technology Information & Forecasting Support in IT

2.8.1 NII for National Development: NII 2000 Action Plan

For immediate implementation of NII for National Development, a short-term, inter-departmentally coordinated NII 2000 Action Plan has been formulated. The broad components of NII 2000 Action Plan cover National High-speed Backbone Network, Internet and NII, Interconnection of Networks, PC Penetration and Localization of Software in Indian Languages, Government Computerization, ERNET Up-gradation, Multimedia Promotion Program, Advanced R&D, Test Beds for Technology Adoption Flagship Applications for NII, Enhanced IT Users/Investment Promotion, Electronic Commerce, Regulatory and Legal Framework etc.

Policies related to Internet and related matters have already been framed. The country now has NII Backbone build-up in phases with a bandwidth of 2.5 Gbps. Availability of bandwidth is expected to precede the demand for datacom users and stimulate the growth and application of IT. Up gradation and expansion plan for Education & Research Network (ERNET) of MCIT has been work-out. Decision has been taken to set-up ERNET India Society as an autonomous Scientific Society under MCIT.

As a part of regulatory framework for digital society the IT ACT 2000 has been promulgated. The National Root Certification Authority and National Repository for digital certificates to promote and institutionalize Public Key Infrastructure (PKI) have been created. These are expected to provide identification, authentication, authorization, access control, confidentiality, integrity and non-repudiation features for on-line transaction across the NII.

Multimedia Promotion Program under NII aims at India as a Village. An online shareware to disseminate the know-how & know-why related to socio-economic development is expected to be available at designated resource centers for use/replication anywhere else. As a first step, entrepreneurship development through reusable multimedia contents repositories, resource and training as a facilitator to multimedia content production industry is envisaged. In this regard, a project on a Development-cum-Training Infrastructure as a National Resource for Low Cost Multimedia Content Creation (CEDTI Mohali) has been formulated and is under implementation at CDAC, Jadavpur University and CEDTI Mohali.

A set of other NII test-beds initiatives have been planned. These test-beds are going far beyond the Proof-of-concept, Demonstration project and will help technology development promotion of new applications leading to operational systems. Present model of Advanced Communications Technologies and services (ACTS), under European Commission built on the experience of earlier European Strategic Program for

R&D in Information Technology (ESPRIT) and R&D in Advanced Communication (RACE) Technologies in Europe is being followed. A major national initiative on test-bed on ATM technology has been developed for implementation. On similar lines, Internet e-commerce, distant-education and telemedicine NII test-beds have been proposed. Further MCIT through C-DAC and CMC Ltd. is working closely with some state governments on e-Governance.

Development and deployment of a multi-purpose and scalable multimedia information warehouse for state-level electronic governance of Andhra Pradesh is one of the projects initiated as a joint effort of C-DAC and Andhra Pradesh Government. Another project initiated for implementation by CMC Ltd. is Vijayawada Municipal Corporation's Vijayawada On-line Information Centre (VOICE). It is expected to provide open access to on-line information to the citizens. Experience of implementation of NII test beds at some of the live-sites in Andhra Pradesh could be used by other states for replication.

Localization in Indian Languages and their applications and PC penetration have been important items on the MCIT Agenda. Work of CDAC (GIST), efforts of NIC to promote local language usage and some of the industry efforts committed to this subject are all well known. Amongst the new initiatives, Microsoft in collaboration with NCST is working to provide Operating System level support for enabling Indian languages in Windows NT to help localize applications commonly used e.g. word processing, office automation, database etc. C-DAC and IIT, Kanpur are carrying out development which will help provide real-time interactivity with Internet in Hindi enabling e-mail to be received/sent, and creating documents, searching etc.

2.8.2 National Software Capability Enhancement Program

There is a need to have focused program to enlarge and improve the quality of human resources related to higher level of computer, software and communication expertise, system managers and project leaders. In order to fill this gap at national level, an Inter-Ministerial Group has evolved a plan-of-action. This is now being put in place as National Software Capability Enhancement Program under Project Soft Cap. The primary stakeholders are some of the premier institutions in the country dealing with software with inputs available from software industry and supported by MHRD and MCIT. The prominent components of Soft Cap are : Increase in intake at UG and PG level in IITs, RECs, IISc and others; Quality Improvement Program for faculty of engineering colleges; focused efforts in software engineering and software project management; software quality certification; collaborative R&D efforts between academic-R&D labs and industry etc. A new initiative has been launched recently with STQC on Software Quality Certification under Project: Soft QC/QM to help SMEs. Another recent initiative has been the setting-up of a JAVA Competency Centre at R&D Centre of CMC Ltd., Hyderabad as a collaborative effort between Sun Microsystems Ltd. and CMC Ltd.

A National Institute for Advances in Software Education and Research (NISER) has also been formulated to focus on Software Engineering, Internet related technologies with inputs from Microsoft. The aim is to improve and expand the quality at higher end of

software capability in education sector as well as in R&D by stepping up the efforts at well-known institutions.

Besides formal sector in computer education, non-formal sector is also providing excellent technical education to meet the needs of IT industry. IT Education itself in certain niche-areas has emerged as a business proposition in India and Indian enterprises abroad. The MCIT is operating a scheme named, DOEACC, under which computer training institutes/organizations in the non-formal sector, subject to meeting well-defined norms and criteria, are given accreditation for conducting specified level of courses at O/A/B/C levels and examinations are conducted on all India Basis. AICTE, the statutory body for technical education has delegated the responsibility of the implementation of the scheme to DOE, which in turn has authorized DOEACC Society to implement the same. There are already 583 accredited institutions subscribing to this program.

2.8.3 Software Technology Parks Scheme: STPI Vision 2000

Success of Software Technology Parks (STP) Scheme implemented by Software Technology Parks of India (STPI), an autonomous society under MCIT has attracted worldwide attention. The single window and clustering approach using dedicated International Gateway has provided the desired ambience for growth. As a single window, STPI plays promotional as well as regulatory role, a facilitator and a catalyst for software exporters. STPI has set up, operates and manages its own earth stations dedicated to software export needs at Bangalore, Hyderabad, Noida Thiruvananthapuram, Bhuvneshwar, Gandhi Nagar and many other places. It provides value added services to STPI member units, customized solutions for software exporters, training in certain niche areas, market intelligence and forecast needs particularly for small and medium enterprises (SME) Sector.

Various state Governments / Agencies have started looking at IT as an opportunity for economic growth and are working with STPI to take advantage of their experience and expertise and to set up dedicated low cost earth stations as part of software technology parka / IT parks. Government of India has recently given special dispensation to STPI to set up, operate and maintain more earth stations as felt necessary by STPI to serve the needs of this sector. In the first phase of the expansion plan, STPI earth stations have been set up at Moholi, Jaipur and Navy Mumbai as collaborative efforts with respective state Governments / Agencies. Replication of cluster model of STPI to support the initiative of State Government / agencies will go a long way to spread the software activities in the country thus providing more employment, entrepreneurship and earn foreign exchange.[85]

2.8.4 Intellectual Property Rights (IPR) Issues

In the post WTO and TRIPs regime, IPR issues had assumed special significance in IT sector, more so in view of the NII / GII / emergent digital economy. In order to build up grater awareness, develop in-sights in to the complex mechanism of creation, ownership and protection of intellectual property across the country has responded to the needs of digital era. MCIT has setup IPR cell and is implementing IPR Promotion Program. IT,

being a specialized and rapidly evolving field having impact on virtually every sphere of life and commerce, handling IPR issues in Electronic and Information Technology Sector also requires specialized knowledge and skills [83].

2.8.5 Technology Information Assessment and Forecasting (TIFAC)

TIFAC-E Cell, set up in MCIT initially as a joint effort of TIFAC and DOE to create a platform for Technology Information Assessment and Forecasting in Electronics had, led the technology vision 2010 exercise in Electronics and Information Technology Sector under the over all co-ordination of TIFAC. Analysis of global technology trends, market conditions, country / sector policy initiatives and incentives for achieving competitive edge has provided valuable inputs to launch new national initiatives.

TIFAC-E cell / TechnoInfo has today emerged as an umbrella structure with current emphasis to address to the needs of IT sectors, by networking national and international resources. On-going initiatives on NII, Cyber Laws, Electronic Commerce etc. draw heavily from the efforts of TIFAC- E cell. STPI and TAFAC-E cell jointly have developed Tradenet to support software exports particularly by SMEs and to attract FDI. This has been modeled on IPN net of World Bank. Another initiative related to market, opportunity and technology forecasting for the country in software and IT services has been launched by the MCIT.

2.9 Critical Issues in Design and Development of the NII

There are wide-ranging issues relevant to the timely development and growth of the NII. Specific principles and goals in areas where action is warranted have been identified along the following lines. [99,100].

2.9.1 NII Framework

A comprehensive NII framework with clearly outlined objectives, goals, policies and road map need to be evolved. This framework should address all the building blocks of NII, services, tariffs, revenue sharing, sensitivity factors of earning, telescoping into regional and global infrastructure, regulation, privatization, convergence, spectrum management, information operations, security, collaboration amongst industry, institutions and the government. This world requires a comprehensive research, design and development blueprint for major building blocks of NII.

2.9.2 Private Sector Investment & Involvement

One of the most effective ways to promote investments in NII would be to introduce and expand competition in communications and information markets. Vibrant competition in these markets will spur economic growth, create new businesses, and benefit end users. [83].

This would require policy changes, communications reforms with respect to universal access in communications markets such as the cable, television and local telephone markets, as well as explicitly promote private sector infrastructure investment. This in

turn would require revision of tax policies, incentives for private sector investments in R&D, new business formation, extension of the R&D credit, a targeted capital gains reduction for investments in small businesses and help spur the private sector investments needed to develop the NII.

2.9.3 Universal Service Concept

In order to ensure that information resources are available to all citizens at affordable prices, a national goal of "Universal Service" for telephones, widespread availability of basic communication services at affordable rates needs to be met.

A major objective in developing the NII will be to extend the Universal Service concept to the information needs of the people as a matter of fundamental fairness and bridge the gap amongst telecommunications or information "haves" and "have-nots" or digital divide.

We would need to develop a broad, modern concept of Universal Service that would emphasize giving all Indians who desire it an easy, affordable access to advanced communications and information services, regardless of income, disability or location. This goal would in turn spur efforts in infrastructure development by increasing competition in communications and information markets and can make low cost, high quality services and equipment widely available. Policies promoting greater competition in combination with targeted support for disadvantaged users or rural areas would advance both rapid infrastructure modernization and expanded Universal Service.

2.9.4 Technological Innovation and New Applications

As we have seen in the recent past, the regulatory, antitrust, tax and intellectual property policies affect the level and timing of new offerings in services and equipment including the technology base that generates innovations for the marketplace. But technological innovations ultimately depend upon purposeful investments in research and development, by both the private sector and government.

The R&D investment helps firms to create better products and services at lower costs. Therefore we need to accelerate the development of technologies critical for long-term growth but not receiving adequate support from private firms, either because the returns are too distant or because the level of funding required is too high for individual firms to bear.

The research support can help create basic information technologies in computing, networking and electronics. There is need for faster NII related research and technology development through partnerships and other mechanisms to accelerate technology development where market mechanisms do not adequately reflect the nation's return on investment.

In particular, these government research and funding programs should focus on the development of beneficial public applications in the fields of education, health care, manufacturing, and provision of next generation government services. Implementation

of NII Pilots in health care, service provisioning schools districts, libraries, universities, and other non-profit entities would help IT penetration immensely. The grants should be awarded after a competitive merit review process and should be used to fund projects to connect institutions to existing networks, enhance communications networks that are currently operational and permit users to interconnect among different networks.

Funded projects should demonstrate the potential of the NII and provide very tangible benefits to their communities. They should help leverage the resources and creativity of the private sector to devise new applications and uses of the NII. The successes of these pilot projects should create an iterative process that will generate more innovative approaches each year.

2.9.5 User-Driven NII Operations

The NII should be a "Network of Networks" and a "System of Systems". The information must be transferable over the disparate networks easily, accurately, and without compromising the content of the messages.

The NII should be of maximum value to users if it is sufficiently "open" and interactive so that users can develop new services and applications or exchange information among themselves, without waiting for services to be offered by the agencies that operate the NII. In this way, users will develop new "electronic communities" and share knowledge and experiences that can improve the way they learn, work, play, and participate.

To assure interoperability and openness of the many components of an efficient, high-capacity NII, standards for voice, video, data, and multi-media services must be developed. Those standards also must be compatible with the large installed base of communications technologies, flexible and adaptable enough to meet user needs at affordable costs. There is a need to adapt and implement a consensus-based, voluntary standards-setting process in communications and information technologies.

Particularly in the area of information and communications technology, where product cycles are often measured in months, not years, the standards processes are critical and have not always worked to speed technological innovations and serve end-users well. Government can accelerate this industry-driven process by participating more actively in private-sector standards-writing bodies and by working with industry to address strategic technical barriers to interoperability and adoption of new technologies as well as adapting a large number of already existing standards.

2.9.6 Information Security and Network Reliability

The trustworthiness and security of communication channels and networks are germane to the success of the NII [76,133,175]. Users must be assured that information transmitted over the infrastructure will go when and where it is intended to go. Electronic information systems can create new vulnerabilities. For example, electronic files can be broken into and copied from remote locations, and cellular phone conversations can be monitored easily. Yet these same systems, if properly designed, can offer greater security than less advanced communications channels [2].

With information systems, gathering, sending and receiving a variety of personal information is now simple, quick, and relatively inexpensive. The use of information technologies to access, modify, revise, repackage and resell information can benefit individuals, but unauthorized use can encroach on their privacy. While media reports often emphasize the role of modern information technology in invading privacy, technology advances, and enhanced management oversight also offer the opportunity for privacy protection. This protection is extremely important to businesses that increasingly transmit sensitive proprietary data through electronic means.

In a climate of tough global competitiveness to gain market advantage, the confidentiality of this information can spell the difference between business success or failure. In addition, it is essential that the government work with the communications industry to reduce the vulnerability of the nation's information infrastructure.

The NII must be designed and managed in a way that minimizes the impact of accident or sabotage. The system must also continue to function in the event of attack or catastrophic natural disaster so that the survival and the sustenance of social, economic, political and military activities are never in peril.

2.9.7 Management of the Radio Frequency Spectrum

Many of the dramatic changes expected from the development of the information infrastructure will grow out of advances in wireless technologies. The ability to access the resources of the NII at any time, from anywhere in the country, will be constrained, however, if there is inadequate spectrum available [84,106].

To ensure that spectrum scarcity does not impede the development of the NII, the government would have to give a high priority to streamline its procedures for the allocation and use of this valuable resource.

2.9.8 Protection of Intellectual Property Rights

Development of an advanced information infrastructure will create unprecedented market opportunities and new challenges for media and information industries. The broad public interest in promoting the dissemination of information to our citizens must be balanced with the need to ensure the integrity of intellectual property rights and copyrights in information and entertainment products. This protection is crucial if these products whether in the form of text, images, computer programs, databases, video or sound recordings, or multimedia formats are to move in commerce using the full capability of the NII.

2.9.9 Coordination

Many of the agencies expected to participate in the NII are now subject to regulation by central and state government agencies. If the information infrastructure is to develop quickly and coherently, there must be close coordination amongst the various government entities, particularly with respect to regulatory policy.

It is crucial that all government agencies work cooperatively to forge regulatory principles that will promote deployment of NII. The NII should also be developed in the context of evolving global networks. Because customers typically would demand that our national communications providers offer services on a global basis. It is also critical that the infrastructure within this country can meet international, as well as domestic, requirements. This would require us to open access to overseas markets. The government therefore needs to ensure that we have an equal opportunity to export telecommunications-related goods and services to potential overseas customers.

2.9.10 Access to Government Information and Improved Government Procurement

The information is the currency of democracy. The government agencies are among the most prolific collectors and generators of information that is useful and valuable to citizens and business.

Improvement of the nation's information infrastructure provides a tremendous opportunity to improve the delivery of government information to the taxpayers who paid for its collection; to provide it equitably, at a fair price, as efficiently as possible. The central and state governments would have to improve every step of the process of information collection, manipulation, and dissemination [83,103,141].

The government should fund research programs that will improve the software used for browsing, searching, describing, organizing, and managing information in local languages. The government should be committed to apply those tools for the distribution of information that can be useful to the public in their various roles as teachers, researchers, businesspeople, consumers, etc.

The key questions to be addressed are, information needs of the public in electronic form, means of distribution, access to it and how can government itself improve through better information management.

2.10 Change Management Through Collaboration

In its report titled, "National Strategy to Secure Cyber Space, Sep 03" the US President's Critical Infrastructure Protection Board has Stresses that people and organizations will be empowered to secure the NII [185]. On similar lines, in India also there is need to build a partnership of business, labor, academia, the public, and government that is committed to deployment of an advanced, rapid, powerful infrastructure accessible and accountable to all sections of our society on equitable basis.

Forging this kind of partnership will require extensive inter- governmental coordination to ensure that central and state government policies regarding the NII are consistent, coherent, and timely. It would also require the development of strong working alliances among industry groups and between government and the businesses responsible for creating and operating the NII. Finally, close cooperation will be needed between government, users, service providers, and public interest groups to ensure that the NII develops in a way that benefits the people of India. Following actions are needed.

2.10.1 National Information Infrastructure Task Force (NIITF)

The government need to set up NIITF that should work with MCIT, Ministry of Information & Broadcasting and the private sector to evolve a formal NII framework, propose the policies and initiatives needed to accelerate development and deployment of a NII components.

Activities of the NIITF should include coordinating government efforts in NII applications, linking government applications to the private sector, resolving outstanding disputes, and implementing policies. The NIITF should focus on telecommunications policy convergence, regulation, information policy, and applications through dedicated working groups or committees.

2.10.2 Advisory Panel on the National Information Infrastructure

This panel should facilitate meaningful private sector participation in the NIITF's deliberations, and advise the government of the NIITF matters relating to the development of the NII. The panel should consist of members, from a variety of NII constituencies and interested parties. The NIITF and its committees should also use other mechanisms to solicit public inputs to ensure that it hears the views of all interested parties.

2.10.3 Communications and Information Policy-Making Agencies

In order to implement the NII agenda, the agencies most directly responsible for the evolution of the NII must be properly structured and adequately staffed to address many new and difficult policy issues. The government should ensure that these agencies have the intellectual and material resources they need. In addition there will be a need to make the organizational and procedural changes needed to most effectively contribute to the NII initiative.

2.11 Conclusion

In this chapter we have concluded that IT is synonymous with our survival and sustenance as a nation in economic, social, political and military terms at national and global levels. Therefore building a secure, safe and trusted NII and making it available to every user worldwide at affordable cost, at all times of the year in the form of concise cyber space at personal, corporate, government, national and global scale is on the priority list of our national IT agenda. In this context the national IT objectives, national and global NII development initiatives have been examined. We have also examined the building blocks of NII and their integration in a technologically neutral manner.

This transformation would involve transition from centuries old and perfected paper based framework and environment to a virtually unknown paperless digital work environment having unprecedented complexities. There are a large numbers of critical issues, which are to be addressed, while engineering the NII. Some of the critical issues viz. NII framework, universal service concept, technology, user driven operations, spectrum management, IPR, security etc. have been identified and examined briefly. Amongst these issues, the security of NII in terms of confidentiality, integrity, availability, and trust are extremely critical and form the broad areas of research in this thesis. These have been examined and addressed in more detail in chapter 3.

CHAPTER 3

NII SECURITY PERSPECTIVE AND ISSUES

3.1 Introduction

In chapter 2, it is emerged that there is a nation-wide awakening to organize information to be instep with global IT trends. The computerization and networking at most echelons of the government and private sector agencies is underway. The pace of development is such that, this capability will enable the country to effectively participate in economic, technological, political and other fields at global level in next 3 to 5 years. This intensive penetration of IT and communication systems would emerge as the National Information Infrastructure, which would underpin all infrastructures across the country. The infrastructures deemed critical are so vital that their disability or destruction would have a debilitating impact on the defense and economic security of the country. Telecommunications, energy, banking and finance, transportation, water, emergency services, and essential government services would be connected to each other in one way or another in this "wired" age.

The intensive penetration of IT and communications will make us dependent on the information infrastructure, which can be exploited by our adversaries in the form of an instrument of war termed as **Information Warfare (IW)**. This relates to waging a war on target nations using information related principals whereby the information systems of an enemy are disabled, damaged, denied or destroyed using own information systems. All information systems in military, government and private sectors are, therefore, prone to such attempts by the enemies within or from across the borders at all times, during peace and war. With a view to resist such attempts by the enemy, it is very essential to ensure that information systems across the National Information Infrastructure should be secure and tamperproof against all such break-ins.

This chapter identifies **Critical National Infrastructures (CNI)**, their interdependence on the NII, the external and internal threats to NII, in built technical or man made vulnerabilities of NII and how these emerge as risks which need to be minimized and/or mitigated. The chapter also examines the changing role of Critical Infrastructure Protection (CIP) and surveys global initiatives for CIP. This chapter also presents an overview of security in digital space, its role and relevance to NII supported CNI, building blocks of basic security overlay and the security model for evolving comprehensive CIP strategy. It presents NII security goals, components of security overlay and the security model.

3.2 Security of Information Operations

The term information infrastructure refers to the complex of sensing, communicating, storing, and computing elements that comprise a defined information network conveying analog and digital voice, data, imagery, and multimedia data. The "complex" includes the physical facilities e.g. computers, links, relays, and node devices. It also encompasses

network standards and protocols, applications and software, the personnel who maintain the infrastructure. and the information itself

The infrastructure is the object of both attack and defense; it provides the delivery vehicle for the information weapons of the attacker while forming the warning net and barrier of defense for the defender. The security of the physical and operational functions of the infrastructure is therefore essential for both the defender and the targeted alike.

3.3 National Information Infrastructure and its Security

The NII constitutes a common foundation for exchange of information amongst all infrastructures across the country such as defence, transport, power, energy, banking, government etc. Each infrastructure is vulnerable in varying degrees to natural or man made disasters, components failures and negligence.

The failure of one infrastructure has serious and compounding effects on the functioning of other infrastructures. The interdependencies among the nations critical infrastructures create new vulnerabilities. These interdependencies refer to the physical, cyber, logical and geographic linkages among the critical infrastructures as shown in the figure 3.1. In an emerging " System of Systems" perspective analysis of these interdependencies is presented in figure 3.2. [95,108,110]

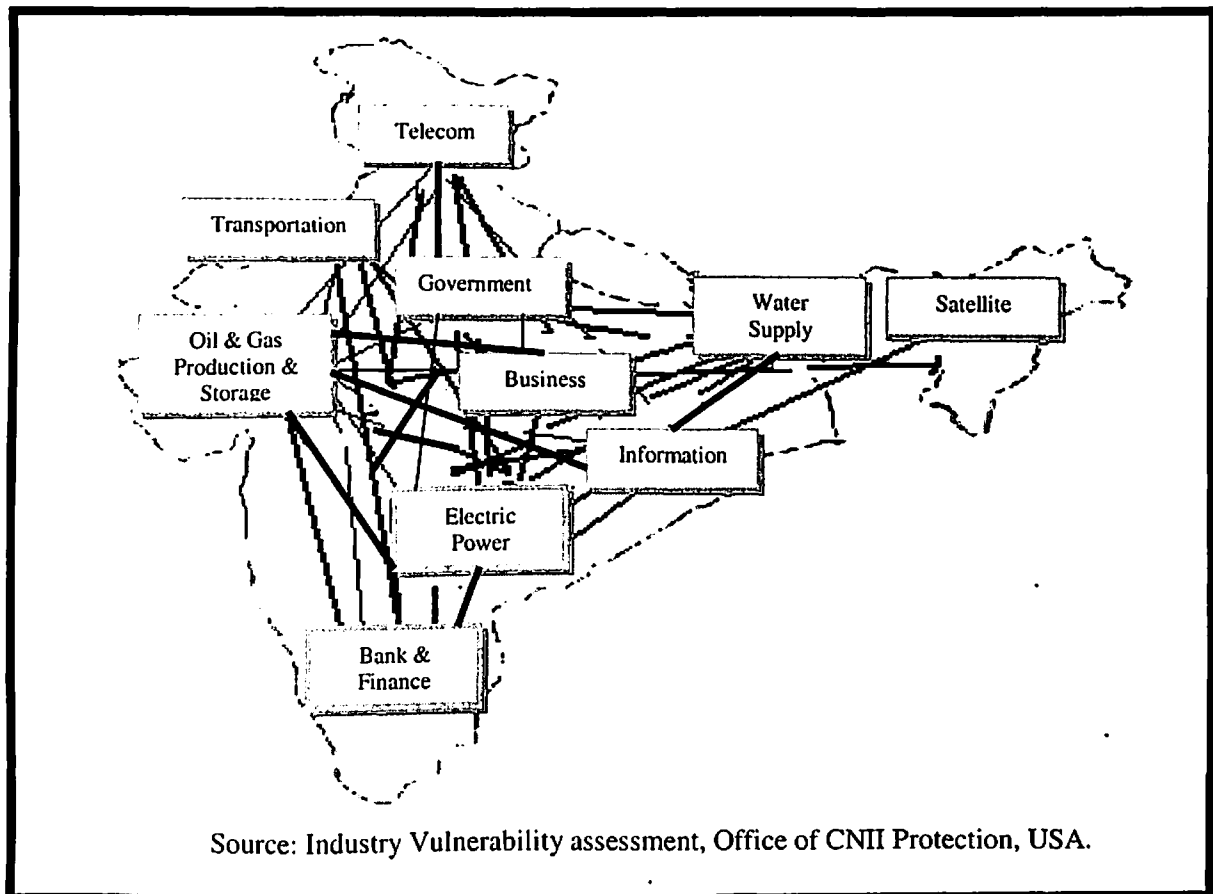


Figure 3.1: National Infrastructure Dependencies

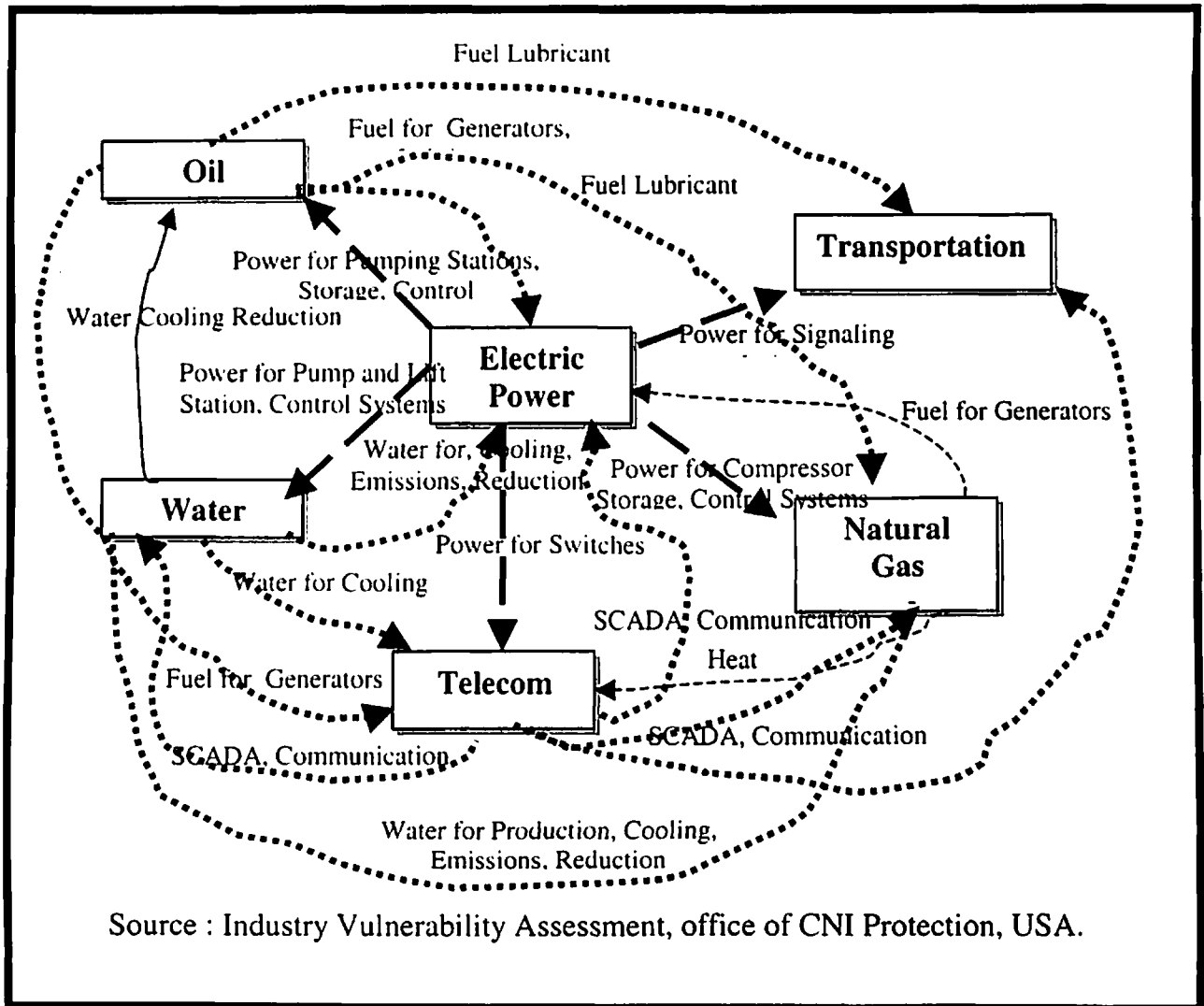


Figure 3.2: Analysis of Infrastructure Interdependencies.

The computer and communication systems constitute the vital functional blocks of the manufacturing, accounting and transportation systems, commerce and a large number of support services. The damage or destruction of the computers and networks of electrical power systems will cut off electric supply and disrupt functioning of telecom, banking, railways, refineries, water supplies, shipping and civil aviation. Similarly non-availability of computers and networks of refineries, water supply and emergency services can disrupt the all other infrastructures. [CRIT FOUND 97]. Therefore safety, security and all time availability of information systems of these critical infrastructures has emerged as a national security issue of unprecedented seriousness, dimensions and complexity.

3.4 The Global Information Infrastructure (GII) and its Security

The GII includes the international complex of broadcast communications, telecommunications, and computers that provide global communications, commerce media, navigation, and network services between NIIs. (Some documents refer to the GII as the inclusion of all NIIs. In this document GII signifies the interconnection layer between NIIs and discussed in the context of NII security.)

At the global level, the international telecommunications, computer networking, and command services such as air traffic management, and global navigation services which are administered by the International Civil Aviation Organization (ICAO), regulated by international laws and treaties and accessible to the international community comprise the GII. The GII is a dynamic, developing infrastructure that is characterized by the following: [83,84].

- International regulation to control the allocation of spectrum and cooperation to achieve interoperability and management of bandwidth resources.
- International standards and protocols to provide universal interoperability.
- Transnational private (and national) ownership, integration, and operation.
- Open access for both providers and users.

The establishment of the GII with a humanitarian objective to ensure that the full potential benefit of advances in information and telecommunications technologies are realized for all citizens is promoted by the group of seven major industrialized nations (G-7). The G-7 nations promote the GII to create a global information marketplace, encouraging broad-based social discourse within and among all countries to increase economic growth, create jobs, and improve infrastructures.

The backbone of the emerging GII includes intercontinental cables and a future commercial network of layered broadband communication satellites operating at three orbital tiers.

- **Geostationary orbit:** This involves relay and direct broadcast satellites in earth-synchronous orbits at 22,300 miles to provide continuous overhead coverage of designated regions on the surface of the Earth while imposing a latency of 250 millisecond (round trip).
- **Medium earth orbit:** This involves satellites operating at 6,000 to 15,000 miles. Small constellations of these satellites relays provide 50 to 150 millisecond latency and moderate dwell on ground terminal subscribers.
- **Low earth orbit:** These are larger constellations of satellites operating at 500 to 1,500 miles to provide low latency of 5 to 100 milliseconds, but require complex intersatellite links and switching to achieve near continuous coverage to stationary and mobile subscribers.

Layered communication satellite constellations will employ both space, and ground based switching as well as intersatellite links to achieve high traffic efficiency. The aggregate latency experienced by the user includes the ground-satellite latency plus many other switching and routing functions. Immediate global access to data, voice, and video communications will become available as these networks are integrated with terrestrial fiber optic links and wireless communication systems within nations. This increased interconnectivity 'will bring access and vulnerability to functions dependent upon the global network.

As the GII increases in expanse, connectivity, and complexity, global security and regulatory issues need to be addressed in the areas of intellectual property rights,

ensorship, encryption, privacy, and cultural sovereignty. The current global regulatory framework of international law, diversity in national policies, and in social and cultural values is not prepared for the impact that the emerging GII will introduce. Therefore in order to operate at global level by integrating NII with GII, the security of both is crucial. Also the IW can emanate from any part of globe through GII. Therefore combined security of NII and GII needs to be addressed.

3.5 Role of NII in Critical National Foundations

The NII includes the information infrastructures across the entire landmass of the country embedded in other infrastructure. It is the single controlling component of the more general "critical national infrastructures" of the nation, which are so vital that their incapacitation or destruction would have a debilitating impact on defense and economic security. The critical components are shown in the figure 3.3. The impact of non-availability of these infrastructures is described in the succeeding paragraphs.

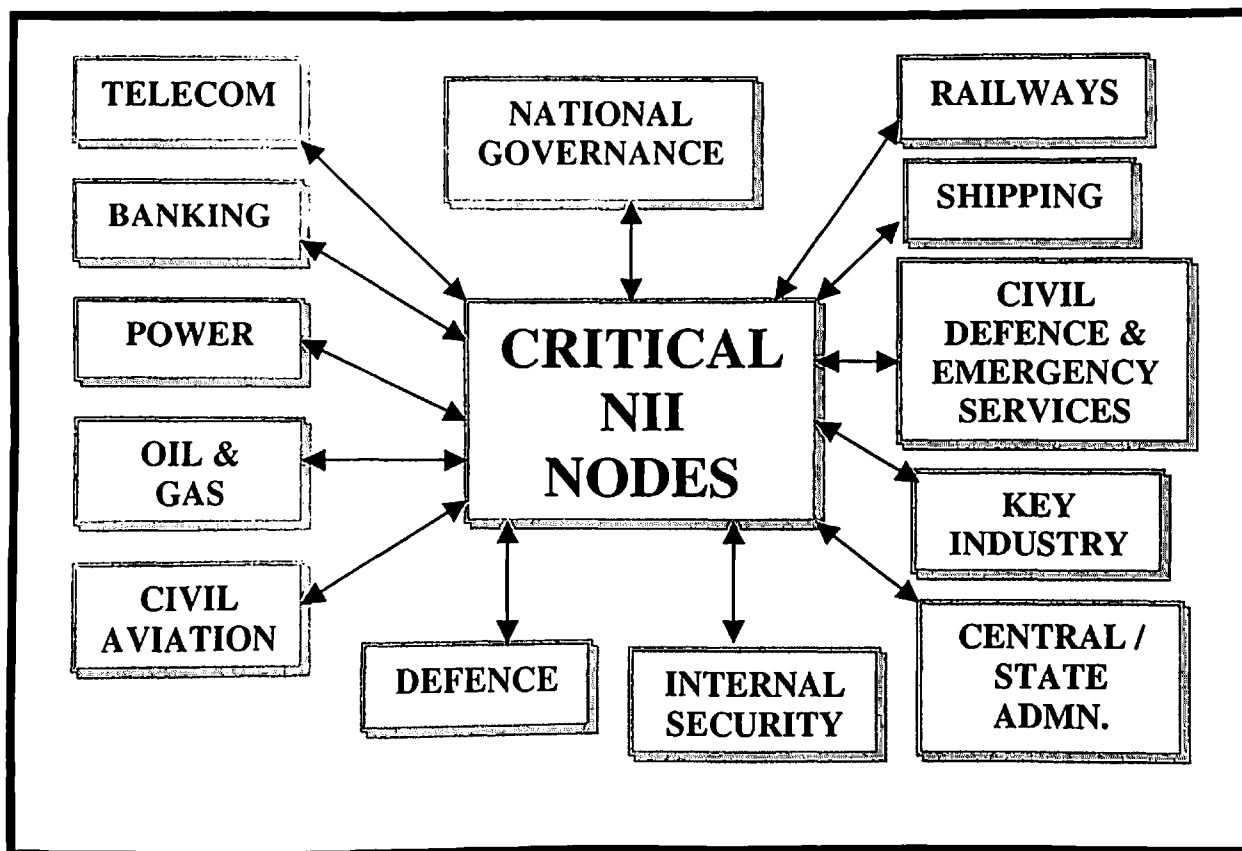


Figure 3.3: Critical NII Nodes

3.5.1 Information and communications

These pertain to Public Telecommunications Network (PTN), the Internet, and millions of computers in home, commercial, academic, and government use. These include the networks and systems that support the transmission and exchange of electronic communications among and between end users and electronic or mechanized devices, such as networked computers.

3.5.2 Financial Infrastructure

Financial infrastructure comprises banking, non-banking financial service companies, payment systems, investment companies, mutual funds, securities and commodities exchanges. These include all the associated operational organizations, government operations, and support entities that are involved in all manners of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments. Some of these aspects are still getting computerized and networked.

3.5.3 Energy

This includes the industries that produce and distribute electric power, oil, and natural gas, generation stations, transmission, and distribution networks that create and supply electricity to end users so that end users achieve and maintain nominal functionality, including the transportation and storage of fuel essential to that system. Also included are production and holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels; the refining and processing facilities for these fuels; and the pipelines, ships, trucks, and rail systems that transport these commodities from their sources to systems that are dependent upon gas and oil in one of their useful forms.

3.5.4 Physical distribution Pathways

The vast interconnected network of highways, rail lines, ports and inland waterways, pipelines, airports and airways, mass transit, trucking companies, and delivery services that facilitate the movement of goods and people within the country and across the international borders.

3.5.5 Human Services

These include those operations and services of government at the centre, state, and local levels which are critical to the functioning of the nation's systems; i.e., public health, safety, and welfare, including water supply systems, emergency services viz. police, fire, rescue and emergency medical services etc. The government services include continuity of government preparedness, planning for the identification of functions that would have to be performed during an emergency, the identification of personnel for performing those functions, the development of plans, and the capability to execute those plans and elements in support of them.

3.6 Threats and Vulnerabilities of NII

An adversary may seek to achieve numerous objectives by attacking these infrastructures. In order to achieve these objectives, numerous intermediate attack goals may be established that can then be achieved by information infrastructure attacks. Examples of these include the following:-

- Reduce security by reducing the ability of a nation to respond in its own national interests.
- Weaken public welfare by attacking emergency services to erode public confidence in the sustainment of critical services and in the government
- Reduce economic strength to reduce national economic competitiveness

- The figure 3.4 signifies that NII underpins every component of infrastructure, which has direct or indirect bearing on the nations defence, economy, trade, industry and social welfare. Therefore any of the above mentioned action by enemy can create an unlimited ways of threats and vulnerabilities to the NII.

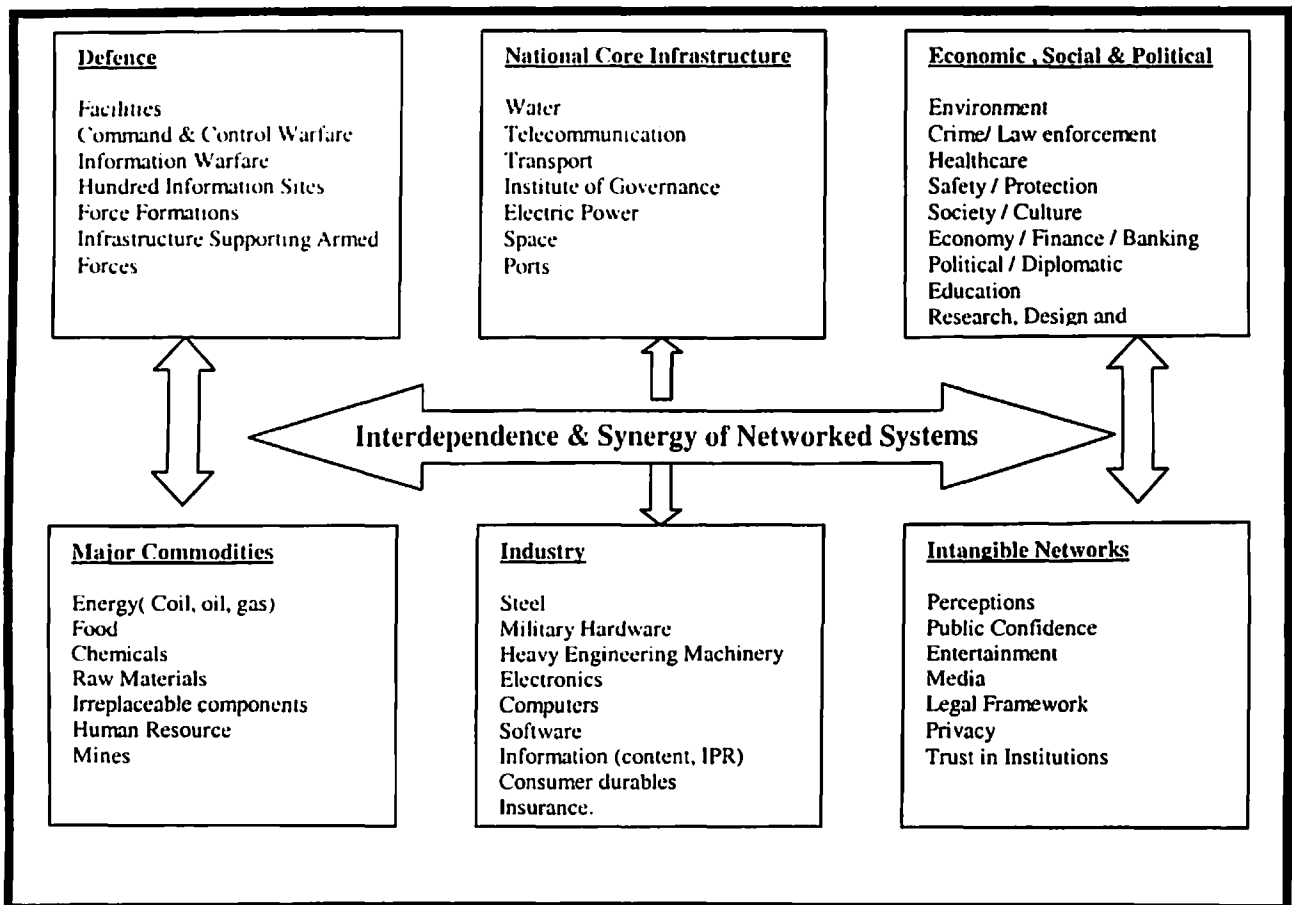


Figure 3.4: Infrastructures at Risk due to ICT Failures.

3.7 Information Component – The Critical Common Threads

The five critical infrastructure sectors are shown in figure 3.5. The information component is the common element that connects all these infrastructures is accessible from any point on the globe to cause disruptions by use of Information Warfare techniques.

The increased usage and dependency for government, commerce, and national security applications therefore drive the numerous concerns about the vulnerability of these information systems as attacks on critical national infrastructure through the NII is a serious national concern.

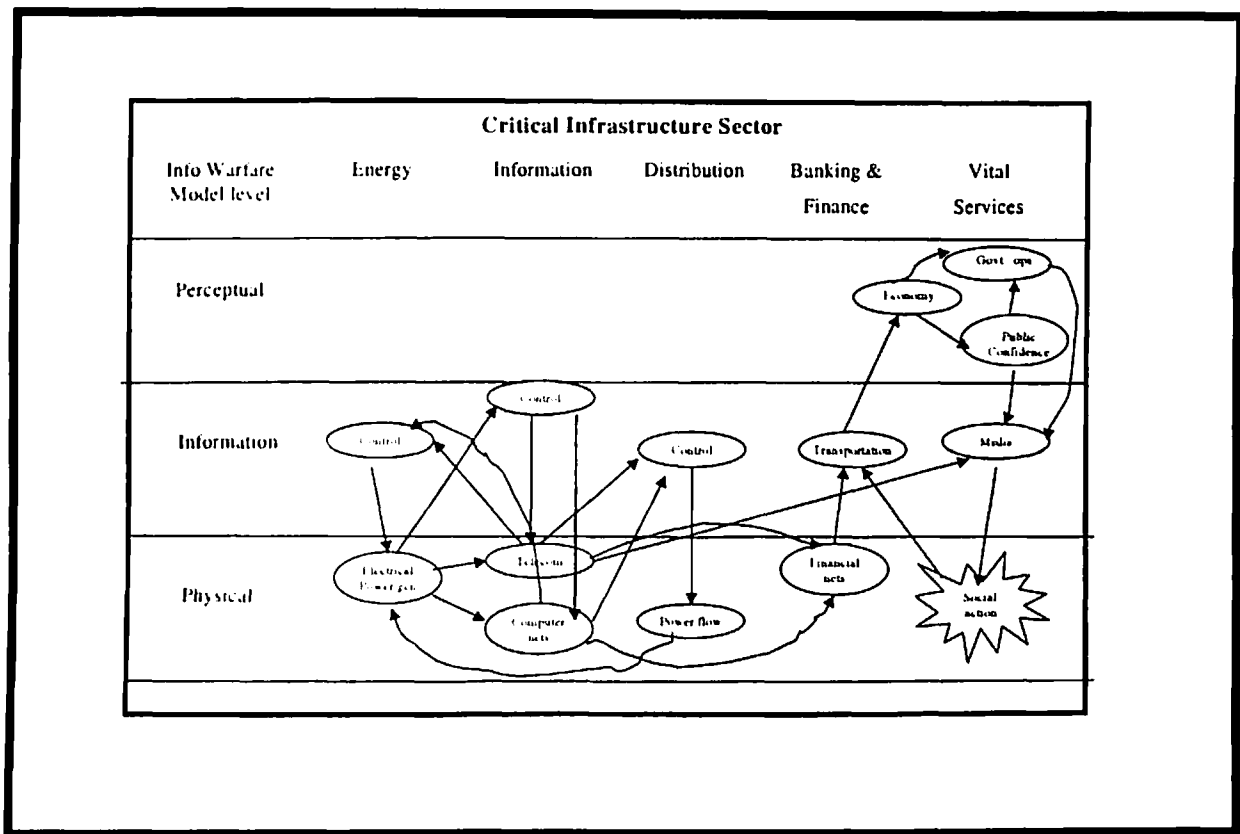


Figure 3.5: Influences Across the Critical Infrastructures.

3.8 Interdependencies Cause Serious National Security Risks

There are extensive natural interdependencies between the critical infrastructure sectors that can be exploited in information attacks across the elements. The controlling leadership of each critical sector, and its perception of the situation, may be a target of attack through the lower information or physical levels of the infrastructure. The figure highlights the effectiveness of information-based attacks, which have the ability to rapidly spread influences across sectors.

- Infrastructure protection requires defenses to prevent and mitigate the effects of physical or electronic attack.
- Infrastructure assurance requires actions to ensure readiness, reliability, and continuity restricting damage and providing for reconstitution in the event of an attack.
- Electrical power production and distribution would be required to sustain long-term telecommunications and computer networks.
- Telecommunications and computer networks would also be required to maintain assured power production and distribution.
- Telecommunications and computer networks are also required to provide electronic transactions in the banking, securities and market infrastructure.
- Proper operation of the banking and finance infrastructure would be necessary to maintain the perception of economic stability, which directly influences public confidence in the economy and in government operations. A cascading attack on a fractional banking system, for example, need not attack all banks. A successful attack on only the most vulnerable (for example Reserve Bank of India), followed by

effective widespread publication of that success, may be all that is necessary to destabilize all banks in the system.

- Media reports about disruption in the government operations can reduce the public confidence in them. This is dependent upon the information infrastructure to produce and distribute media messages.
- Physical social actions such as commerce and economic decisions, and influence on center and state governments are influenced by the media and they further influence financial transactions and the economy.

These relationships, at national level illustrate the complex interdependencies between infrastructure elements and the critical role that information would play in the network. The attacks, integrated across all elements of critical infrastructure and targeted at levels of the NII, will attempt to destabilize the balance and security of these operations. The objective and methodology of the enemy would be as follows:-

- Achieve perception objectives at the perceptual level, causing leadership to behave in a desired manner.
- This perception objective would be achieved by influencing the components of the critical infrastructure at the application level.
- This influence on the critical infrastructure would be accomplished through attacks on the information infrastructure, which can be engaged at the physical, information, and perceptual layers.

3.9 The Changing Nature of Critical Infrastructure Protection

3.9.1 Pre-Cyber Age

In the past the efforts for protection of critical infrastructure was limited to utilities such as power plants and grids, oil and gas pipelines, telecommunication, and facilities that affected the continuity of government. These facilities were the only forms of infrastructure protection to receive major funding in the context of a war or nuclear disaster. The response relied largely on the existing law enforcement capabilities and those resources already required for dealing with accidents, weather, and acts of God. The threat posed by other perpetrators such as terrorists, extremists, criminals, and ideologically motivated individuals was seen as too limited and to justify action beyond the self-protection measures taken by individual companies and institutions involved, and routine law enforcement. Even the most serious attempts at sabotage – usually by disgruntled employees -- historically was in the “noise level” of the damage done by accidents, weather, and acts of God.

3.9.2 Cyber Age CNI Vulnerabilities

Ensuring that essential services and industries survive a crisis has always been a part of our national security strategy. What is new is that Computer networks have created extremely complex linkages and interdependencies that have never existed before, and majority of critical infrastructures is outside the government control. Consequently, identifying what is critical is becoming both more difficult and more vital. The

Information Age, in bringing us an exciting new era of technology, has also given us a new set of security problems. This system of systems is extremely vulnerable to natural or manmade threats and vulnerabilities, as evident by the following statement of Osama Bin Laden. "It is very important to concentrate on hitting the U.S. economy through all possible means . . . look for the key pillars of the U.S. economy. The key pillars of the enemy should be struck . . .— Osama Bin Laden, December 27, 2001.

- Computer networks create new avenues for those with malicious intent. While still vulnerable to actual destruction by physical attacks, such as bombs or arson, these networks are targets of threats of mass disruption. Our economy can be crippled by strategic information warfare in the form of computer intrusions, scrambling software programs, undetected insiders within computer firewalls, or cyber-terrorists around in the world. Severity of computer attacks can vary from mere annoyances that disrupt business for a few hours to attacks designed to shut down or cripple entire systems.
- The integration of telecommunications and computer systems into energy, transportation, human services, telecommunications, finance, and civilian government sectors also includes the Armed Forces. It has been estimated that over 95 percent of defense communications in the USA rely on the public phone system which is equally applicable to us. Accordingly there is a need to develop a “strategy” for:
 - Identifying what is critical and vulnerable.
 - Increasing two-way information sharing between the public and private sectors.
 - Improving analysis and warning capabilities.
- In a study concluded by the Joint Economic Committee of US Congress in May 03, following had emerged [176]
 - Most agencies had not identified their mission-essential infrastructure assets.
 - Almost none of the agencies had completed their vulnerability assessments of their assets or developed remedial plans.
- The chart in figure 3.6 highlights the status of assessments in various sectors:

Infrastructure Sector	Vulnerability Assessment	Remedial Plan
Banking and finance	Some assessments	No / Few remedial plans
Electric power, oil, and gas	Some assessments	No / Few remedial plans
Emergency fire services	No assessments	No / Few remedial plans
Emergency law enforcement	No assessments	No / Few remedial plans
Information and communications	No assessments	No remedial plans
Public health services	No assessments	No remedial plans
Transportation	No assessments	No remedial plans
Water supply	Some assessments	No remedial plans

Source: Report of JEC, US Congress titled "Security in the Information Age", May 2002.

Figure 3.6: Sector wise Vulnerability Assessment Plan

- Our Infrastructure Owners and the central and state governments are facing a steep learning curve as they begin to assess its new technological vulnerabilities and security threats. We must begin developing a strategy that includes the private sector and the government, utilizing the strengths of each. A comprehensive strategic approach to infrastructure protection must include identifying what is critical and vulnerable, increasing information sharing, and improving analysis and warning.
- It is imperative to think "horizontally," to be mindful of the connections between physical buildings and networks in cyberspace that create complex interdependencies in which the weakest links become targets. These interdependencies require us to think differently about security.

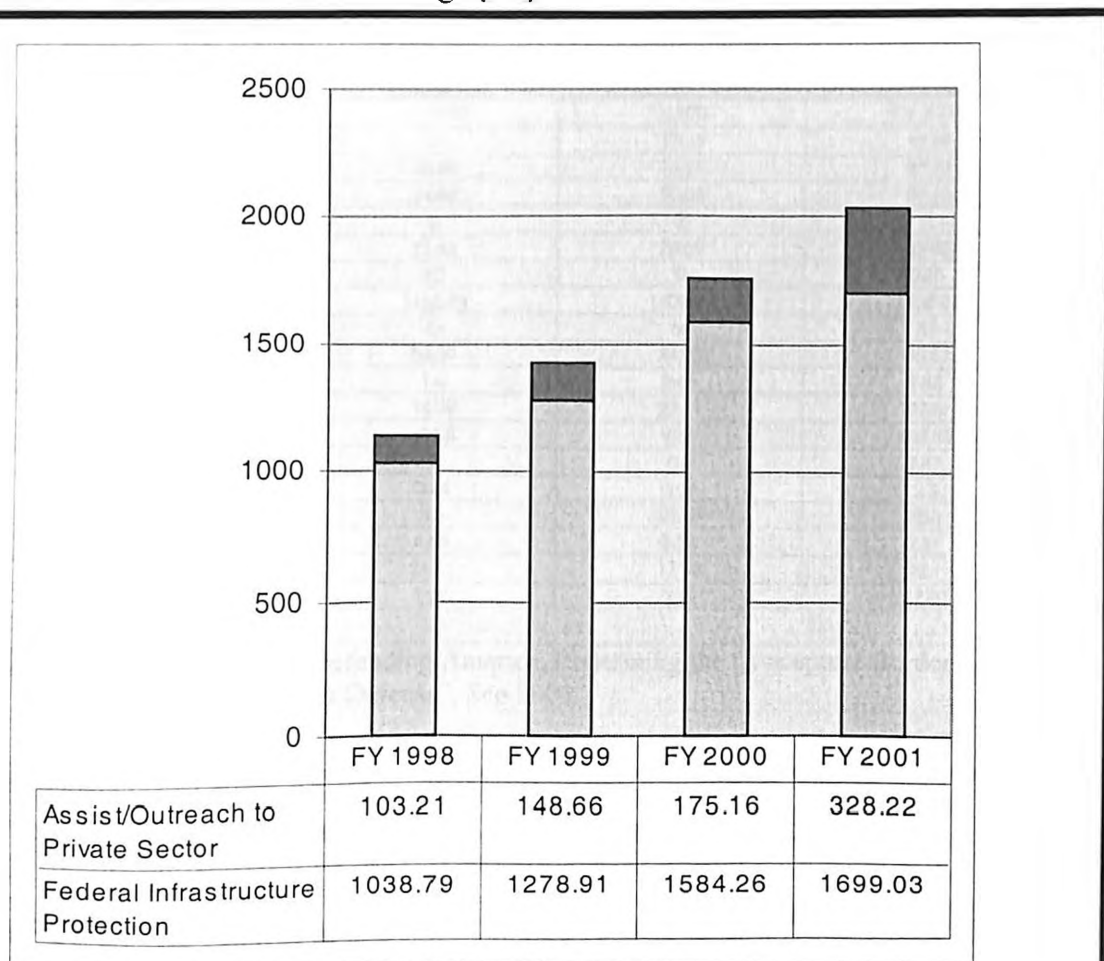
3.9.3 Cyber Age Protection Strategy

During the last two decades, the infrastructure underpinning the economy has fundamentally changed. It has steadily increased its reliance on its service sector and high technology economy and increasingly relies on computers, electronic data storage and transfers, and highly integrated communications networks. The result is a new form of critical infrastructure, one that is vulnerable to a new family of threats, loosely grouped together as information warfare. There is no way to forecast precisely how this new infrastructure will the new generation products are being released every six to nine months. Information systems are steadily becoming a more critical aspect of the economy, government, and national security at every level. These systems are

increasingly being linked and integrated both on a national and global level, and have already radically changed the way we do business. While physical damage to the nation's infrastructure remains a problem, information systems can be attacked electronically from anywhere in the world, posing a new kind of Information Warfare threat to nation's critical infrastructure.

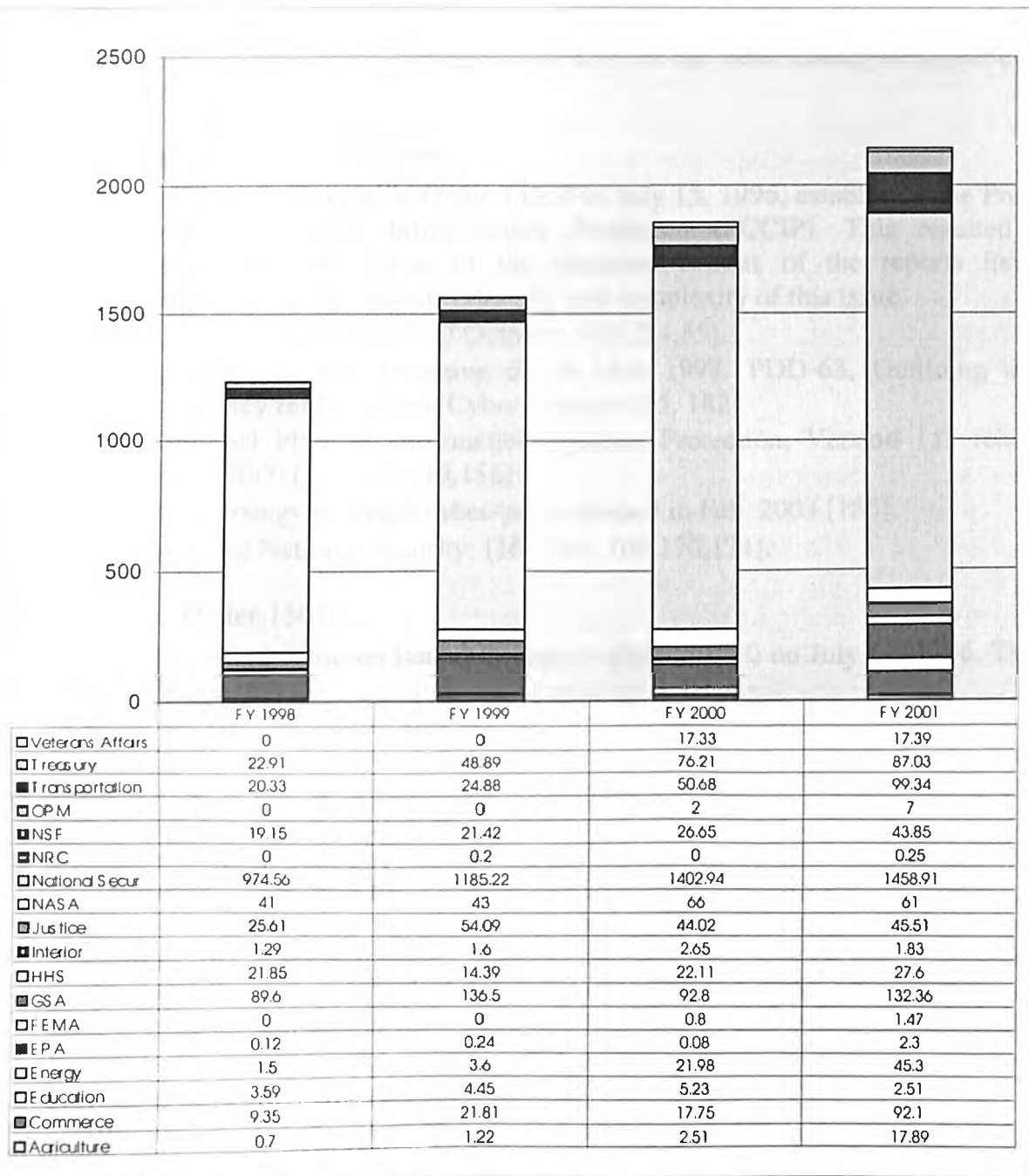
This process of change needs to be recognized by government, as well as civil and private sector users of information systems, to fundamentally reassess the role they must play in critical infrastructure protection.

The "pre-computer" officials and managers must try to cope with a technology, economy, and society they no longer fully understand, as this "generation gap" has not existed since the early 19th century, and the peak periods of change during the industrial revolution. In this regard the concern of the US government is evident from the funding for critical infrastructure protection which has risen from 1.14 billion in FY 98 to \$2.03 billion in FY 01 as shown in figures 3.7 and 3.8 The private sector is also learning to cope with the fact that its growing dependence on IT creates new threats vulnerabilities, patterns of crime and risks of sabotage [46].



Source: Draft Report of CSIS, US titled, Defending America, Redefining the Conceptual Borders of Home & Defense, Sep 2000.

Figure 3.7: Activity wise USA spending on CIP for FY 1998 - FY 2001



Source: Draft Report of CSIS, US titled, "Defending America, Redefining the Conceptual Borders of Home & Defense", Sep 2000.

Figure 3.8: Agency wise US spending on CIP for FY 1998 - FY 2001

3.10 Survey of Critical Infrastructure Protection Initiatives Across the Globe

In the wake of emerging network economy nations across the world are sensitized to the cyberspace threats and vulnerabilities, which can range from disruption of economic activity, social and political disturbances and also national security threats. Consequently national level programs identify and address these threats and

vulnerabilities are underway in Europe, Australia, China, USA etc. The literature survey reveals that US has taken a lead in this area which has been further strengthened after 9 September 2000.

3.10.1 Overview of US CIP Initiatives

President Clinton's Executive Order 13010 of July 15, 1996, established the President's Commission on Critical Infrastructure Protection (PCCIP). This resulted in the following actions [46]. Some of the recommendations of the reports have been reproduced to signify the volume critically and complexity of this issue.

- PCCIP. Commission report of October 1997 [34,35].
- Presidential Decision Directive 63 of May 1998. PDD-63, Outlining the Base Federal Policy for Protecting Cyber Systems [95, 182].
- The National Plan for Information Systems Protection, Version 1.0. released on January 7, 2000 [108,140,149,156]
- National Strategy to secure cyberspace released in Feb. 2003 [185].
- Roadmap for National Security: [161,166, 169,170,171].

3.10.2 Executive Order 13010:

The Clinton Administration issued Executive Order 13010 on July 15, 1996. This order recognized that

"Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats"). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation."

This is signified by the following statements by former US President William J Clinton and General John M Shalikashvili, Chairman JCS, USA. The threat to our military and commercial information systems poses a significant risk to national security and must be addressed". William J. Clinton, President of the United States

" Information in all its forms, information protection and the increasingly prominent position of information in the attack have become central features in determining the outcome of modern and future conflicts." General John M. Shalikashvili Chairman of the Joint Chiefs of Staff"

3.10.3 The President's Commission on Critical Infrastructure Protection

The PCCIP report of October 1997.

- "The US' growing dependence on information systems to run critical infrastructures leaves the country more vulnerable to both physical and, more importantly, cyber threats
- The rapid spread of the computer related technology has given more people the tools to cheaply and effectively strike at critical infrastructures
- Threats to critical infrastructures come from a wide variety of sources
- There is a lack of awareness concerning the vulnerabilities faced
- There is no national focus or advocate for infrastructure protection
- Infrastructure assurance is a "shared responsibility" and calls for the adoption of infrastructure protection best practices, increased research and development, and the adoption of a national organization structure".

3.10.4 Presidential Decision Directive-63.(PDD-63)

Based on PCCIP's recommendations, the Clinton Administration set forth a national "Policy on Critical Infrastructure Protection," also known as Presidential Decision Directive-63 (PDD-63) on May 23, 1998. The PDD-63 identifies CIP as "those physical and cyber based systems essential to the minimum operations of the economy and government. They include, but are limited to telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private." It recognized that Increased Automation of Infrastructure is so Dependent on Information Systems that Critical Infrastructure Protection must be tied to Information Warfare [35].

3.10.5 National Infrastructure Assurance Plan

The Principals Committee was also tasked with creating a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks.

- *"Vulnerability Analyses: For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector.*
- *Remedial Plan: Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities and funding.*
- *Warning: A national center to warn of significant infrastructure attacks will be established immediately. As soon thereafter as possible, we will put in place an enhanced system for detecting and analyzing such attacks, with maximum possible participation of the private sector.*
- *Response: A system shall develop a system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage.*
- *The Intelligence Community shall elevate and formalize the priority for enhanced collection and analysis of information on the foreign cyber/information warfare threat to our critical infrastructure.*

- *The Federal Bureau of Investigation, the Secret Service and other appropriate agencies shall: (1) vigorously recruit undergraduate and graduate students with the relevant computer-related technical skills for full-time employment as well as for part-time work with regional computer crime squads; and (2) facilitate the hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks.*
- *The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System. This evaluation shall include sponsoring an independent, integrated assessment of risks to civilian users of GPS-based systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations.*
- *The Federal Aviation Administration shall develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks.*
- *GSA shall identify large procurements (such as the new Federal Telecommunications System, FTS 2000) related to infrastructure assurance, study whether the procurement process reflects the importance of infrastructure protection and propose, if necessary, revisions to the overall procurement process to do so.*
- *OMB shall direct federal agencies to include assigned infrastructure assurance functions within their Government Performance and Results Act strategic planning and performance measurement framework.*
- *The NSA, in accordance with its National Manager responsibilities in NSD-42, shall provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability information; establish standards; conduct research and development; and conduct issue security product evaluations".*

3.10.6 Cooperation with the Private and Civil Sectors

PDD-63 called for the federal government to expand the scope of its efforts to work with the private sector, and recognized that such cooperation is essential to information and critical infrastructure protection. The directive include the following:-

- *"The Department of Commerce and the Department of Defense shall work together, in coordination with the private sector, to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards.*
- *The Department of Justice and Department of the Treasury shall sponsor a comprehensive study compiling demographics of computer crime, comparing state approaches to computer crime and developing ways of deterring and responding to computer crime by juveniles".*

PDD-63 also recognized the need to foster a climate of enhanced public sensitivity to the problem of infrastructure protection and for an outreach program. It directed that the following actions be taken:

- *"The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall consider a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations.*
- *The National Academy of Sciences and the National Academy of Engineering shall consider a round table bringing together federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security.*
- *The intelligence community and law enforcement shall expand existing programs for briefing infrastructure owners and operators and senior government officials.*
- *The National Coordinator shall (1) establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign; and (2) in coordination with the private sector, launch a continuing national awareness campaign, emphasizing improving infrastructure security."*
- *Information Sharing and Analysis Centers (ISACs). Two of the proposed six private sector computer security centers have been established (banking and finance and telecommunications). We are working with the other four sectors to get their proposed ISACs operational in 2000.*
- *National Infrastructure Assurance Council. The President signed an Executive Order creating this advisory Council, last year. Its members are now being recruited from senior ranks of the IT industry, key sectors of the corporate economy, and academia".*

3.10.7 Assurance Plan Objectives

The plan set forth three objectives: prepare and prevent successful attacks on critical infrastructures, detect and respond, to assess and contain attacks quickly, and to build strong foundations. Ten programs were included in the plan to achieve these objectives.

- *"Prepare and Prevent Program 3: Identify Critical Infrastructure Assets and Shared Interdependencies and Address Vulnerabilities*
- *Detect and Respond Program 2: Detect Attacks and Unauthorized Intrusions*
- *Program 3: Develop Robust Intelligence and Law Enforcement Capabilities to Protect Critical Information Systems, Consistent with the Law*
- *Program 4: Share Attack Warnings and Information in a Timely Manner*
- *Program 5: Create Capabilities for Response, Reconstitution, and Recovery*
- *Build Strong Foundations*
- *Program 6: Enhance Research and Development in Support of Programs 1-5*
- *Program 7: Train and Employ Adequate Numbers of Information Security Specialists*

- *Program 8: Outreach to Make Americans Aware of the Need for Improved Cyber Security*
- *Program 9: Adopt Legislation and Appropriations in Support of Programs 1-8*
- *Program 10: In Every Step and Component of the Plan, Ensure the Full Protection of American Citizens' Civil Liberties, Their Rights to Privacy, and Their Rights to Protection of Proprietary Data"*

3.10.8 Studies and Research

PDD-63 recognized that there were many areas where the federal government lacked the information to develop an effective critical infrastructure program. It directed the National Coordinator to commission studies on a wide range of legal and regulatory issues

- *"Liability issues arising from participation by private sector companies in the information sharing process.*
- *Existing legal impediments to information sharing, with an eye to proposals to remove these impediments, including through the drafting of model codes in cooperation with the American Legal Institute.*
- *The necessity of document and information classification and the impact of such classification on useful dissemination, as well as the methods and information systems by which threat and vulnerability information can be shared securely while avoiding disclosure or unacceptable risk of disclosure to those who will misuse it.*
- *The improved protection, including secure dissemination and information handling systems, of industry trade secrets and other confidential business data, law enforcement information and evidentiary material, classified national security information, unclassified material disclosing vulnerabilities of privately owned infrastructures and apparently innocuous information that, in the aggregate, it is unwise to disclose.*
- *The implications of sharing information with foreign entities where such sharing is deemed necessary to the security of United States infrastructures. The potential benefit to security standards of mandating, subsidizing, or otherwise assisting in the provision of insurance for selected critical infrastructure providers and requiring insurance tie-ins for foreign critical infrastructure providers hoping to do business with the United States".*

3.10.9 National Plan for Information Systems Protection, Version One

The "National Plan for Information Systems Protection, Version One" called for "the establishment of the U.S. government as a model of information security, and the development of a public-private partnership to defend our national infrastructures." It also outlined the following key initiatives to protect the federal government's computer systems that had been developed and provided full or pilot funding:

- *"Working to Recruit, Train and Retain Federal IT Experts. We have developed and provided FY2001 funding for a Federal Cyber Services Training and Education initiative led by OPM and NSF which calls for two programs: the first is an ROTC-like program where we pay for IT education (B.S. or M.S.) in exchange for federal*

service; and the second is a program to establish competencies and certify our existing IT workforce.(\$25 million)

- *Conducting federal agency vulnerability analyses and developing agency CIP plans. Federal agencies have all developed CIP plans, and these have been reviewed by a newly created "Expert Review Team" (ERT) of federal computer security experts. We have also established the ERT as a permanent team (at the Commerce Department's NIST), with funding lines in FY2000 and 2001. (\$5 million)*
- *Designing a Federal Intrusion Detection Network (FIDNET). To protect vital systems in Federal civilian agencies, we are providing funding for development of a cyber "burglar alarm" which alerts the federal government to cyber attacks, provides recommended defenses, establishes information security readiness levels, and ensures the rapid implementation of system "patches" for known software defects. (\$10 million)*
- *Piloting Public Key Infrastructure Models. The Clinton Administration is funding seven PKI pilot programs in FY2001 at different federal agencies. (\$7 million)*
- *Developing Federal R&D Efforts. In addition to the Institute, we have worked to ensure that R&D investments in computer security will grow more than 35% in the FY3003 budget. (\$621 million)*
- *Building the Public-Private Partnership. The President is committed to building partnerships with the private sector to protect our computer networks through the following initiatives:*
- *Institute for Information Infrastructure Protection. Building on a Science Advisory Panel, we are proposing to create an Information Infrastructure Institute which would combine federal and private sector energies to fill the gaps in critical infrastructure R&D that are not now being met in the private sector or the Department of Defense. It would also provide demonstration and development support in key areas like benchmarks and standards, and curriculum development. (\$50m)*
- *Partnership for Critical Infrastructure Security. This alliance of more than ninety Fortune 500 companies is spearheaded by Secretary Daley and had a successful kickoff in New York on December 8th. We will build on this partnership to provide public education and cooperation with the private sector on a wide variety of information security issues."*

3.9.10 The US President's office report titled "The National Strategy to Secure Cyberspace Feb 2003 " has addressed the cyberspace security on five events as shown in figure 3.9. The five levels addressed encompass small / home users of information system large enterprises critical sectors / infrastructures, national issues and vulnerabilities and the global issues. The report seeks implementation of security and protection measures for each these infrastructure categories in a phased manner with duly assigned priority and role and responsibilities [29,30,31,185].

Roles and Responsibilities in Securing Cyberspace					
	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5
	National Cyberspace Security Response System	National Cyberspace Security Threat and Vulnerability Reduction System	National Cyberspace Security Awareness and Training Program	Securing Governments Cyberspace	National Security and International Cyberspace Security Cooperation
Home User/Small Business		X	X		
Large Enterprises	X	X	X	X	X
Critical Sectors/ Infrastructures	X	X	X	X	X
National Issues and Vulnerabilities	X	X	X	X	
Global					X

Source: US, White House Report titled " The National Strategy to Secure Cyberspace, Feb.03"

Figure 3.9: 5 Level Threat & Vulnerability Model

3.11 Infrastructure Assurance Issues

A conceptual overview of infrastructure assurance is needed. This should outline challenges related to who protects infrastructures and what the role of the government should be in ensuring essential government services and orderly operation of the national economy. Some of these are enumerated below.

3.11.1 Cyber Security Policy

Advocating the need for a true national debate on infrastructure assurance, there is a need to rethink national security strategy—and, by extension, economic security and our nation’s security from a military perspective. An approach to critical infrastructure protection and information assurance centered on three “prongs”: policy, technology, and people is needed.

3.11.2 National Information Power

We require a national information strategy designed to support a broad range of policy goals, a balanced approach to the strategic concept, which may defend a defined set of information equities, culled from the vast body of information that surrounds our daily lives.

3.11.3 Cyber Early Warning

We require strategic early warning capabilities, which can enable us to detect and deter potential IW attacks. We also require components of historical warning models to early warning for cyber attacks demonstrate the complexity of the challenge, the need for

burden sharing for the development of warning capabilities and a series of private sector issues requiring more thoughtful consideration.

3.11.4 Transitions between Law Enforcement and National Defense

In response to criminal activity, law enforcement and national security personnel have struggled to remain effective in an increasingly complex technological world. What we need now is further interaction between law enforcement and national defense and the integration of their respective efforts, the security dilemma, the public safety/ national security conundrum and the evolving role of private markets.

3.11.5 The Defense and CIP

An integrated legal, policy, and management philosophy to support critical infrastructure protection efforts.

3.11.6 Definitions of National Security

Defining national security and national interests in the context of the changing geopolitical environment, with particular emphasis on the challenges of diffuse and asymmetrical threats and the rapid increase in global connectivity and technological interdependence.

3.11.7 Counterintelligence and CIP

Identifying the inseparability of critical infrastructure protection and counterintelligence, the need for collaborative government-private efforts to address a wide range of policy challenges.

3.11.8 Risk Management

Risk management process involved in assuring delivery of critical infrastructure services, a range of business approaches to prevention or deterrence, mitigation, and crisis management and recovery. While each national agency has an economic and public interest to assure its own service, concerted attention and action is required to assure that disruptions to networks supporting one part of the infrastructure system do not cascade.

3.12 NII Architecture from Security Point of View

Three functional layers to characterize the technical architecture of NII that emphasize the information services and applications have been presented in figure 3.6. At the lowest level are bitways, the physical information pathways made up of network computers, landlines (coaxial and fiberoptic cables), satellite links, and wireless cellular links. The figure 3.10 compares the seven layers of the Open System Interconnection (OSI) reference model, which emphasizes the network sub layers, with the three NII functional layers.

<u>NII Layer</u>	<u>Description</u>	<u>Representative Components</u>	<u>OSI Model Layers</u>
Applications	Tools and application programs that perform specific functions for a variety of disciplines, using the NII	<ul style="list-style-type: none"> • Electronic commerce, Energy management, • Health care, Law, enforcement, • Environmental monitoring. 	7 Application
Services	The basic capabilities that from the building blocks for applications, including I/O, basic processing, displays, and data fusion/mining etc.	<ul style="list-style-type: none"> • Data Storage and retrieval, Data exchange, • Protocol translation, Metaknowledge (indexes), Multilevel security, Electronic transactions, Information agents, Collaboration support, • Data fusion and mining. 	
Bitways	The physical infrastructure that provides the means of transmission of information, including controlling software	<ul style="list-style-type: none"> • Fiber-optic and cable, landlines, • Satellite links, • Satellite direct broadcast, Cellular Wireless, Telecommunications, Network nodes (switches, routers, exchanges). 	6 Presentation 5 Session 4 Transport 3 Network 2 Link 1 Physical

Figure 3.10: NII Security Architecture

The services level integrates the bitways into a functional NII architecture, providing common utilities to integrate the bit ways, to route, retrieve and store information, and provide seamless operation. The security would have to be addresses at each of the OSI layer.

3.13 Volume and Complexity of NII & GII Security

India's NII is still evolving and is expected to mature by the year 2005-2007. The NII would be gradually telescoped and dovetailed with the APII and GII. Following vulnerabilities to NII, APII and GII are foreseen. [30,134,139]

3.13.1 NII security

NII would weave through every computer and network in its functional and physical form across the continental landmass of India. This would also include island territories influencing at the level of individual, corporate, state and national interests in economic, social, political and military sense, spanning over 65 central ministries, 35 state governments and union territories and their counterparts in the private sector. Its volume and complexity would be enormous and unprecedented.

This NII must function uninterrupted for all the 365 days of a year under all circumstances against any type of information warfare threat. This would require a NII security overlay of very large dimensions and complexity involving confidentiality, integrity, non-repudiation, identification, authentication, access control, surveillance, control, monitoring contingency planning, disaster control etc. A large part of this security overlay in terms of architecting, policies and processes would have to be homegrown due to obvious fears of IW and import restrictions. This would require a national information security initiative involving very large investments in terms of money and human talent.

3.13.2 GII (including APII) Security Issues

As brought out above the intent of GII has been to ensure that the full potential benefit of advances in information and telecommunications technologies are realized for all citizens of the world in equal measure. The idea is to create a global information market place, encouraging broad-based social discourse within and among all countries to encourage broad-based social development within and among all countries to increase economic growth, create jobs and improve infrastructures [16,76].

Against this background, the vulnerability of GII and its compounding effect on NII is extremely large and crippling. Therefore security and regulatory issues in terms of ownership, operations, international laws, social and cultural values need to be examined and addressed keeping our own national interests in view.

3.14 Security Overlay for NII

Economic and military related NII is extremely prone to disability or damage through attack by vested interests within the country or from across the border. The threat of Information Warfare to NII is equally applicable to civil as well as military sectors. The inter-dependencies and reliance on civil NII is so critical that no meaningful war effort can be sustained by the Armed Forces without all time availability of at least critical segments of NII in civil sector as shown in the figure 3.1.

On the other hand the economic activity is becoming key to the survival at national and global scale. This activity has its roots in Corporate Information Infrastructure (CII), which is equally critical segment of NII and needs to be engineered with same care and caution. Therefore, for the country to emerge as global economic and military power, the entire NII including CII must be able to operate in a hostile environment.

3.14.1 Security Goals of NII

The security goals for the NII are as follows:

- Uninterrupted availability of NII sources
- Uninterrupted economic activity in terms of e-governance, e-commerce, electronic fund transfer etc
- Comprehensive business continuity measures for vulnerable portions of NII assets
- State of practice, practical, cost effective, sustainable security model and policy
- Trustworthy and responsive NII to the Constitutional and Sovereign rights and privileges of our citizens

3.14.2 Components of the NII Security Overlay

The security related solution specific components that can be suitably transposed to NII are as follows:

- Technologies and processes for Identification, Authentication and Access Control system for physical and logical access to computer systems, software, applications, databases and networks
- Technologies and processes that can ensure data and message confidentiality, availability, integrity and trustworthiness anywhere on NII at all times of the year during peace or war
- Technologies and processes that can enable round-the-clock monitoring, surveillance and control over sensitive NII resources
- Technologies processes and practices which can prevent damage or disability to sensitive NII nodes against non-nuclear weapons as well as prevent monitoring of sensitive NII nodes by enemy
- Technologies and processes that enable us to monitor networks of interest to our own economic and military agencies
- Technologies and processes that enable us to put in place the working systems for disaster management, control and recovery
- Technologies and processes that enable us to develop and integrate IW-Defense and IW-Offense capability of our Armed Forces and other security agencies in civil sectors. A generic NII security overlay is illustrated in the figure 3.11

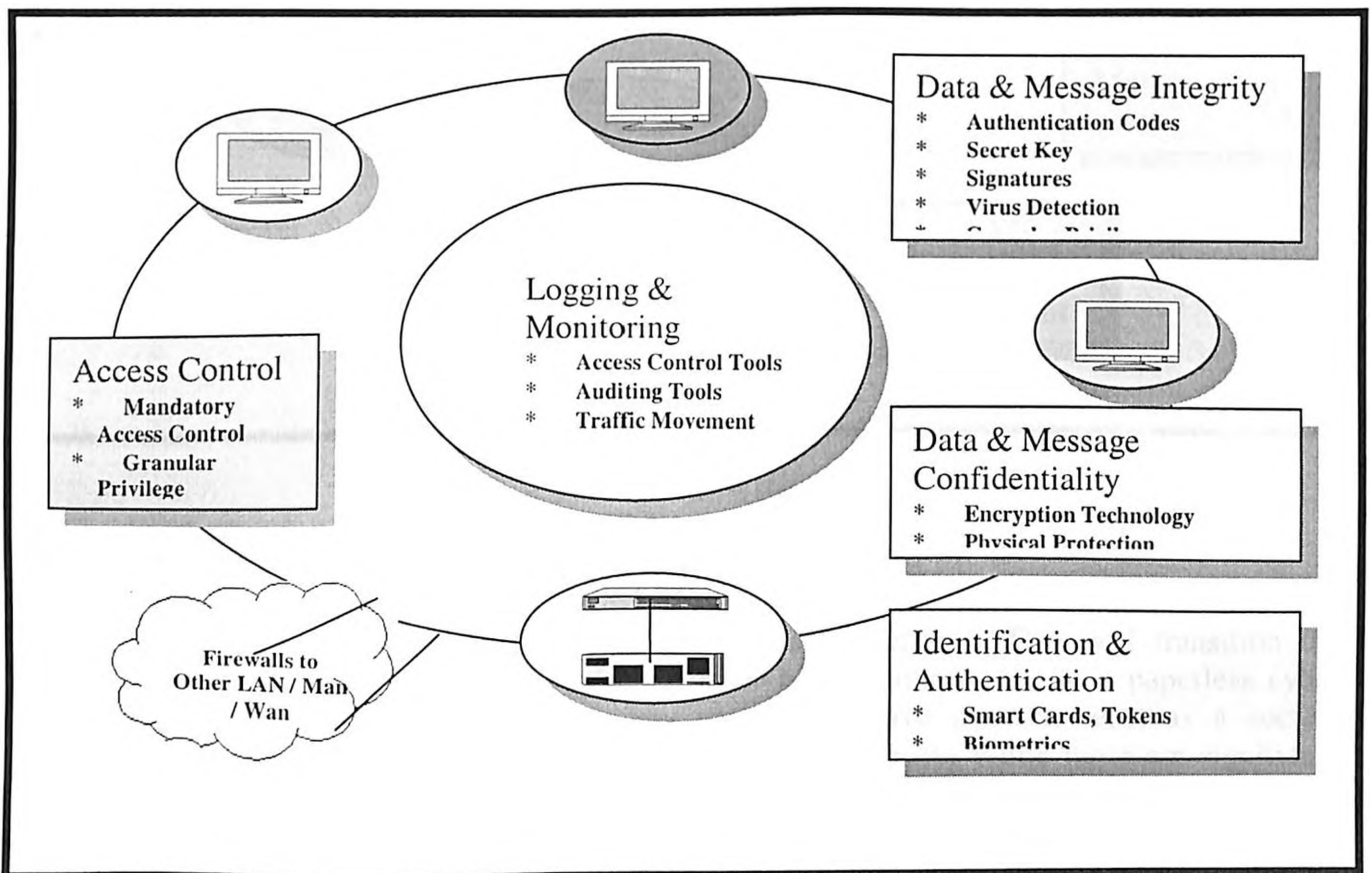


Figure 3.11: Integrated Information Infrastructure Security Overlay

3.14.3 NII Security Model

A generic NII security model encompassing information security, computer security, network security, database security, physical security, personnel security along with support process and frameworks for vulnerability assessment, business continuity management, security management, counter virus counter measures is presented in the figure.3.12

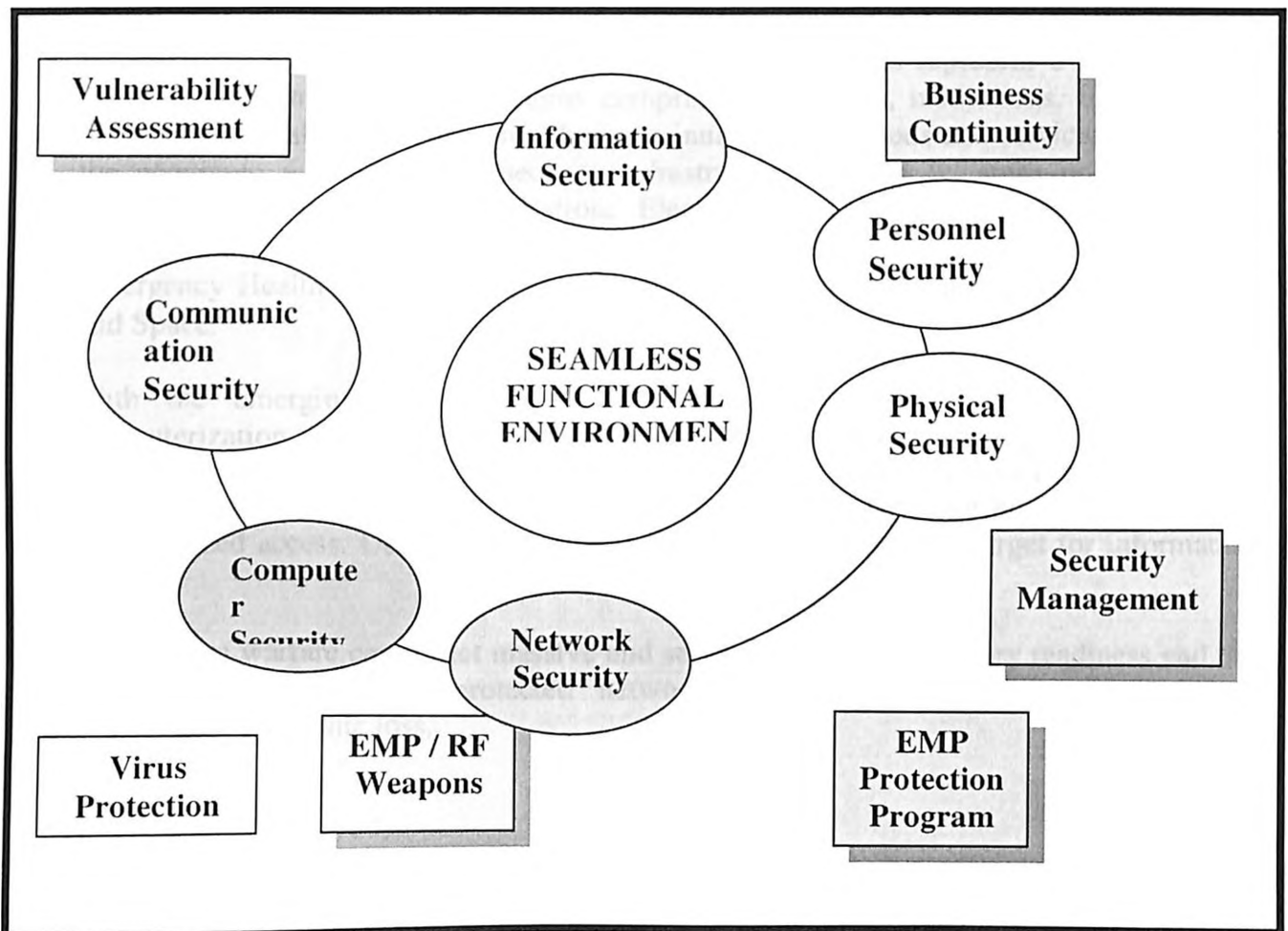


Figure 3.12: Security Model

3.15 Conclusion

In this chapter we have concluded that intensity and inertia of Information and Communication Technology (ICT) revolution is irreversible. This will transition the centuries old and significantly perfected paper based environment to a paperless cyber environment thereby changing the way we live, behave interact, react as a society affecting us socially, economically, politically and militarily. While these are significant gains of this forward movement into cyber space, there are very serious concerns about the safety, security and trustworthiness of the underlying NII that would support the new environment. It emerges that the concerns span across all infrastructures viz. Energy, information distribution banking, financial and vital services which constitutes the critical

foundations for our national level survival and sustenance. We have also concluded integration of NII with APII and GII makes our national cyber space borderless and extends it to the whole world. This extended connectivity borderless and extends it to the whole world. This extended connectivity makes it prone to Information warfare attacks from all parts of the world.

APII and GII have large dimensions and unprecedented complexity. In order to minimise or mitigate these vulnerabilities and threats, the need for a comprehensive security overlay and a robust security model has been signified and its building blocks have been identified. In the following chapters we will further examine and identify specific security issues of the cyber space. It emerges that the infrastructures represent a framework of interdependent networks and systems comprising industries, institutions, functions and distribution capabilities. They provide a continual flow of goods and services essential to the economic well-being and security infrastructure defined by areas or sectors viz. Banking and Finance: Transportation: Electric and Gas (Power): Information and Communications (Telecommunications): Law Enforcement: Government Services: Fire: Emergency Health Services: and the Water Supply. Health Affairs: Personnel: Logistic and Space.

With the emerging NII, we as a nation are becoming heavily dependent on computerization and networking for military operations, governance, global commerce, and industrial activity. The information infrastructure of critical national infrastructure is at grave risk to natural or man made attacks. Data and systems are highly vulnerable to unauthorized access. Use of networking makes us most vulnerable target for information warfare.

Information warfare can inflict massive and serve disruption of military readiness and the economy. Reliance on unprotected networks carries risk of military failure and catastrophic economic loss.

PART- II
INFORMATION WARFARE AND EMERGING
SERIOUS THREAT TO NII

CHAPTER 4: INFORMATION AGE WARFARE

CHAPTER 5: INFORMATION WARFARE THREAT ASSESSMENT

CHAPTER 4

INFORMATION AGE WARFARE

4.1 Introduction

The emergence of microelectronics has led to the design of high performance military systems. The performance edge in terms of faster and accurate response emanates from embedded intelligence, which has proliferated into almost every facet of systems. Therefore, technologically advanced nations have produced platforms, weapon systems, delivery systems, command and control infrastructure which can provide them overwhelming superiority almost instantaneously in terms of detection of targets, location and targeting in any part of the globe, underwater, on surface or in space. Amongst these, a new breed of systems is emerging under the name of "Non-Lethal Weapons" or "Disabling Systems". Classes of these non-lethal weapons with computers as their basic building blocks have been termed as Information Warfare (IW) Weapons, which are aimed to disable, damage, deny, destroy or render enemy IT embedded systems completely ineffective.

The use of microelectronics has also proliferated equally deeper into systems in the civil sector. This wide spread use of IT products in communications, transport, finance, energy, engineering, health care, governance etc. has made the resulting infrastructures organized, efficient, intelligent and responsive. However these IT embedded system are becoming equally vulnerable to IW attacks.

In this chapter we have examined the potential of IT to turn into a war winning effort. Terms like "Cyber warfare", "Information Warfare" and "Net war" which are being used interchangeably in literature are analyzed and explained more precisely and mapped as Information Based Operations (IBO) resulting in Revolution in Military Affairs (RMA). The IW perspective has been examined and analyzed in respect of spread of IT as Information-in-War, IW spectrum, dimensions of IW, cyber war, infowar and netwar. It has been highlighted that IW is a new warfare paradigm, which affects civil and military IT infrastructures alike and thus has serious implications on the social, economic, political and military landscape of a country.

The impact of cyber war on the over all warfare perceptions and perspectives, the need to change doctrines at tactical and strategic level, alterations in organizational structure, force level, training etc., have been explained. It has been signified that IW is a stark reality facing our country and there is a need to prepare for it to give us a war winning advantage with deterrence posture near equal to nuclear capability.

4.2 Information Warfare Perception

There is a universal awakening to organize information. The computerisation and networking at most echelons of the governments and private sectors is underway all over the world. In times to come, this capability will enable all nations to effectively participate in economic, technological, political and other fields at global level. However in recent

times this type of information superiority is being planned to be exploited by the IT advanced nations in the form of an instrument of War termed as Information Warfare (IW).

The IW is defined as a war on target nations using information related principles, whereby the enemy information systems are disabled, damaged, denied or destroyed using own information systems in the form of weapons. At the same time IW also encompasses protection of own systems against all enemy attempts to disrupt or damage them. The IW therefore has both offensive and defensive elements. A class of IW weapons makes use of non-nuclear Electro Magnetic Pulse (EMP) or microwave energy to disable or damage microelectronics embedded in IT infrastructure. IW however does not entail collateral damage or harm to human beings as applicable to conventional and nuclear warfare. Therefore it emerges that all information systems in military, government or private sectors are prone to such attempts by the enemies with-in or from across the border at all times. during peace and war [144,150,184].

There is now a fear psychosis of IW amongst the third world or those countries, which politically, regionally or economically do not share common interests with IT advanced nations and their allies. These IT have-nots perceive that a day would come when this overwhelming superiority in non-lethal IW weapons would be utilized by the advanced nations to extract any advantage of political, regional or economic significance. Even the non-lethal use of these assets would assume "deterrence value" hitherto possible only with nuclear weapons. Today, the third world nations have virtually no defense against them.

The war objectives of IT advanced nations and their allies may not be emanating into World War type of destruction but it would emerge into a different type of cold war on the strength of IW weapons. Considering the emerging geopolitical situation, China, Pakistan, India, Malaysia, Middle East etc., may be the target nations for attacks with IW weapons because of very large economic potential of this region. The level and potential of vulnerability of these nations to IW may not be yet very apparent because such "Disabling Techniques" are yet being evolved and have not become "Disabling Systems" as part of warfare establishment.

Even if there is an evidence of this, developing nations are pre-occupied with economic, industrial, social and internal problems and are unable to recognize their vulnerability from such IW weapons. Moreover, the details about high-end of IW systems are not yet available in the open literature and the IT community in the developing nations is unable to comprehend this type of danger.

4.3 Evolution of IT Based Warfare

In order to understand the concept of IW, it is important to trace genesis of the three major societal transformations following first and second industrial revolutions followed by the current network revolution. These transformations in terms of significant gains in technology, institutions, culture, values and perceptions are illustrated in figure 4.1. The security consequences of these transformations in terms of main actors, reasons of conflict, methods of warfare and vulnerabilities have been shown in figure 4.2 [71].

	THE FIRST INDUSTRIAL REVOLUTION	THE SECOND INDUSTRIAL REVOLUTION	THE NETWORK REVOLUTION
Technology	<ul style="list-style-type: none"> • The steam engine • Textile industry • Railways • Telegraph 	<ul style="list-style-type: none"> • Electricity • Organo-chemical Industry • Car • Airplane • Telephone • Radio 	<ul style="list-style-type: none"> • Semiconductor • Computers • Digital networks (Internet) • Modeling & simulation • Modularity Interoperability through standardized interfaces • Bioinformatics • Telematics
Institutions	<ul style="list-style-type: none"> • The Joint -stock limited company • Modern capital markets • Rational bureaucracies • Mass newspapers 	<ul style="list-style-type: none"> • The Multi - division firm • The industrial R & D lab • Mass political movements • Cinema • Broadcasting 	<ul style="list-style-type: none"> • Network organizations • Process-and - project oriented organizations • Ventures Capital markets • Standards coalitions and R7D consortia • Issues-oriented networks • Electronic commerce
Culture, values and perceptions	<ul style="list-style-type: none"> • Uniform national culture • Urbanization • Literate, disciplined labor force 	<ul style="list-style-type: none"> • Global popular culture 	<ul style="list-style-type: none"> • Global niche cultures

Source : The Non proliferation Review / Spring –Summer 1999

Figure 4.1: Three major Societal Transformations: Examples of Key Novelties

	THE FIRST INDUSTRIAL REVOLUTION	THE SECOND INDUSTRIAL REVOLUTION	THE NETWORK REVOLUTION
Actors, reasons of conflict	<ul style="list-style-type: none"> • Nationalistic mass movement • Colonies 	<ul style="list-style-type: none"> • Totalitarian political movements 	<ul style="list-style-type: none"> • Niche players with a broad variety of agendas, including financial gain. • Rouge states, extremist movements.
Methods of warfare	<ul style="list-style-type: none"> • Conscript mass armies • Mass produced firearms • Railway-based logistic support 	<ul style="list-style-type: none"> • Machanized forces • Air power • Radio Communication • Radar • Weapons of mass destruction 	<ul style="list-style-type: none"> • High-performance special operations • Precision munitions • Cyber weapons
Vulnerabilities / targets	<ul style="list-style-type: none"> • Population centers 	<ul style="list-style-type: none"> • Infrastructure 	<ul style="list-style-type: none"> • Knowledge and information assets
Source: The Non proliferation Review / Spring –Summer 1999			

Figure 4.2: Three major Societal Transformations: Security Consequences

4.4 Information Based operations (IBO)

In order to understand the concept of IW it is important to trace the genesis of the recent Revolution in Military Affairs (RMA), which is powered by IT, and then examine where IW fits into it.

4.4.1 IT in Military Operations

According to US, DOD's office of Net Assessment [15] the IBOs are major change in the nature of warfare brought about by the innovative application of new technologies. These IBOs, combined with changes in military doctrines and operational and organizational concepts, fundamentally alter the character and conduct of military operations. The technological developments in military intelligence, surveillance and reconnaissance (ISR) systems, precision strikes capability and developments in command, control, communications, computers and intelligence (C⁴I) systems have resulted in profound changes in military operations and military organisations. The IBOs are means to dominant battlespace awareness by protecting friendly C⁴I and command and control warfare (C²W) systems and attacking the information - based enemy systems. The IBOs can be summarised as a combination of ISR, C⁴I, precision strikes and IW. However it can be argued that ISR, C⁴I and precision strikes are a mere evolution in technology and advancement of the concept of Information -in-War.

4.4.2 Defining C²W and IW

C²W is the integrated use of Operations Security (OPSEC), military deception, Psychological Operations (PSYOPS), Electronic Warfare (EW) and physical destruction, mutually supported by intelligence. The goal of C²W is to deny information, to influence, degrade or destroy adversary command and control capabilities, while protecting friendly C² capabilities against such actions. C²W is the first step in the transformation of the armed forces from the industrial model to the information model of warfighting. [130]

As explained above IW has been defined by the US Joint Staff as actions to attain information superiority by affecting adversary information, information-based processes, information systems and computer-based networks, while defending one's own information, information based principles implied in cyberwar and netwar. Cyberwar is conducting, or preparing to conduct military operations according to information-related principles. Netwar is societal level ideational conflict waged in part through inter-netted modes of communication. It is irrelevant whether declared or undeclared military conflict is involved. It might be argued that Netwar is to information warfare what cyber is to C²W. Netwar is likely to affect entities other than just the governments of nation-states and it will be based on information - related principles far beyond the mere communication to control or shape the enemy, especially the enemy battlespace, cyberspace does the same through information- related principles.

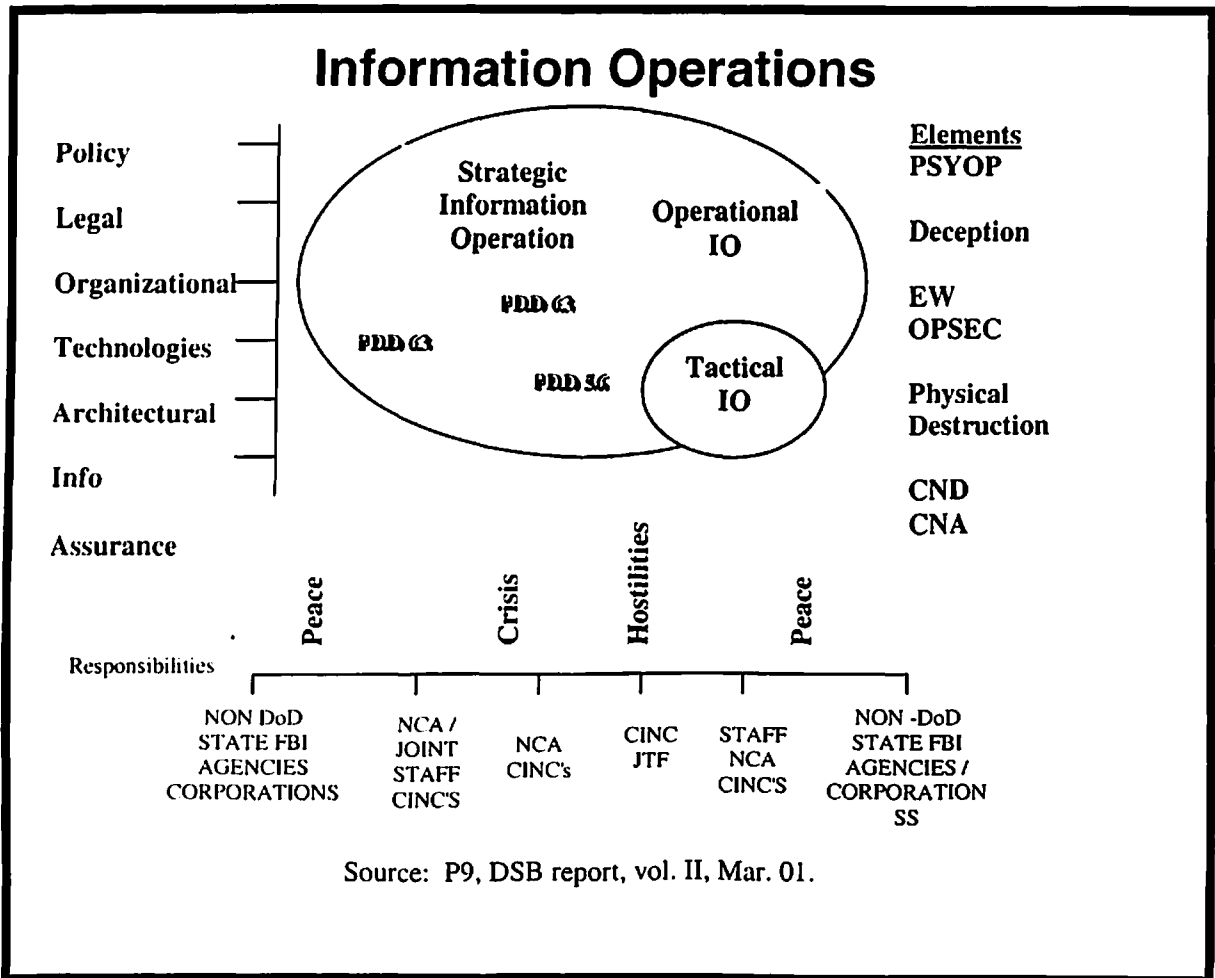
According to Martin C. Labicki there are seven forms of war or conflicts that involve the protection, manipulation, degradation, and denial of information. [130]. This characterisation of information warfare shows that it can be conducted against a country's military as well as its civil society. Against the military, information warfare could consist of command and control warfare, intelligence-based warfare (IBW) and electronic warfare, whereas against the society it could primarily consist of info-economic warfare and cyber war. Common denominators of information warfare for the military and society would be psychological warfare and computer hacking.

The C2W is the military strategy that implements information warfare on the battlefield and integrates physical destruction. The C2W is a subset of IW whose target is the command and control functions of the adversary's military forces and, when it incorporates the information attack concept, will approach cyberwar. Full cyberwar capabilities will require an extensive re-thinking of how to organise, train and equip to conduct warfare according to information related principles. Information attack, the sixth addition to the standard five pillars of C2W, as an operational mission with potential for strategic effect far from the battlefield, is a clear recognition that C2W information-in-war operations are far from exhausting the potential of IW.

4.4.3 Information Operations

The term Information Operations (IO) encompass a set of information-age warfare concepts tied to the ongoing rapid evolution of cyberspace, the global information infrastructure and new vulnerabilities of the high-value national assets outside the traditional battle space boundaries but critical to the conduct of military operations. The spectrum of information operations range from peace, to crisis, to hostilities, and back to

peace, and have characteristic actions and effects at the strategic, operational, and tactical levels.



Source: P9, DSB report, vol. II, Mar. 01.

Figure 4.3 Information Operations Systemic Issues

Information Operations responsibilities as defined in the Defence Science Board, USA (DSB) report (109,152), and shown in the figure 4.3 cross the boundaries between military and civil agencies with respect to authority, supervision, hand-off, response and coordination. The report has addressed these issues in categories including policy, legal, organization, operations, technologies, architectures and information assurance. The strategic IOs as applicable to IW signify the following:-

- Vulnerability of Entire National Landmass:** Information warfare has no front line. Potential battlefields are anywhere-networked systems allowing access. Economy will rely on increasingly complex, interconnected network control systems for such necessities as oil and gas distribution management, electric grids, telephone service, air traffic control and much, much more. The vulnerability of these systems is poorly understood. This lack of understanding and recognition inhibits a thorough assessment of the vulnerabilities that may exist in both the technology-driven control systems. In addition, the means of deterrence and retaliation are uncertain and may rely on traditional military

instruments in addition to information warfare threats. In summary, the interior of the country is equally prone to outside IW attack.

- **Low Entry Cost:** Interconnected networks may be subject to attacks and disruption by states, non-state actors, including dispersed groups and even individuals. Potential adversaries could also possess a wide range of capabilities. Cyber attacks have moved beyond the domain of the mischievous teenager and we are now being learned and used by terrorist organizations as the latest weapon.
- **Blurred Traditional Boundaries:** The wide array of opponents, weapons, and strategies makes it difficult to distinguish between foreign and domestic sources of information warfare threats and actions. It may not be known who is under attack by whom, or who is in charge of the attack.
- **Perception Management:** Opportunities for information warfare agents to manipulate information that is essential to public perceptions will increase.
- **Difficulty in Tactical Warning and Attack Assessment:** Due to difficulty in events such as accidents, system failures, or hacking by thrill seekers, it is difficult to assess the threats and generate warnings.

4.4.4 US Joint Vision 2020 - IT Intensive Paradigm

The US Armed Forces' concept for future warfare is formulated in the Joint Vision 2020 [109,152]. It is assumed that the technologies leading to information supremacy will provide dominant battlespace awareness. The Joint Vision 2020 proposes that new concepts of operations will need to be developed. These new concepts are dominant maneuver, precision engagement, full-dimension protection and focussed logistics. Dominant maneuver is an evolution of the US Army's Force XXI modernisation of Air-Land Battle in which the massed effects of ground and air maneuver are supplemented with some deep interdiction. Precision engagement is to be realized through system of systems made possible by a better use of C⁴I supported by intelligence, surveillance and reconnaissance. Full-dimensional protection is the protection of forces with air superiority and better defensive IW. Focussed logistics is the sustainment and logistical requirement of expeditionary forces projected from the continental United States. The dependencies of joint vision would pertain to the ability to detect, see, heal and track, capacity to move information, ability to process and fuse information, necessity to protect information compatibility and inter-operability, thereby signifying the role and relevance of IT and IW in realization of the Joint Vision.

4.4.5 Joint Vision 2020 and the Importance of Information Superiority

The Joint Vision 2020 (JV2020), builds upon and extends the conceptual template established by Joint Vision 2010, which guides the continuing transformation of America's Armed Forces. The primary purpose of these forces has been and will be to fight and win the nation's wars. The overall goal of the transformation described in JV2020 is the creation of a force that is dominant across the full spectrum of military operations – persuasive in peace, decisive in war, preeminent in any form of conflict. The overreaching focus of this vision is full spectrum dominance – achieved through the interdependent application of dominant maneuver, precision engagement, focused logistics, and full dimensional protection as shown in the figure 4.4 [96,97,109].

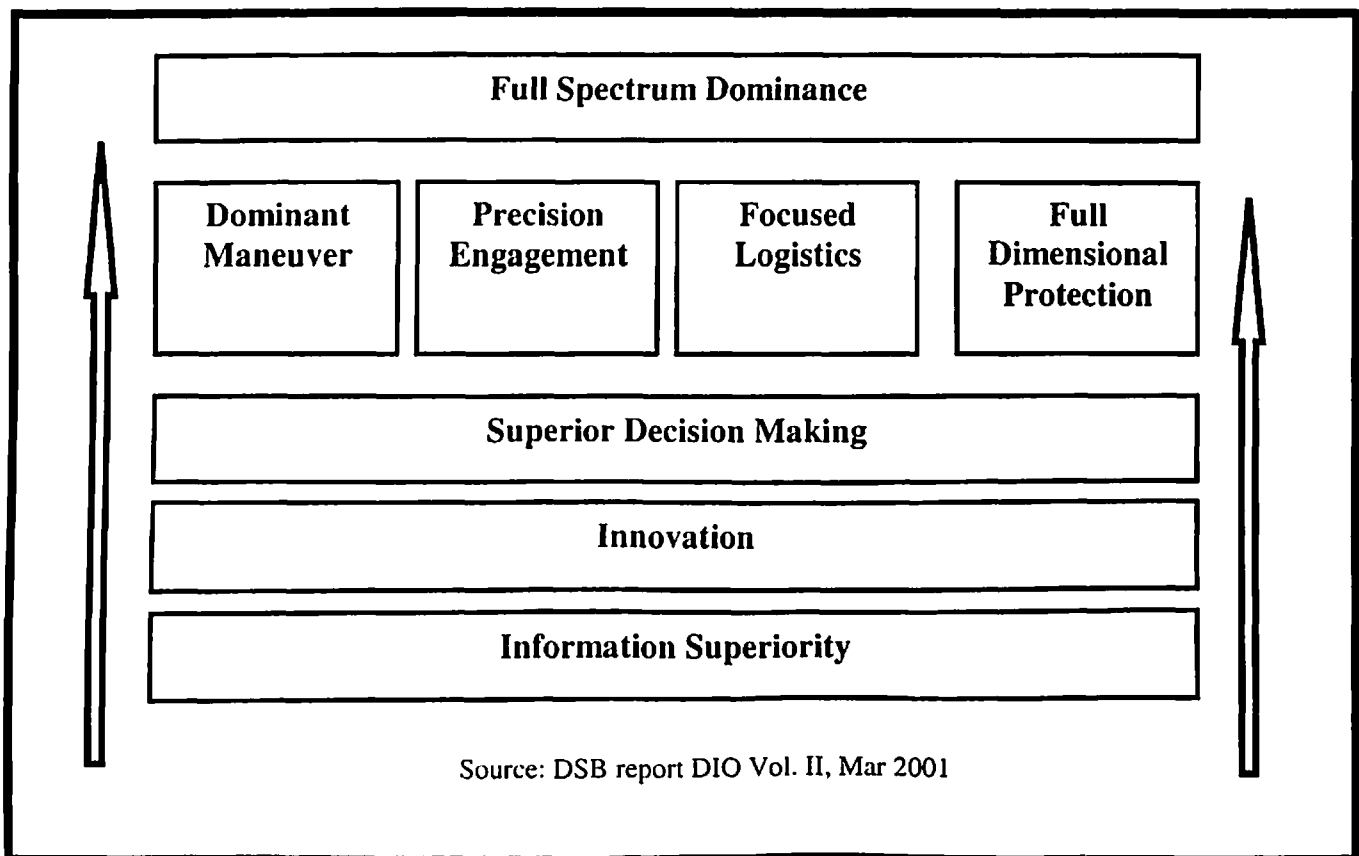


Figure 4.4: Joint Vision 2020 of US, DOD

The information superiority and innovation will form the foundation for superior decisions. The DSB has projected following areas for further research.

- Assurance about the Information Infrastructure that must provide information and decision superiority at the time and place of need, when an adversary is likely to establish the time and place of conflict.
- Assurance for the command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) capabilities provide critical information at precisely the right time to the command element needing it.
- Assurance of the availability and integrity of critical information in a coalition environment with a high data rate and a dynamic information exchange with allies of the time; given that such an environment is likely for most future conflicts.
- Impact of not having information superiority and decision superiority in a particular circumstance viz.
 - Objectives not met.
 - Loss of men resources.
 - Constrains in approach.
 - Inappropriate force structure.

4.4.6 Information-in-War and IW

The concept of future warfare formulated in the Joint Vision 2020 assumes that information supremacy is central to any possible developments in dominant maneuver, precision engagement, full-dimension protection and focused logistics. Information – how to get it, how to use it and how to protect it – is a common denominator for all serious attempts to address the future wars. Information supremacy is defined as the capability to collect, collate, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. This is a perfect traditional definition of information-in-war and C⁴I in a new package. Information supremacy, according to the Joint Vision 2020, will require both offensive and defensive information warfare.

The operational concepts of the Joint Vision 2020 will provide “full spectrum dominance”. This will allow dispersed forces to achieve massed effects across the spectrum of military actions from peacetime engagement through deterrence and conflict prevention to fight-and-win a war. The notion of full spectrum dominance assumes that massing of land, sea, air and space forces are the major, means to accomplish the mission. It also assumes that the military-relevant, strategic, operational or tactical effects might be produced by IW without combining the various joint forces in theatre. This is the key difference between thinking in terms of Information-in-war and thinking in terms of Information Warfare. However the implication for information-age armed forces if the potential for information warfare were to be something beyond a technology-based, more sophisticated version of command and control warfare is not yet clear. Therefore creative thinking about operational concepts for IW, however, requires that unusual questions be asked. What is the future battlespace? What are “forces” in future conflicts? What if the adversary does not employ forces? The goal of IW is to produce a “strategic” situation so advantageous that national security objectives can be achieved without “battle” or, if necessary, to have such a information-based military superiority that if “continuation by a battle” is necessary, victory can be assured. The primary strategic goal would be to shape the battlespace, not the battlefield, through air, space and information superiority. Information superiority does not merely permit joint force operations. Rather, information superiority achieved through properly used IW might achieve with precision the “effects” only possible previously by massing forces or even “mass effects” [5,15,101]

4.4.7 Information Age Warfare

Information-in-war is the concept of information superiority. The IW, however, is a new concept, in which presence at the theatre of operations is not necessary. IW involves the actions taken to achieve information superiority. It is an advancement of the concept of C²W. Thus information-age-warfare is a combination of the traditional concept of information-in-war with its modern advancements and IW, which is a new concept to wage a war using information-based principles. The components of information-age-warfare are shown in Figure 4.5. The detailed explanation and relevance of terms “Information Warfare”, “Cyber War” and “Net War” have been presented later in this chapter this chapter.

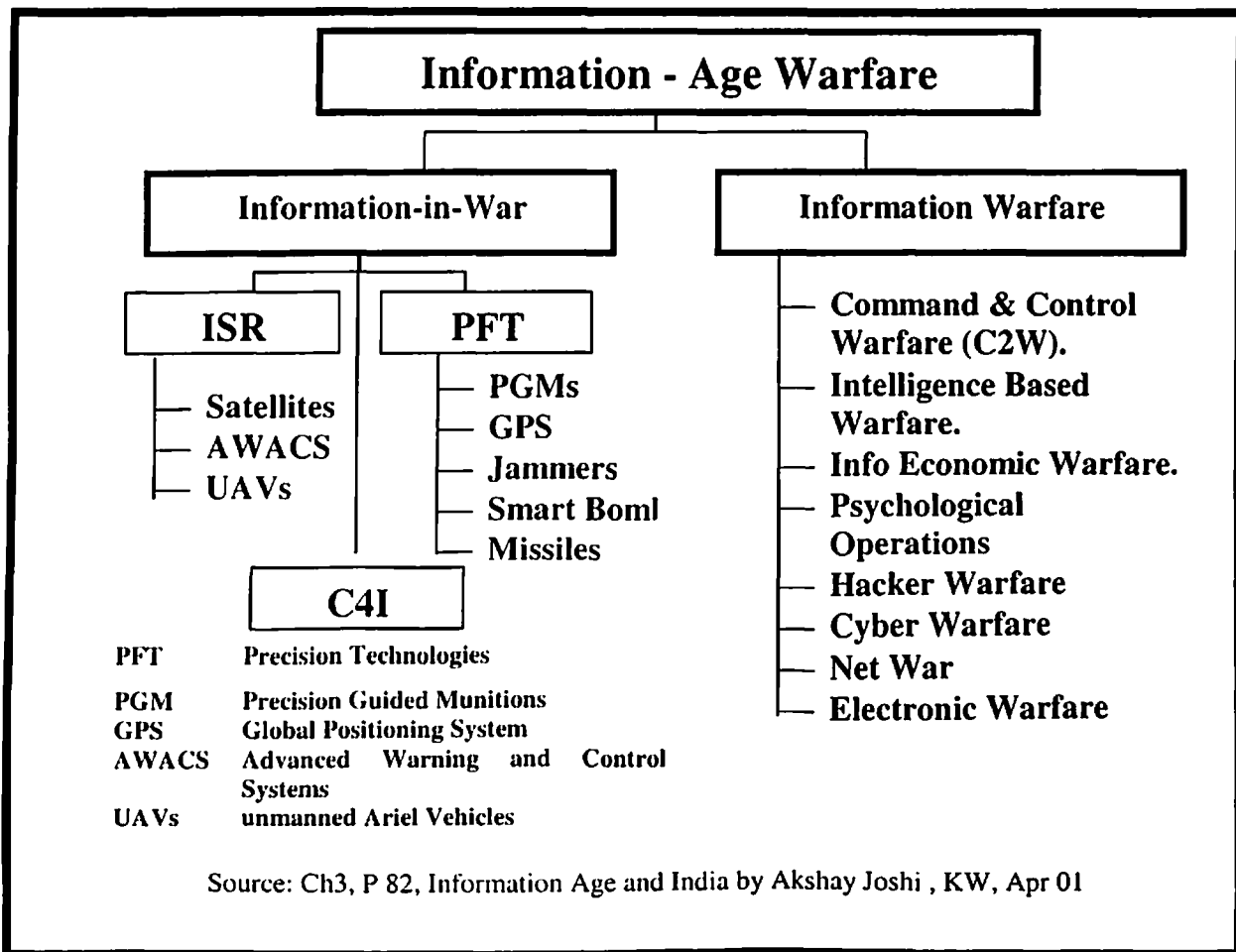


Figure 4.5 Components of Information Age Warfare

4.5 Impact of IT on Warfare

As described above, the RMA due to IBOs is giving rise to new tools and processes of waging a war. The implications of IBOs on RMA are illustrated in figure 4.6 and discussed in succeeding paragraphs.

4.5.1 Information Warfare (IW)

There are a number of definitions of information warfare. The US Joint Chiefs of Staff definition reads like this: “Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our own information and information systems”. Simply put, Information Warfare is defined as “any action taken to deny, exploit, corrupt or destroy the enemy’s information and it’s functions, while protecting ourselves against those actions and exploiting our own military information functions”. The definition of IW indicates that actions would have to be taken to achieve information superiority by affecting adversary’s information environment while defending ones own in any future conflict [129].

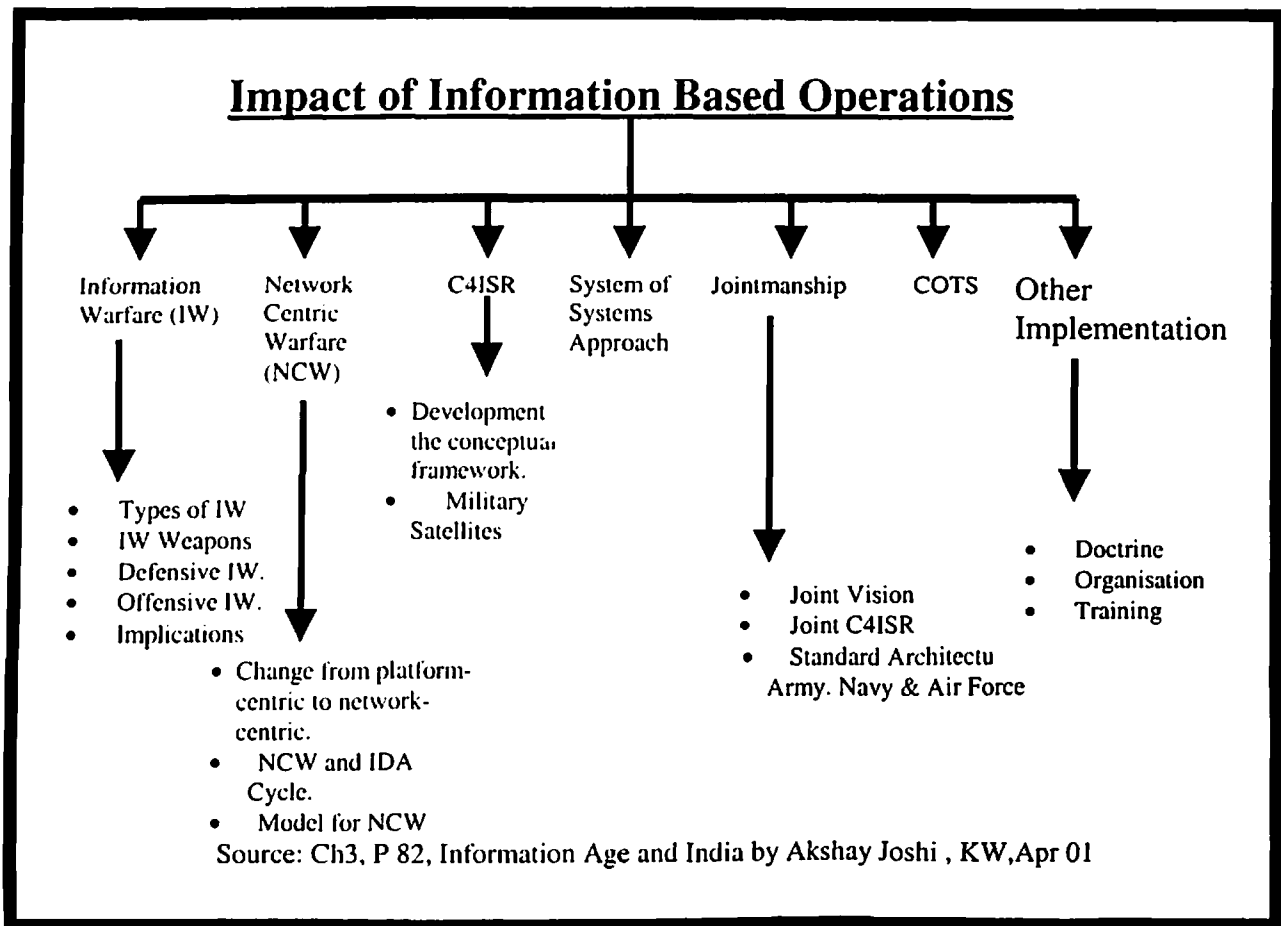


Figure 4.6 Impact of Information Based Operations

The Gulf War was the first time information was used both as a target and as a weapon. Command and control nodes, communication facilities, TV and radio stations were the first to be struck with missiles and bombs. In the initial stages itself the Iraqi units were cut off from their leadership. Information Warfare as a concept has fast gained acceptance after the Gulf War. The understanding of the concept though trails far behind. As of now IW does not exist as a separate technique of waging war, but there are several distinct forms of IW, each laying claim to a larger concept. The IW weapons either destroy information systems, or mutate the content. These include electromagnetic transients, chipping and microbes that eat, burn or disable the hardware; malicious software, that decimates data and pulverize operating systems, information swingers of varied types which engulf the adversary in a fog of misinformation and EMP devices which cause massive microelectronics burn outs.

A major implication of Information Warfare is that it empowers non-state actors. These non-state actors have a non-hierarchical command structure while state actors follow a hierarchical command system. This fact needs to be appreciated while formulating steps to counter cyber terrorism, hacking etc by non-state actors. Another major implication of IW, which falls under psychological warfare, is the media factor. The USA unabashedly used the CNN in the Gulf War to win public opinion against Iraq. What has further emerged post Gulf war is the importance of media management, news blackouts, propaganda and misinformation in the conduct of future wars.

The concept of IW is not a new one. Strategists such as Sun Tzu had spoken of the importance of knowing the enemy and one's self, centuries ago in order to defeat an opponent strategy before battle was joined physically. Today the methods for entering the enemy's decision making cycle and gaining insights into his strategy are powered by information technology. Information of superior quality is available in real time, thereby enhancing battlefield awareness. The methods of refining this information and filtering it to avoid information overload are getting more sophisticated. Simultaneously, defensive methods of denying the enemy accesses to our own systems and offensive methods of getting into enemy systems to disrupt their smooth flow of information are also being pursued.

The success of information warfare largely depends on the technological base of a nation, the extent of dependence on electronics for warfare and the extent of networking of its systems. Only the most advanced countries with superior technologies can fully prosecute IW. This also makes them more vulnerable to disruption by even modest technological powers. In the industrial age, the most powerful industrial nations attained supremacy. The same is true for the information age. Unless a nation becomes a pre-eminent information power, its military, ships, submarines and aircraft will be fighting wars with their hands tied. Chinese are studying the Gulf War and the subsequent US developments in this field before devising their infowar strategy.

4.5.2 Network-Centric-Warfare

Armed forces need to fulfill their tasks with decreased resources and decreased manpower. This necessitates working smarter and looking for force multipliers. Network-centric warfare enables us to manage this paradox. Network-centric computing is governed by Metcalfe's Law, which asserts that the 'power' of a network is proportional to the square of the number of nodes in the network. Sun Microsystems were the first to point out that it is not so much about the computer as it is about the computer in the networked condition. The International Business Machines (IBM) chairman Lou Gerstner announced that the IBM was moving to network-centric computing. The compelling business logic for this shift in strategy was the opportunity for the IBM to link its heterogeneous computing lines more effectively and provide increased value for its customers. This is the same value proposition we seek in warfare. Chief of Naval Operations, US Navy Admiral Jay Johnson has called it "a fundamental shift from what we call platform-centric-warfare to network-centric-warfare". Admiral Robert J. Nattar in his paper titled "The Future of the Fleet Information Warfare further justified this stand [8].

Emergence of new technologies has created the conditions for network-centric computing. There is an explosive growth of the Internet, intranets, extranets, transmission control protocol/ Internet protocol (TCP/IP), hypertext transfer protocol (HTTP), hypertext markup language (HTML), Web browsers, search engines, and Java Computing. These technologies, combined with high-volume, high-speed data access (and technologies for high-speed data networking have led to the emergence of network-centric computing. Information "content" now can be created, distributed, and easily

exploited across the extremely heterogeneous global environment. Networking for example in stock markets has led to a shift from a trader-centric system to a network-centric system. This has considerably reduced the time taken to complete transactions and increased customer awareness about prices of stocks and shares. This is very similar to a soldier having real-time battlefield awareness, which will enable him to complete his task quickly and efficiently. Network-centric retailing in departmental stores enables better inventory management. Similarly, a shift to network-centric operations will help the military improve its logistics management. It can be concluded that the military stands to benefit from network-centric operations in the same way as the corporate sector does.

The basic element of military activity on the battlefield is the Information-Decision-Action (IDA) cycle. This is also called the Observe-Orient-Decide-Act (OODA) loop. The information part of the cycle is carried out by sensors and associated systems responsible for generation of information. This activity is followed by decision and action in a cyclical fashion till the specific activity is completed. An activity might require more than one cycle for completion or a number of cycles before the action reaches finality. The probability of a single-cycle task is very low, considering that some cycle overrun would be needed for a reasonable degree of task achievement. The objective should be to complete the IDA cycle as economically as possible. Each part of the IDA cycle requires information technology in one form or another, whether for information processing, decision making or action. In fact, information technologies operate in all segments of the IDA cycle as catalysts since they hasten the individual segments, which in turn leads to dramatic compression of time. The structure or model for network-centric warfare is designed so as to compress the time taken to complete the IDA cycle.

The structure or logical model for network-centric warfare is shown in Fig. 4.7. It consists of a high-performance information grid (which corresponds to the information part of the IDA cycle) that provides a backplane for computing and communications. The information grid enables the operational architectures of sensor grids and engagement grids. Sensor grids (which corresponds to the decision part of the IDA cycle) rapidly generate high levels of battle-space awareness and synchronise awareness with military operations. Engagement grids (which correspond to the action part of the IDA cycle) exploit this awareness and translate it into increased combat power. The US Navy is rapidly shifting from platform-centric warfare to network-centric warfare and many key elements of the grids are in place. New classes of threats have required increased defensive combat power for joint forces. The combat power that has emerged—the cooperative engagement capability (CEC)—was enabled by a shift to network-centric operations. The CEC combines a high performance sensor grid with a high-performance engagement grid. The sensor grid rapidly generates engagement quality awareness, and the engagement grid translates this awareness into increased combat power. This power is manifested by high probability engagements against threats capable of defeating a platform-centric defense. The CEC sensor grid fuses data from multiple sensors to develop a composite track with engagement quality, creating a level of battlespace

awareness that surpasses whatever can be created with stand alone sensors. The whole is clearly greater than the parts.

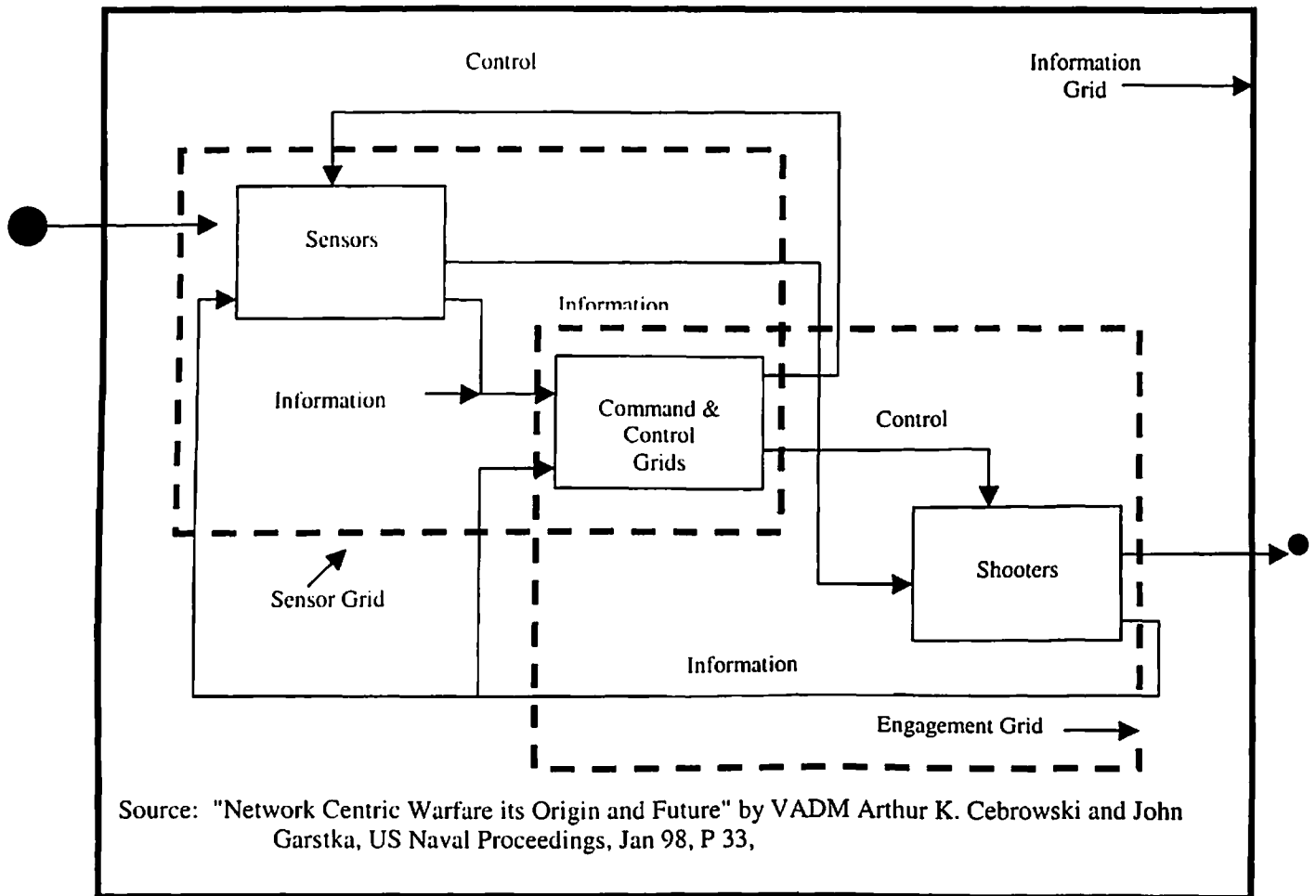


Figure 4.7: Logical Model of Network Centric Warfare

The pace of the future battle will be so swift that there will be no time to revert to the rear headquarters all the time for instructions and advice. A typical military hierarchical structure in such an environment will fail. It would be necessary to decentralise and delegate, while the people on the battlefield will have to be fully aware of rules of engagement and the political factors so that they can take quick decisions. Network-centric-warfare enables a shift from attrition-style warfare to a much faster and more effective war fighting style characterised by the new concepts of speed of command and self-synchronization. Strategically it allows an understanding of all elements of battlespace and battle time, operationally it provides a close linkage between the units and the operating environment and tactically it provides speed.

4.5.3 C⁴ ISR

The advent of new forms of communication and imaging technology, incorporated into systems such as 'smart' weaponry and digitised battlefield networks has led to the rethinking on warfare concepts. As technology has developed, new methods of collecting information have emerged. These new methods have improved the battlefield

awareness. C⁴ISR has enabled the integration of these new inputs. Technological advancements of weapons and vehicles of air power are being developed in a manner that will continue to shorten the time cycles for action along with the other segments of the IDA. A significant portion of technological progress being made in the military sphere deals with reconnaissance, surveillance and target acquisition (RSTA) systems. The employment of the RSTA technologies is moving warfare further towards greater utilisation of aerial assets for gathering of information, greater range of striking power through long-range offensive systems, and higher accuracy through availability of better target information. If viewed holistically, then the RSTA with communications give military forces the ability to locate targets with accuracy, carry out designation and cueing of weapon systems that significantly enhance combat power. Although airborne sensors have been used in the past, a more recent example was the Bekka Valley conflict of 1982 where the Israeli armed forces achieved a high degree of favorable asymmetry in the opening stages itself. On a larger scale, the Gulf War of 1991 saw the use of the RSTA and communication technologies that multiplied the combat power of the allies while degrading that of the Iraqis. The use of these technologies in this war led to far greater compression of time than before and signs of a new RMA emerged. The use of the RSTA systems, Airborne Warning and Control Systems (AWACS), the Unmanned Aerial Vehicles (UAVs) and their integration into a C⁴ISR system has enabled the use of sophisticated weapons like 'smart bombs' and Precision Guided Munitions (PGMs) which are extremely accurate and reduce civilian casualties. C⁴ISR has also led to the expansion of space and the compression of time on the battlefield.

The C⁴ISR provides situational awareness (SA) for integration and coordination of joint element manoeuvres and sensor to shooter connectivity for weapons employment. It is the essential capability for binding the nation's armed services, defence and intelligence agencies and other government and private organisations into a viable, coherent force. The resultant information superiority fundamentally changes the way operations are conducted. Joint C⁴ISR enables ability to mass effects without massing forces; protects against asymmetric threats; and, provides joint force flexibility, interoperability and efficiency. Throughout history one of the important elements of military tactics has been Command and Control (C²). The concept developed into Command, Control Communication and Intelligence (C³I), Command, Control, Communication, Computers, and Intelligence (C⁴I), Command, Control, Communication, Computers, Intelligence and Interoperability (C⁴I²) and finally to C⁴ISR. The concept has developed with the development of technology and various nations are at different stages depending on the integration of technology into their Command and Control structure. India like many developing countries is implementing C³I at the tactical level and has drawn out the plans for a National C⁴ISR system [32,109].

4.5.4 System of Systems Approach

In the proceeding section we have examined how the RMA has introduced new concepts like Information Warfare, sophisticated weapons like 'smart' bombs and precision-guided munitions, a change from platform-centric warfare to network-centric-warfare thereby reducing the time taken to complete the IDA cycle and C⁴ISR which has integrated various inputs thereby altering the time-space paradigm on the battlefield. In

order to further streamline the complex business of warfare Admiral William Owens, former Vice Chairman of the Joint Chiefs of Staff of the US introduced the concept of "System of Systems". This approach is heavily draped in high technology weapon and surveillance systems of the battlefield and focuses on the integration of three sets of technologies that relate to precision strikes, communications, and sensors on the battlefield. The system of systems approach is pegged on the application of information technologies to warfare with a view to integrate and network existing and emerging technologies that can look, shoot, and communicate. System of systems is integrating the technical advances of ISR, C⁴I and precision force technology into a command and control platform at the national level. In figure 3.7, the sensor grid, command and control grid and shooters grid are independent systems by themselves at one level. However they together form a composite combat system when integrated thereby giving the notion of a "System of Systems".

4.5.5 Jointmanship

The US has changed to radically divergent techniques of warfighting in the information age. It is called 'joint warfighting', is an umbrella phrase under which a multitude of changes are taking place. Under the Goldwater-Nicholas Act of 1986, the US military has not only been busy converting the task of joint warfighting into an art form, but it is continuing to do more with less. This means that the US military is continuing to come up with different organisational and functional ways to serve as a credible warfighting force. In fact, the Joint Vision 2020 has emerged as an abbreviated discussion of the utmost significance and can address information based operations across the entire warfare spectrum as shown in the figure 4.4 [15].

All the implications of the RMA dictated by IBOs imply the need for jointmanship amongst the three wings of the armed forces. All future operations may not be joint, but having a standard architecture for all three services enables merging of architectures if and when the need arises. Merging of architectures is important so that information from any of the sources can be used to deliver maximum firepower on the enemy.

4.5.6 IW Doctrine, Training and Organisation

The Armed Forces have to address doctrine, organisation of forces and training as core issues. They have to work with other government agencies to develop architectures, which can be merged later. Standardisation of hardware and software, identification of reliable sources of supply with backups, and the need to commence careful tests on all electronic equipment for hidden computer virus, malicious software, etc. need to be included in a nation's security doctrine.

An effective organisation of the armed forces is very important in order to derive the maximum benefit of the IBOs. In the information age, the dominant organisational model is the network. Traditional military hierarchies and the network forms have very different strengths and vulnerabilities. We must consider ways to respond and adapt to this organisational challenge, which can be effectively created through jointmanship. Just as computers have flattened the organisational charts of corporations, the Armed Forces will have to restructure ranks with fewer layers of staff officers needed to process

orders between senior staff and the men on the ground. The distinction between civilian and soldier will blur with more private contractors needed to operate complex equipment on the battlefield. There will, no doubt, be bureaucratic and even cultural opposition within the military to this new form of fighting. Chinese defence analyst Xu Chuangie writes in *Military Revolution Gives Impetus to Evolution in Command*, "The revolution in information technology has increasingly changed with each passing day the battleground structure, operational modes, and concepts of time and space while dealing blows to the traditional 'centralised' and 'tier-by-tier' command structure". He recommends that a traditional vertical and tiered command structure be converted into a networked command structure and the centralised command system be converted into a dispersed type command [55]. The US Review talks about reduction in personnel, restructuring the reserve component of the army, reducing size of the fleet of the navy etc. It will also accelerate its Force XXI modernisation plan, which will revolutionise combat capability by enhancing battlefield awareness through modern information technology [77].

Most current generation cyber warriors are self-taught. In June 1995, the National Defence University in Washington D.C. graduated its first class of 16 infowar officers, specially trained in everything from defending against computer attacks to using virtual reality in planning battle maneuvers. Armed Forces need to conduct customised courses covering all aspects of the Revolution in Military Affairs. Converting Information Operations (IO) into a separate specialisation, distinct from the "Signals and Communication" branches of the Army, Navy and the Air Force, is long overdue. Training in Information Operations needs to be introduced at the basic level.

4.5.7 Role of Commercial-off-the-Shelf (COTS) Technology

The four objectives of the RMA spelt out by the US and other western nations were, the focused logistics, dominant battlespace awareness, good command and control and precision weaponry. This was made possible because of the availability of COTS from the civilian IT industry. Information technology is a dual use technology whereby, it can be used for both military and civil purposes.

Former US Chief of Staff General Colin Powell in an article in the July 1992 edition of the *Byte* magazine had underlined the fact that "increasingly military requirements are being met by off-the-shelf hardware and software". This is a remarkable paradigm shift. Traditionally, militaries sustained whole industries and civilian/ commercial spin-offs as a consequence of that. In the cyber-age, where IT industry works on smart ideas and massive volumes that create the necessary economies of scale, the militaries are no longer the prime consumers. They have to look at the shop shelves, pick and choose and have the ability to employ essentially civilian technologies for military use. From militaries driving the market to market-driven militaries – this is the impact of the RMA]. The Quadrennial Defence Review by the US Department of Defense (DoD) emphasises the need to take advantage of the Revolution in Business Affairs [77]. However when viewed in the context of need for EMP hardened systems, the COTS route may not work.

4.6 Analysis of the - Cyber Warfare, Netwar and Information Warfare Paradigms

The terms cyber Warfare, Netwar and Information Warfare are being used in the literature interchangeably. Their precise definitions in the context of military operations and terrorism etc. are amplified in the succeeding paragraphs [17,18,111].

4.6.1 What is Cyber war?

Cyber war refers to the preparation and conduct of military operations according to information related principles to disrupt or destroy information and communications systems on which an adversary relies in order to know itself, who it is, what it can do, when, why it is fighting, which threats to counter first and so forth. This amounts to knowing everything about an adversary while keeping the adversary from knowing much about oneself. It means turning the "balance of information and knowledge" in one's favor, using knowledge so that less capital and labor may have to be expended.

Cyber war involves use of large-scale diverse technologies used for C⁴ISR. It also involves electronically blinding, jamming, deceiving, overloading and intruding into an adversary's C⁴ISR system.

At a minimum, it represents an extension of the traditional importance of obtaining information in war; having superior C⁴ISR and trying to locate, read, surprise and deceive the enemy before he does the same to you. It, therefore, emerges that information related factors are far more important than ever before due to new technologies but it does not indicate a break with traditional factors governing the war efforts.

Cyber war is as much about "organization" as "technology", implies creation of new man-machine interfaces that can amplify man's capabilities but not a separation of man from the machine. In some situations, combat may be waged fast and from afar, but in many other situations, it may be slow and close in. Therefore, new combinations of far and close and fast and slow may be the norm for the future in cyber war than one extreme or the other.

In the cyber war, battlefields would be fundamentally altered by the information glut at both strategic and tactical levels. The increasing breadth and depth of this battlefield and the ever improving accuracy and destructiveness of conventional munitions would further heighten the importance of C⁴ISR to the point where dominance in this aspect alone may not yield consistent war winning advantages. Cyber war is a much broader idea than attacking an enemy's systems while improving and defending one's own. The advantages would be visible only when we are able to turn knowledge into capability.

Many military planners believe cyber war would require advanced technology, while others perceive it does not necessarily require the presence of advanced technology. The

organizational and psychological dimensions would be as important as the technical content. Cyber war may actually be waged with low technology under some circumstances.

Cyber war also has civil dimensions. In a densely computerized and networked environment in the government and private sector, the information exchange model is similar to that of a military C⁴ISR network. Therefore, vulnerability assessment and counter measures for protection of civil computers, data bases and networks need to be evolved on lines similar to those applicable for military systems but possibly at a lesser scale of severity due to in-built redundancies and inherent flexibility. Time sensitivity of such networks may not be as critical as applicable for military systems. However civil agencies have rarely faced any threat of disability, damage or destruction from unfriendly sources and may tend to be lax. This aspect needs assessment of the impact of cyber war on civil networks carefully and is a potential area of research.

Cyberwar is the application of the electronic tools and techniques to military operations in the traditional sense. Called as command and control warfare or C2W by the armed forces, cyberwar uses the new opportunities for intermitted communications to amplify the battlefield application of the more traditional war-fighting techniques of operations security, electronic warfare, psychological operations, deception, and physical destruction of enemy communications to achieve information dominance in the battle

4.6.2 What is Net war - A Potential Civil Domain Activity?

Net war refers to information related conflict at a large scale between nations or societies, whereby the adversaries try to disrupt, damage, or modify what a target population knows or think it knows about itself and the environment around it. The focus is on public or elite opinion, or both.

It involves public diplomacy measures, propaganda, psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across communication.

Net war covers a wide spectrum of conflicts, which can span economic, political, and social as well as military forms of war. In contrast to economic wars that target the production and distribution of goods, and political wars that aim at the leadership and institutions of a government, net war is distinguished by its targeting of information and communications.

Like other forms, net wars are largely non-military, but they could have dimensions that overlap into military war. For example, an economic war may involve trade restrictions, dumping of goods, illicit penetration and subversion of business and markets in a target country and the theft of technology. None of these need involvement of the Armed Forces. On the other hand, an economic war may also include an armed blockade or strategic bombing of economic assets, thereby a military war. On similar lines, a net

war that leads to targeting an enemy's military capabilities, at least in part, turns into what we mean by cyber war.

Net war may occur between the governments of rival nations states, it may arise between governments and non-state agencies, waged by governments against illicit groups and organizations involved in terrorism, proliferation of weapons of mass destruction and drug smuggling.

On the contrary, advocacy groups and movements involving for example, environmental, human rights, or religious issues, may wage it against the policies of specific governments. This is what Pakistan has been attempting against India whereby its Consulate in USA had hired public relations firm to launch a propaganda war through TV and media against India. The terrorist activities in Punjab and Jammu & Kashmir have been underway on similar lines. USA along with its allies in Western Europe was successful in waging low intensity net war on Soviet Union prior to its disintegration. The events of post 9th Sep 2001 to mobilize global opinion against terrorism are a case of net war. In some cases, the non-state agencies may or may not be associated with nations, and in some cases they may be organized into vast transnational networks and coalitions.

Another kind of net war may occur between rival non-state agencies with governments maneuvering on the sidelines to prevent collateral damage to national interests and to support one side or another. This is the most speculative kind of net war, but the elements for it have already appeared, especially among advocacy movements around the world. Some movements are increasingly organizing into cross-border networks and coalitions, identifying more with the development of civil society (even global civil society) than with nation-states, and using advanced information and communications technologies to strengthen their activities. This is foreseen to be the next major frontier for ideological conflict and net war may be a prime characteristic.

Most net wars would be non-violent, except some low-intensity conflict scenarios. As brought out above, some net wars may involve military issues viz., nuclear proliferation, drug smuggling and anti-terrorism because of the potential threats they pose to international law and order and national security interests. Societal trends e.g., the redefinition of security concepts, the new roles of advocacy groups, the blurring of traditional boundaries between what is military and what is non-military, between what is public and what is private, and between what pertains to the state and what pertains to society may engage the interests of at least some military planners in some net war related activities. Net wars would not be real wars as traditionally defined. They would be developed into an instrument for trying to prevent a real war. Deterrence may become as much a function of cyber posture.

4.6.3 What is Information Warfare?

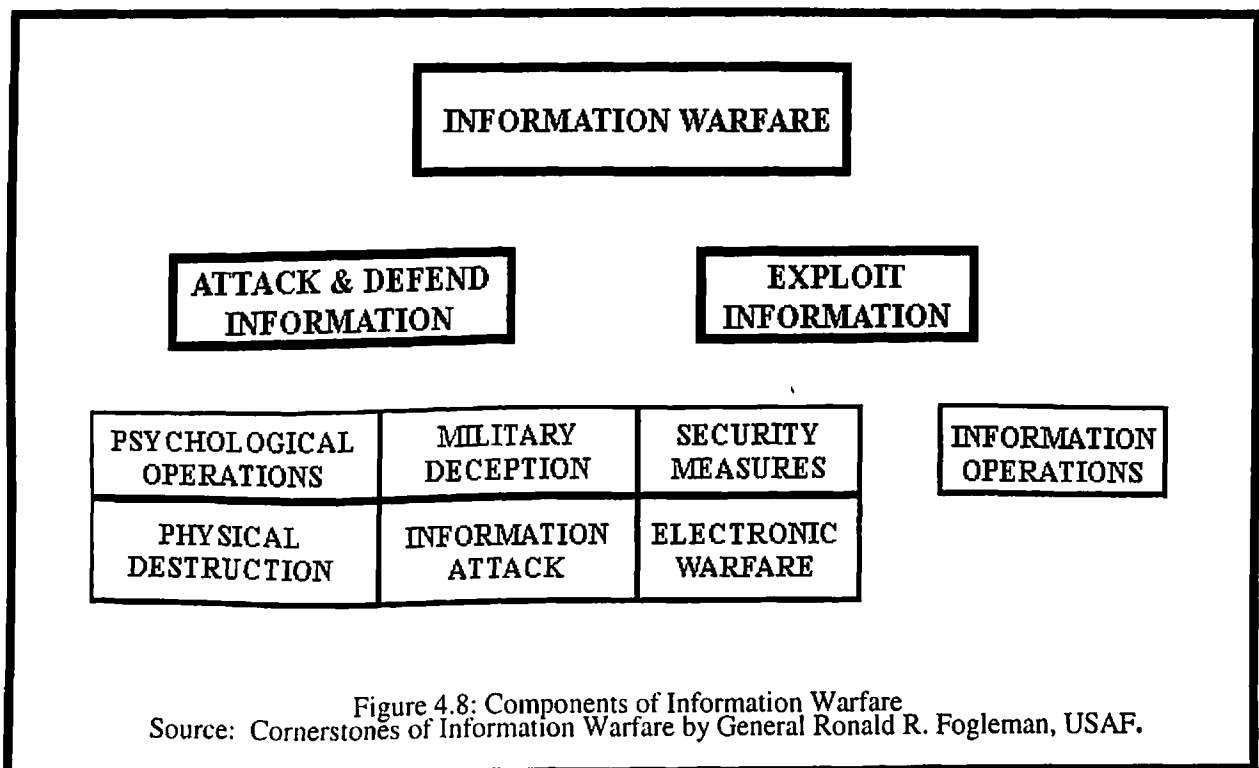
In military terms, Information Warfare is defined as the action taken to achieve information superiority by affecting adversary information, information based processes and information systems while defending one's own information, information based

processes and information systems. These concepts stress the fact that future conflicts will be fought by "networks" and whoever masters the network will have the upper hand. It is a force multiplier and the single theme is to "own the net".

Information Warfare covers activities such as psychological operations, electronic warfare, military deception, physical destruction, information attack and security measures. This spectrum takes into account the physical, economic, political, military and information infrastructures. The spectrum can be viewed as "content", "technology", "organization" and "infrastructure". Considering the Information Warfare spectrum as a "content", it is seen to be made up of Data, Information, Knowledge and Feedback.

Data is the observation and Information is the orientation of our present position in this domain. Knowledge is the decision on what to do about this particular information. Feedback is the process of acting upon this information and the decision to act. The Observation, Orientation, Decision and Acting together constitute what is called OODA loop.

DOD USA has expanded its doctrine of Command and Control Warfare into the broader concept of Information Warfare (IW). According to a provisional DOD definition, IW consists of "actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our own information and information systems. This formulation is intended to encompass military and non-military actions as well as defensive and offensive aspects. It also covers all levels of war from the tactical to strategic, and applies to peacetime and wartime conditions. The composition of Information Warfare is presented in the figure 4.8.



Offensive IW: Employed offensively, IW emphasizes the manipulation of electronic information systems to influence an adversary's perceptions and behavior. This might, for example, involve disabling military and civilian telecommunication systems through computer viruses or electromagnetic pulse devices. Infiltration is, however, the "maneuver of choice" since an enemy, unaware that his information sources have been compromised, will continue to trust them, creating opportunities for deception. Offensive IW also emphasizes the use of direct broadcast satellites, the commercial media, and "visual stimulus and illusion" technologies such as holography to conduct propaganda and subversion.

Defensive IW: Defensively, IW requires an ability to detect and thwart attempts to tamper with one's own sources of information. In the military sphere, this entails assuring the integrity of command and control, communications, and intelligence systems. Critical elements of the civilian infrastructure such as power grids, financial networks, and telecommunications systems must also be protected. In addition, defensive IW is an ability to counter enemy propaganda and misinformation. According to the Tofflers, this can best be accomplished in an Information Age context by "precision-targeting" audience segments, disguising propaganda as news and entertainment, and employing computer-generated special effects.

IW has begun to touch many areas of military systems. The figure 4.9 indicates various IW aspects being addresses in military aircraft, electronics systems, electronic systems integration, data systems etc.. The IW expertise is being created across company divisions of equipment manufactures to enhance IW Defence and IW - Offensive roles of military systems [98].

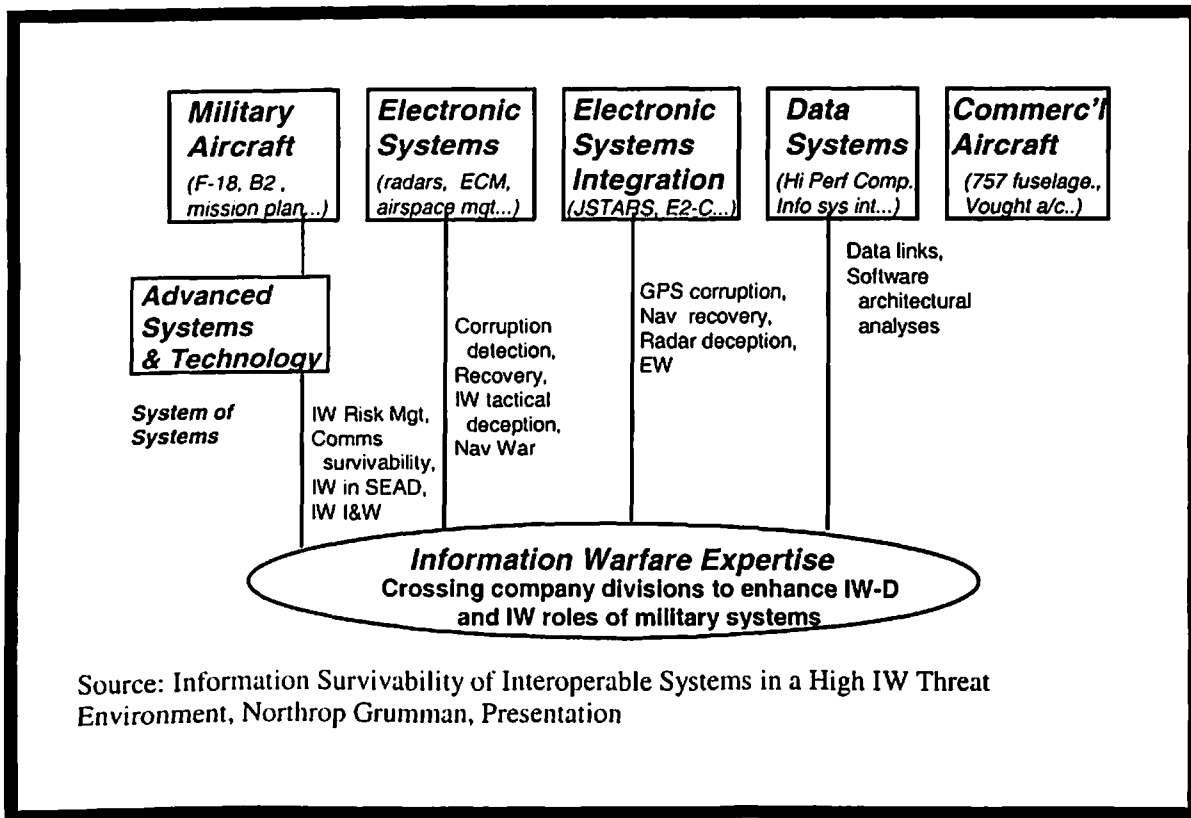


Figure 4.9 Component in Northrop Grumman Built Military systems

According to writers like Donald Ryan, IW is based on the assumption that information technologies have developed to the point where they can now be employed as a weapon in their own right rather than as a "handmaiden" of armed combat. It thus becomes possible to envision wars being "won" or "lost" without, a shot being fired. In contrast to Command and Control Warfare, which aims at victory on the battlefield, IW seeks to avoid the need to resort to lethal force by putting "enemies in positions where their information resources are useless or, worse, unreliable." In this respect, IW aspires to realizing Sun Tzu's famous dictum that "to subdue the enemy without fighting is the acme of skill."

4.7 Role of IT in IW

Historically Armed Forces have kept installing new technology to make specific operations more effective. Techniques crucial to cyber war are aimed at improving the cost effectiveness of military operations irrespective of the overall strategy. These are illustrated below:

- Improved surveillance and intelligence gathering capabilities that can help identify timely opportunities for surprise as compared to a traditional attrition warfare strategy.

- New capabilities based on IT for informing the member of a unit in real time about where their comrades are located and what each is doing, as in the case of Inter-Vehicular Information Systems (IVIS) can improve ability to concentrate forces as a unit and maintain that concentration throughout an operation.
- Availability of a Global Information Transport mechanism like the Internet and availability of terminal equipment i.e. a large spectrum of information appliances, IW would spread to very low levels. The technical availability and performance of such a mechanism would be increasing while the cost would reduce, thereby making it much more attractive.
- In the past, military doctrine, organization and strategy have continually undergone changes, dictated by technological breakthroughs. New weapons, propulsion, communication and transportation technologies have provided a basis for advantageous shifts in doctrine, organization and strategy that have enabled innovators to avoid exhausting battles of attrition and instead pursue a "decisive" warfare. Today, a variety of new technologies are again emerging and further innovations are on the way viz., non-nuclear high explosives, precision guided munitions, stealth designs for aircraft, tanks and ships, Radio Electronic Combat (REC) systems, new electronics for intelligence gathering, inference and deception, functions and futuristic designs for space based weapons and robotics, virtual reality systems, simulation, Non-Lethal & Less-Lethal Technologies etc.
- The ability of nations to anticipate and wage war will be shaped in part by how these technologies are assimilated and adopted. Yet, technology permeates war but does not govern it. It is not technology, but the organization and management of technology that is important. As perceived by Russell Weigly, "the technology of war does not consist only of instruments intended primarily for the waging of war. A society's ability to wage war depends on every facet of its methods of organizing its technology". Also as Van Creveld put it, "Behind military hardware there is hardware in general, and behind that there is technology as a certain kind of know-how, as a way of looking at the world and coping with its problems". In the present view, the technological shift that matches this broad view is the Information Revolution. This will bring the next major shift in the nature of conflict and warfare.
- Advanced information and communications systems can improve the efficiency. But improved efficiency is not the only or even the best possible effect. Information Technology has a transforming effect, for it disrupts old ways of thinking and operating, provides capabilities to do things differently, and suggests how some things may be done better if done differently. The consequences of IT usage are viewed as "Efficiency Effects" and "Social System Effects". The history of previous technologies demonstrates that early in the life of a new technology, people are likely to lay emphasis on the efficiency effects and underestimate or overlook potential social system effects. For example, advances in networking technologies now make it possible to think of people, as well as databases and processors, as resources on a network. Beyond efficiency, at behavioral and organizational changes, we will see IT can change the way people spend their time and what, who they know, and care about. The full range of payoffs and the dilemmas will come from how the technologies affect the way people think and work together. The PSYOPS is an example of this phenomenon.

- The information revolution, in both its technological and non-technological aspects, challenges the design of many institutions. It disrupts and erodes the hierarchies with which institutions are normally designed. It diffuses and re-distributes power, crosses borders, and re-draws the boundaries of office and responsibilities, expands the spatial and temporal horizons that actors should take into account, compels closed system to open up. This may make life difficult, especially for large, bureaucratic, aging institutions, the institutional form is not becoming obsolete. Institutions of all types remain essential to the organization of society. Institutions will adapt their structure and processes to the information age. Many will evolve from traditional hierarchical forms to new, flat, flexible, network like models of organization and Armed Forces would be one of them to face this eventuality.
- The information revolution is strengthening the importance of all forms of networks, such as social networks and communication networks. The network form is different from the institutional form, particularly when it applies to military. While institutions, large ones, in particular, are traditionally built around hierarchies and aim to act on their own, multi-organizational networks often consist of small organizations or part of institutions that have linked together to act jointly. The information revolution favors the growth of such networks by making it possible for diverse and dispersed actors to communicate, consult, co-ordinate and operate together across greater distances and on the basis of more and better information than ever before, the factors extremely crucial in warfare.

4.8 IW Survivability

IW survivability aspects are increasingly being embedded in Warfighting Systems (legacy & new) as well as Distributed Information Systems in civil and military services. The IW survival strategy proposed by Dr. Anita D'Amico, Manager IW, Northrop Grumman suggests improving survivability by extending focus through defence in depth, which adds layers of defence/ response at each stage. Separate approaches for war fighting legacy and new systems and distributed information systems across the NII has been suggested. In specific the information survivability in an IW environment must address the following [98,160]:-

- **Threats** - Understand potential attack sources & methods
- **Vulnerability** - Reduce system weaknesses that open us up to attack
- **Impact** - Given an attack, reduce its impact on the mission or damage to the system
- **Recovery** - Reconstitute, reconfigure or reroute after attack
- **Response** - Answer an attack with defensive or offensive countermeasures that reduce future threats & vulnerabilities.

The summary of IW – Survivability steps for various categories of IT systems in military and civil applications is illustrated in figure 3.10 [98]

S. No.	Survivability Approach	Vulnerabilities	Impact	Recovery & response
1.	Current Focus	how well we keep them out & reduce system weaknesses	How much effect they have	How we return to effective functioning response (how we respond to the attacker)
2	By defence in Depth	Keep More Attacks Out: <ul style="list-style-type: none"> • Earlier & more accurate prediction of attacks • Fewer access points • Fewer weaknesses 	Reduce Mission Impact & Damage: <ul style="list-style-type: none"> • Make defensive response earlier • Work-arounds • Resilient ConOps 	Continue Operations: <ul style="list-style-type: none"> • Real time information recovery & system reconfiguration • Deceive BDA
3	Military systems	<ul style="list-style-type: none"> • Deny enemy info • Mitigate risks of IW implanted during pre-IOC and operational support phases • Overload enemy information systems 	<ul style="list-style-type: none"> • Improve overall situational awareness • Provide automated information reconfiguration • Deceive enemy BDA 	<ul style="list-style-type: none"> • Recover compromised info in real time • Identify potential targets for offensive response
4	Disturbed System	<ul style="list-style-type: none"> • Predict the “who, when & how” of attacks • Expand reporting sites • Institute formal IW risk management processes 	<ul style="list-style-type: none"> • Institute IW countermeasures • Contain attack • Establish self-reconfiguring systems 	<ul style="list-style-type: none"> • Real time recovery and system reconstitution • Deceive BDA
Source : Information Survivability of Interoperable Military Systems in a High IW Treat Environment, North Grumman				

Figure 4.10 IW Survivability Summary

4.9 IW Risk Management Strategies

The literature survey reveals that considerable work is underway to examine and assess IW threat and vulnerabilities, map them as potential risks and evolve formal methods to minimize or mitigate these risks. The system level vulnerabilities are tested by concentrating on external IW attacks, using methods that IW attackers would use, examining mission impact of IW attacks and conducting attacks on systems in test environment and analyze results, using proactive methodology and tools. The approach comprises of following steps [98].

- Catalog results of all risk assessments of weapons/ C⁴ISR systems and their support systems, to identify common methods and findings.
- Determine mission impact of identified vulnerabilities.
- Based on the above, develop a standardized risk assessment methodology to test for IW vulnerabilities with greatest mission impact
- Evaluate and refine the standard risk assessment methodology by conducting passive and proactive risk assessments on weapons/C⁴ISR systems, and their ground support systems.
- Develop a database with hypertext links to document the IW risk assessment standard, applicable directives, and the results of all other applicable risk assessments.
- Develop a repository of potential vulnerabilities and associated risk mitigators and make results available on need-to-know basis.

The examples of IW Risk Management Programs (IW-RMP) of Northrop Grumman for weapon systems and distributed Information systems are shown in figures 4.11 and 4.12

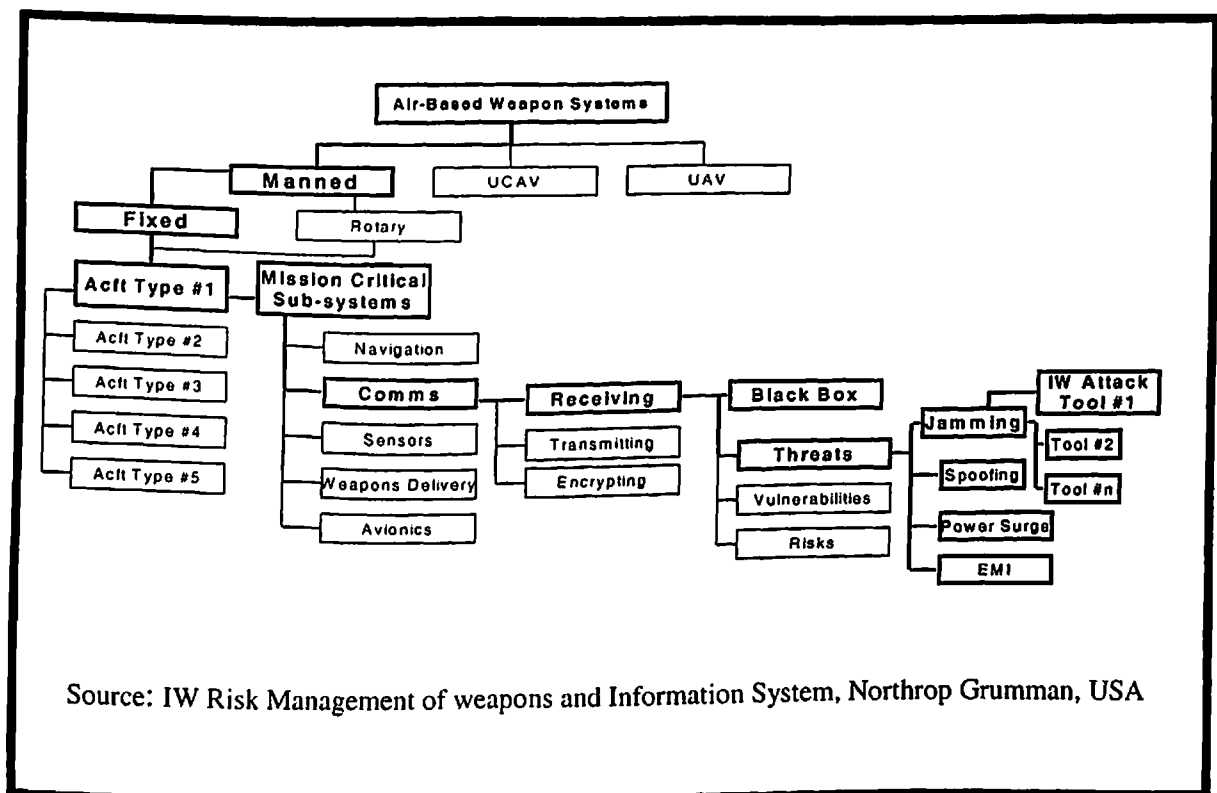


Figure 4.11: IW RMP for Weapons Systems

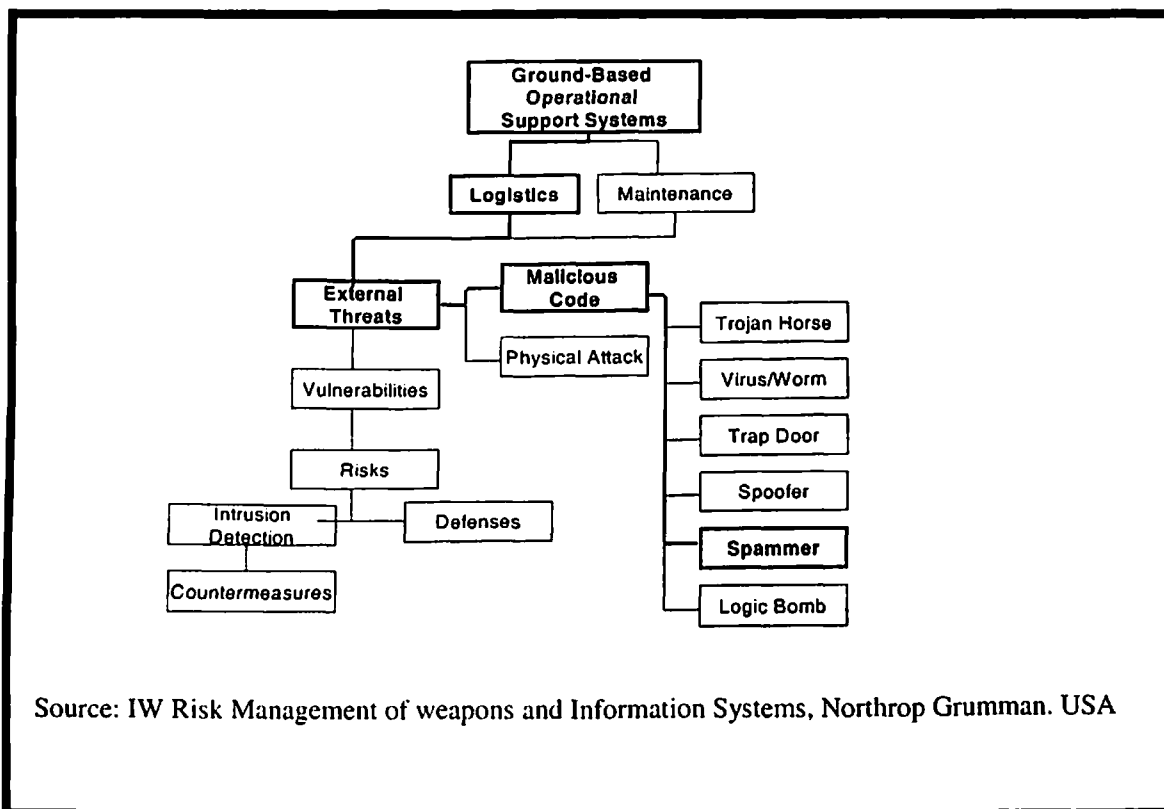


Figure 4.12: IW RMP for Distributed Information Systems

4.10 Conclusion

We have seen that the unprecedented and rapid penetration of computers and communications has connected infrastructures to one another in a complex network of interdependence. This inter linkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of natural or manmade threats poses serious risks. Therefore the safety, security and all time availability of the critical national infrastructure such as energy, banking, finance, transport, defence, telecommunications, etc., need to be viewed in a new context in the information age.

It has also emerged that the Armed Forces, terrorists groups, antisocial elements, business rivals, smuggling cartels, ideological or political adversaries have recognized these unprecedented threats and vulnerabilities and have sought to exploit them for their own respective gains. The risks to these IT intensive infrastructures have emerged in the shape of Non-lethal weapons or “Disabling Systems”, and, the art and science of using them has been termed interchangeably as ‘Information Warfare’,

‘Netwar’ or ‘Cyber war’: These forms of warfare are being continuously refined, restructured and integrated into existing tactical and strategic warfare capabilities by the Armed Forces and other security agencies of the advanced nations. The Information Age Warfare is thus being founded on Information and Information Warfare. The Information superiority is the lynchpin of emerging warfare paradigm. The critical

infrastructures can be disabled, denied, damaged, or destroyed by attacks using informational weapons, which can range from hacking, phreaking, malicious code and EMP/ RF energy weapons.

The report of the Defence Science Board of USA acknowledges the validity of this type of scenario as evident from the following statement. " Unlike an attacker in conventional war, an attacker using the tools of information warfare can strike at critical civil functions and processes such as telecommunications, electric power, banking, or transportation and other centers of gravity or even at the stability of the social structure, without first engaging the military. Such a strategic information warfare attack can occur without forewarning or escalation of other events. In addition, attacks on the civil infrastructure could impede the actions of the military as much as a direct attack on the military's force generation processes or command and control".

Military organizations are formulating measures to conduct offensive information warfare operations. However, while the military clearly must defend civilian physical infrastructure against military attack, it is not clear that the defence of the civilian information infrastructure is a task best suited to the military alone or even that the military alone could mount an effective defence of the civilian information infrastructure. These aspects need to be researched further.

We recognize that the critical infrastructures are central to our survival and sustenance in social, economic, political and military terms. Therefore we need to lay the foundations for their future safety and security in the information age. However an effective response to information warfare threats can only be devised by bringing together Armed Forces and civilian agencies and the industry. Although the Armed Forces seem now to be aware of the threats to military systems and to civilian systems upon which the military depends, there is a need to heighten awareness of the threats to civilian systems and to involve the operators of these systems in formulating appropriate responses. Furthermore, in view of the global nature on information technology, effective action will have to be taken at national scale and level to make every effort to assess the nature of the information warfare threat and consider how best to develop effective countermeasures. This work has been presented in Chapter 5.

CHAPTER 5

INFORMATION WARFARE THREAT ASSESSMENT

5.1 Introduction

In chapter 3 we have concluded that Information-Age-Warfare has been evolved over the years around two constituents viz. Information-in-War and Information Warfare. These in turn have organically evolved around C4I, ISR, C2W, PSYOPS, Intelligence Based Warfare, EW, Hacker War, Info Economic War, Cyber War and Net war. We have also concluded that information is a common thread that binds all the national infrastructures and therefore makes them prone to warfare using information-based principles. It also emerged that Cyber Space is a virtual space formed by connection of any two or more computing devices, people or information appliances through wired or wireless media and defies border based boundary definition. The Cyber Space is therefore prone to Information Warfare attacks from within or across the transnational borders at any time, anywhere and by any body during peace and war.

This chapter examines the impact of IT penetration and the consequent cyber space environment, sources and diversities of cyber space intrusions, sophistication of IW attack tools, emergence of information warfare weapons, targets of attack, threats and vulnerabilities of the NII. It signifies that IW threat is indeed serious and some of the IW weapons under development in the West have deterrence potential hitherto possible only from nuclear weapons. It also highlights that for protection of NII, India needs to develop IW defensive and offensive capability. The incremental steps in short, medium and long term to develop this capability have been suggested. It brings out that EMP and RF energy weapons are the most threatening information-age arsenal and identifies them as the focus of research and development by India under a comprehensive IW program. It also identifies EMP and RF energy weapons as area of research for this thesis.

5.2 Impact of ICT Penetration: Emerging Cyber Environment

The following trends in ICT are irreversible

- Industry is increasingly reliant on information and communication infrastructures
- National level governance is dependent on secure IT and communication infrastructures.
- Defence Information Infrastructure is enmeshed with government, industry and other agencies through shared resources of the electrical grid, telecommunications, and the Internet
- On line services for financial institutions, insurance, banking, transport, energy etc. are emerging as the largest users of NII.
- Downsizing and cuts in government and private infrastructure are "off-set" by information technology.
- COTS technology is used widely in defence and civil sectors.

- Open architecture leaves sources of information readily available to opponents and therefore prone to attack. The attack on ICT can be virtually indefensible. Corrupting computers on a massive scale can attack economy. Counterfeit electronic currency can flood bank accounts. Hyperinflation can cause economy collapses.
- Warfare has become very visible. Televised atrocities and deaths of own troops become a tool for adversaries to sway public opinion.

5.3 Impact of IW in the Emerging Cyber Environment

The IW threats have significant bearing on the socio-political, socio-economic, techno-economic and military strategic domains across the globe. With the emergence of state of the art ICT infrastructure, we in India will also be the targets of these IW threats in each of these domains as described in the succeeding paragraphs [15,131,132].

5.3.1 Socio-political Dimension

- The ICT penetration has lead to rapidly expanding awareness among the people even in remote areas which hitherto was possible only through formal education, leading to the following:
 - Disparity and unequal distribution of wealth.
 - Political developments are broadcast into public domain even before government receives them. This forces the leadership to react and respond rather than guide and lead the population.
 - Awareness about the quality of life induces expectations far beyond means.
 - Cultural visibility of increasing ethno-nationalism, religio-political radicalism results in erosion of state control over social, economic, political and administrative issues.
 - Rampant corruption, societal violence and conflicts, erosion of trade barriers, protectionism and cartel building.
- This often leads to expectation trauma and its management because of the following:
 - Structural and situational limits to the rate of growth of achievements in the developing world causes frustration.
 - Widening actuality gap between expectations and reality or fulfillment
 - Consciousness and perception of deprivation
 - Destabilization effect in the face of diminishing family life, spiritual solace, moral values and traditions
 - Expectation – achievement gap leading to disillusionment and frustration
- Impacts of these developments are as follows.
 - Political interference in economic activities
 - Social crisis and turbulence
 - Struggle to alter elite structures and systems controlling economic opportunities and social justice

5.3.2 Techno–Economic Dimension

The ICT revolution has led to unprecedented economic activity resulting in the following: [15].

- New range of sources of IT based economic productivity
- Unprecedented rate of change of technology (electricity, radio, personal computer, fibreoptics)
- Unlimited opportunities
- The business is expected to grow to \$1.4 trillion by 2003.
- Private currency trade will grow to \$ 1.3 trillion per day.
- Global financial market was already \$ 83.0 trillion in 2000.
- Information and knowledge are the new sources of wealth.
- Distributed production and global marketing.
- Emergence of weightless goods (software, internet, entertainment).
- Emergence of new class of services (tele-medicine, medical transcription).

5.3.3 Military-Strategic Dimension

The development in ICT has led to the following:

- Emergence of new areas of Information Age War.
 - Information-in-Warfare.
 - Information Warfare.IT embedded sensor technologies (reconnaissance, surveillance, target acquisition).
- ISR, C4I, PFT, Network Centric warfare paradigms system of systems.

5.3.4 New World Information Order

The ICT development has led to a new world Information Order leading to the following [152]:-

- Bearing on social, political, economic and military balance.
- Empowerment of non-state actors and individuals.
- Integrating illegal activities of terrorists, profilers, drug cartels, and criminals. It strengthens anarchy and control.
- Large volume and mobility of funds across the globe including money laundering.
- Breaks hierarchies, creates new power structures.
- Brings supremacy and vulnerabilities to possessors of IT.Cedes authority to market and transnational entities.
- Reduces risk to soldiers, increases cost of conflicts.
- Cuts across military, political, social and economic power.
- Reduces strategic relevance of territory, large army and heavy industry.

5.3.5 Collateral Effect

The combined effects of the emerging ICT on the social, political, economic and military landscape has led to the following:

- **e-Foreign Policy** : ICT facilitates tackling of global challenges by a new constituency of information scientists, lawyers and international civil servants.

- **e-Governance:** ICT facilitates strategic economic planning, better resource utilization, control and monitoring of development programs, reduced cost of operation, single window citizen and business services, improved investment climate, equitable distribution of wealth and social equivalence to all.
- **e-Politics:** ICT changes the nature of politics and methods of exercising power, controls information glut, illuminates most important, introduces historical perspective and simulates alternatives.
- **e-Military:** ICT can enable a pound of silicon to outperform a ton of uranium.

The combined effects of all these is resulting into a cyber space which while giving over whelming advantages to the human society, is also beginning to threaten individuals, organizations, states, regions and nations in correspondence with their role and relevance. This is taking many forms of internal and external conflicts termed as information warfare, cyber war or net warfare of a different kind which can cause disabilities, damage or destruction to information assets at personal, organization, state, national or global level, depth and scale.

5.4 IW Threat Scenario

In Information Warfare, there are no fixed boundaries. One may not know who is under attack and who is in charge. One may not know what is real and what is not in case of information disorientation.

Finding strategic intelligence is difficult, as we may not know who will be our adversaries or what will be their capabilities. We may not know that we are under attack, who is attacking us or where the attack is coming from. If we are looking towards building and sustaining coalition with a friendly nation, in all probability we may depend on some one who is as naive and vulnerable to attack as we.

With the current and projected level of NII sophistication, India as a subcontinent is vulnerable to IW attacks. With an unknown enemy, unknown point of attack and unknown target, India will be lost as a sanctuary if we build our strategy around critical vulnerabilities. We will be vulnerable on every front be it economic, social, religious, transport, agriculture, trade, communication, defense, space etc. It is therefore extremely critical to map our national cyber space, establish precise boundaries, entry and exit points, examine operational and technical vulnerabilities in NII, assess internal, external, natural or manmade threats and prepare a profile of risks to the NII which can be minimized, mitigated or managed.

5.5 Source and Diversity of IW Threats

The IW threat to NII / ICT can come in many forms. The challenge in evaluating that threat, and the appropriate level of protection or response would be in sorting out the actual from the perceived, and determining the potential for future developments on the following lines. [35,36,37,54,102]

- What is known -- the validated threat

- What is suspected -- trends, indications, and the assessment process
- What is unknown -- potential events based on existing capabilities

These threats vary in terms of intent, sophistication, technical means, origin and potential impact and can be categorized into the following groups.

- Incompetent, inquisitive or unintentional blunderer by mischief-makers, pranksters or hackers driven by technical challenge
- Disgruntled employees, unhappy customers intent on seeking revenge for some perceived wrong
- A crook interested in personal financial gain or stealing services
- Major organized crime operators interested in financial gain or in covering their crimes
- Individual political dissidents attempting to draw attention to a cause
- Organized terrorist groups or nation states trying to influence policy by isolated attacks
- Foreign espionage agents seeking to exploit information for economic, political or military intelligence purposes
- Tactical countermeasures intended to disrupt specific military weapons or command systems
- Multi-faceted tactical and strategic IW capability built around EMP and RF energy weapons applied in a broad orchestrated manner to disrupt a major military mission or to launch an IW attack to support a major military mission against an adversary
- Large organized groups or major nation-states intent on overthrowing by crippling the NII of a target nation

5.6 Analysis and Perception of IW Attacks

The perception about the type, source and impact of IW attacks is still at nascent stage in the country. The availability of tools, expertise and organized framework to examine information about intrusion, crime, threats, vulnerabilities, is still very low. Therefore perception about on-going IW attacks on the national infrastructures is at a low key as the central information repository and analytic capability to examine cyber events, physical disruptions, criminal activities and coordinated attacks does not exist at national scale.

5.6.1 Targets of IW Attacks:

The physical and information technology facilities, networks and assets whose disruption or destruction would have serious impact on the health, safety, security, economic well-being of the citizen or on the effective functioning of government in the country are illustrated in figure 5.1.

Type of Infrastructure	Services
Government	Essential Government Services/ Activities not

	included elsewhere.
Energy and Utilities	Electrical Power, Water Purification, Sewage Treatment, Natural Gas Industry, Oil Industry.
Services	Health Care, Food Industry, Postal/Courier, Meteorological, Financial Services, Customs, Immigration.
Transportation	Aviation, Surface, Rail, Marine.
Safety	Nuclear, Hazardous Material, Prisons, Flood Control, Environment, Search and Rescue, Emergency Services, Building Systems.
Communication	Telecommunications, Television Industry, Satellite Systems, Radio Industry, Cable Television Industry, Mobile Phones etc.

Figure 5.1 CNI targets of IW attacks

5.6.2 Integrated Physical and IW Attacks Scenario

A typical scene illustrated in figure 5.2 can happen and we need to possess sufficient capability at inter agency, central or state government level, for correlation of data to support crisis and action planning in response to natural, man made unintentional or deliberate cyber attacks.

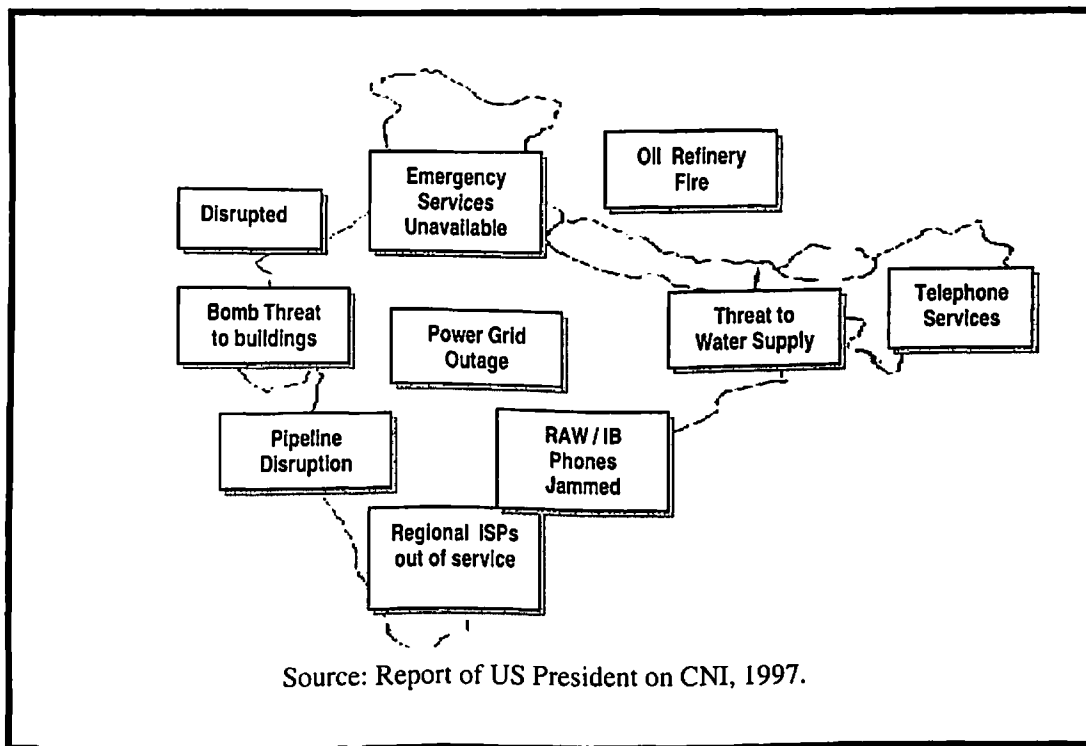


Figure: 5.2 Integrated Physical and IW Attack Scenario

5.7 Impact of IW Attacks

The Critical National Infrastructure (CNI) can be disabled, damaged or disrupted through physical or IW attacks. Impacts of these attacks is examined in the succeeding paragraphs [36,37,80].

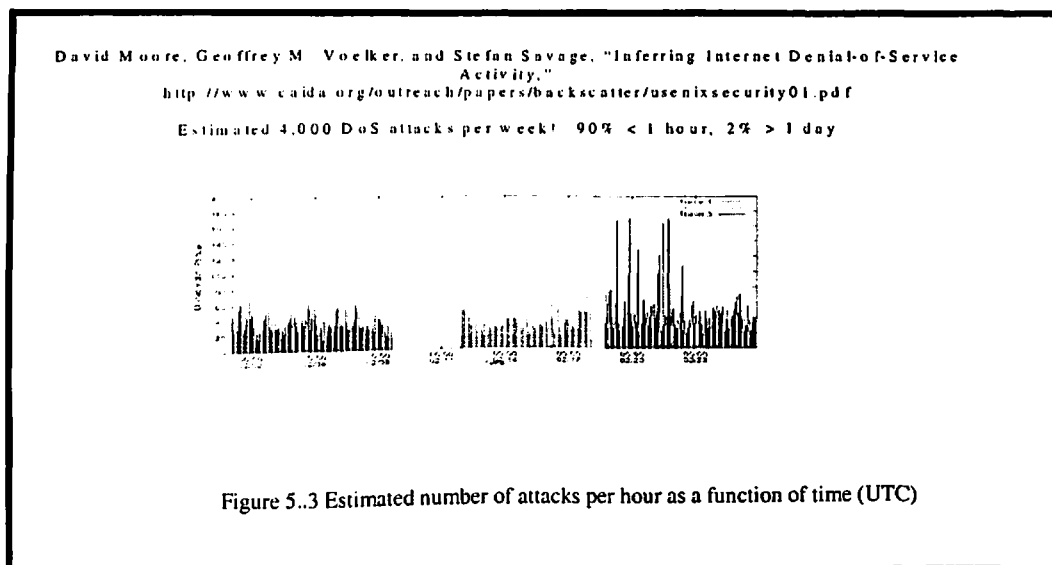
5.7.1 Type of Damage

The IW attacks on NII can result from the third party connections to other organizations, dial up, remote access, internet, foreign governments, use of EMP and RF energy weapons etc. The attacks can results in the following:

- Disability, damage or destruction of electronics embedded in ICT infrastructure targeted by EMP and RF energy weapons.
- Disruption of business, loss, misuse and modification of critical data, perpetration of frauds, damage or stealing of assets, denial of service, loss of customer confidence etc.
- The enemies or own employees with malicious intent can force business outages through viruses, system outages, network outages and site outages.
- The FBI; USA 1999 survey has revealed the following:-
 - 90% security breaches detected
 - 70% were serious breaches involving theft of proprietary information, financial fraud, sabotage of data or networks
 - average loss due to financial fraud or theft of proprietary data was over \$1M
 - 71% reported insider attacks
 - 49% reported Internet as frequent source of attack
 - 34% reported 2 to 4 incidents
 - 19% reported 10 or more incidents

5.7.2 Attack Frequency:-

The number of Denial of Service (DoS) attacks analysed by Davis Moore et all as a part of study titled “Inferring Denial of Services Activity” are shown in the Figure 5.3 [47].



5.7.3 Point of Attack

The IT systems can be attacked through remote dial in access, Internet or Intranet. The CSI/FBI, USA survey of attacks from 1996 to 2001 indicates increasing incidents of

attacks from internet, followed by attacks by own people from the Intranets as shown in the figure 5.4.

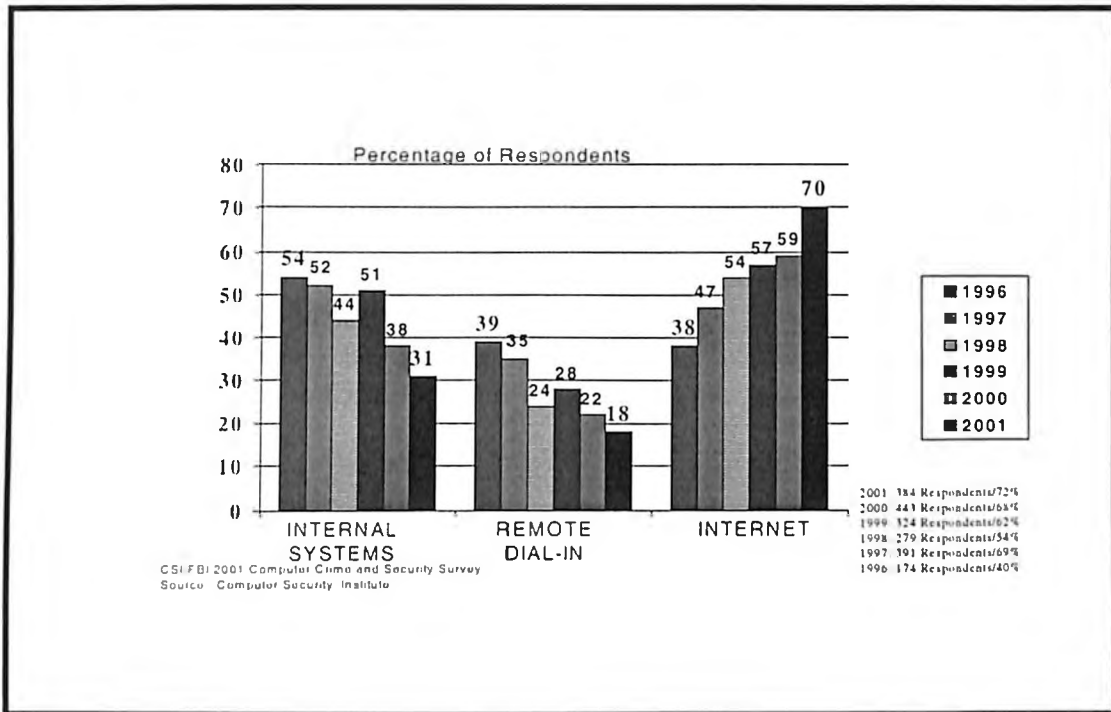


Figure 5.4 Point of Attack

5.7.4 Financial Losses

The CSI/FBI, USA survey reveals that most of the victims do not report financial losses suffered through cyber stealing or fraud. The trends are shown in the figure 5.5.

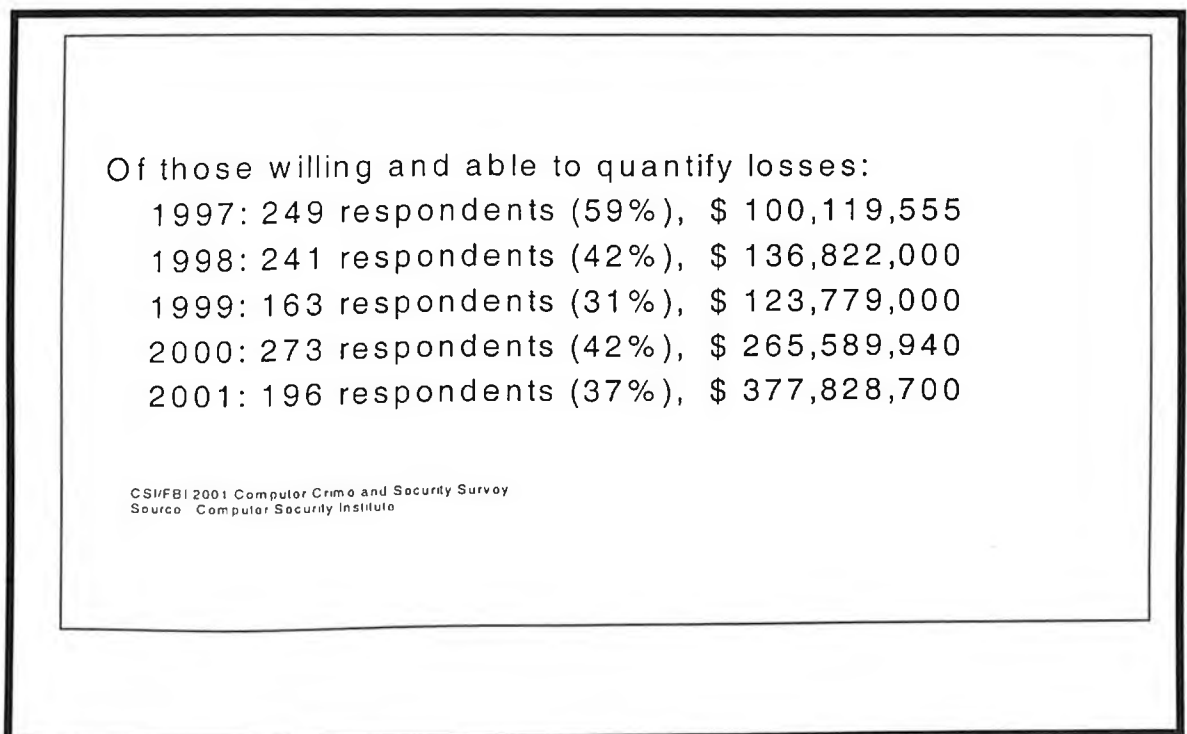


Figure 5.5 Financial Losses

5.7.5 Systems Affected (Code Red Worm)

The consequent of attack by worm code red is given as follows: -

- Worm probes random IP addresses and infects web servers vulnerable to IIS exploit
- Defaces English websites hosted on server with message:
 - Welcome to <http://www.worm.com>! Hacked by Chinese!
- On July 19, over 359,000 hosts infected in 13-hour period
 - over 2,000 hosts infected per minute at peak
 - at 5:00 pm, worm attempted DoS attack against 198.137.240.91 (www.whitehouse.gov)
 - David Moore – www.caida.org/analysis/security/code-red/index.xml Estimated 975,000 servers infected by end of August with losses of \$2.4 billion – Computer Economics

5.7.6 Attack Sophistication

Initially due to lack of tools and technology support, very high level of individual level competencies were needed to launch an IW attack. However with the emergence of high end tools the attack sophistication has reduced as shown in figure 5.6.

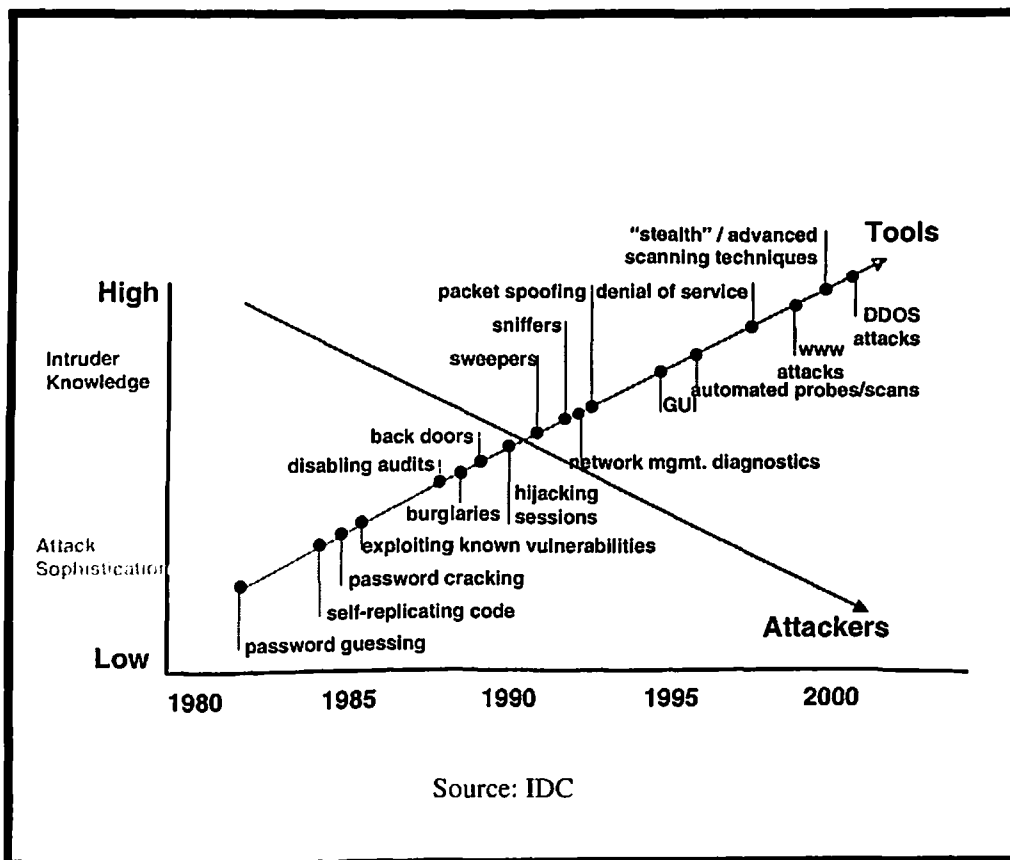


Figure 5.6 Attack Sophistication vs. Intruder knowledge

5.8 China and Russia's Electromagnetic Weapons

Following details of China's EM weapon's program signify the seriousness of IW threat to India [137,151]

5.8.1 Electromagnetic Gun

- In 1999-2001, the PLA was engaged in developing a "shell-less gun" (electromagnetic gun, or EMG). Present efforts are concentrated on developing:
 - An anti-tank EMG
 - An anti-aircraft EMG
- At the same time, the PLA is engaged in developing a new generation of light weapons for the 21st century (portable weapons for ground troops), based on new principles. This includes a shell-less gun and small-sized sources of an electromagnetic field.

5.8.2 EMP Bombs

- At the beginning of 2000, Chinese military strategists called for the accelerated development of EMP bombs or missiles as a means to destroy U.S. aircraft carriers.
- The PLA claims the "high degree of electronization" is the Achilles' heel of U.S. aircraft carrier fleets, whose electronic equipment is their "central nervous system." Also, U.S. carrier groups are easy targets for attacks by satellite-guided EMP missiles, which could paralyze the fleets' electronic equipment and render ships helpless to conventional air and sea attack.
- Short- or medium-range EMP bombs or missiles only need to explode within dozens of miles around the carrier to destroy all important shipboard integrated circuits and chips in the electronic equipment, thus paralyzing the radar and telecom system of the aircraft carrier and the vessels around it, as well as ship-mounted missiles and aircraft.
- Remarkably, the joint development of electromagnetic weapons of several kinds is definitely included in the June 1999 and January 2000 Chinese-Russian agreements on long-term military-technological cooperation on high-tech weapons.
- In December 2000, Col.-Gen. Zhang Wannian, second in command of the PLA (after Jiang Zemin), said that war with Taiwan is "inevitable" and that the use of EMP warheads will paralyze Taiwan's electrical power supply and potentially its air force as well.
- Reportedly, the development of EMP warheads in China accelerated in 2001.

5.8.3 Radio-Frequency (Microwave) Weapon

- By the end of 2001, Russia had developed a microwave weapon and proposed it to "old friends" China and India [137].
- Particularly, in November-December 2001, Russia's state-owned arms-export monopoly, Rosoboronexport, began selling the world's first openly marketed radio-frequency weapons, the "super-enemy" of electronics.
- Experts have long worried that terrorists and thugs would use radio frequency (RF) weapons. RF weapons can disperse a non-nuclear electromagnetic pulse over a wide

area, crippling computers, phone networks and electrical appliances, civilian as well as military.

- Executives from Rosoboronexport made presentations about two weapons – "Ranets-E" and "Rosa-E" – at the Lankagwi International Maritime and Aerospace 2001 exhibition in Malaysia in October 2001.
- The Ranets-E system is claimed to be able to incapacitate the electronics of incoming aircraft and missiles. It is a "mobile RF defense system against high-precision weapons." This system consists of an antenna, a high-capacity power generator, control and measuring equipment and an energy supply subsystem. The Ranets-E can be installed on a stationary or mobile base, including transport aircraft. Its energy output exceeds 500 megawatts and it can disable the guidance system of missiles and avionics of fighter aircraft in a 20-mile range. The Ranets-E is a real "RF cannon." It has a maximum range of 20 miles and can fire in a 60-degree arc. Targeted electrical and electronics systems stop functioning.
- The Rosa-E system is designed to break the electronics of the enemy's radar systems and other ground-based military installations. Though smaller in size and having less output than Ranets-E, Rosa-E is intended to disperse over a wide area, affecting any and every electronic device in the target area. It can be launched from aircraft or even from short-range missiles. It releases an energy burst of 100 kilowatts, affecting everything from computers to power distribution systems and radar screens. It, too, works in the centimeter-wave frequency range. It will not be difficult for China to rapidly organize serial production of both systems.

5.9 Survey of IW Capability of Different Nations

The US, DoD has prepared a list of nations who have developed a range of IW capabilities as shown in figure 5.7.

Enabling Technologies	Country	OPESEC	PSYOPS	EW	Deception	Destruction Lethal	Destruction Non - lethal	Encryption	S/W Eng.	Network Eng.	Computer Security	Info Security	Comms. Technologies	HPMW	Physical Security	Intelligence
	China	↗ D	= D	= A	= D	↘ D	↘ D	↘ D	↘ A	↘ A	↗ A	= D	↘ D	= D	↗ D	= D
	North Korea	↗ D	↗ D	↘ A	= D	↘ D	↘ A	↘ D	↘ A	↘ A	↘ A	= D	↘ A	↘ A	↗ D	= A
	Iraq	↘ D	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↗ D	= A
	Iran	↘ D	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	= D	= A

India	= D	↘ A	↘ A	↘ A	↘ D	↘ A	↘ D	↗ D	↗ D	↘ D	↘ A	= D	↘ A	= D	= A
Egypt	↘ D	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	= D	= A
Cuba	↘ D	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	= D	= D
Libya	↘ D	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	= D	= A
Syria	↘ D	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	= D	= A
Legends	↗ Signifies, equal to our best effort.		= Average or good capabilities		↘ Minor or nascent capabilities		D Developer making and / or exporting		A Acquiring from external sources.						
Source : DSB Report, IW Defence, Threat Assessment															

Figure 5.7 IW capability of Different Nations

As an example of a country heavily involved in developing its own capability, consider Russia. Of the 15 categories listed, Russia has a significant capability in seven categories and a good capability in four (total: 11 of 15). Today almost any nation is capable of developing significant Information Warfare capabilities. Unlike nuclear capabilities, IW is relatively inexpensive and easy to acquire. A country can acquire a strategic capability without requiring a significant investment, or a long-term development cycle. The technologies required to perform many of the IW attacks are available today. The issue of whether or nor they comprise a strategic threat is more a matter of coordinated timing. Some may come in the form of a simple attack on a target identified as a single point of failure. A more complex, coordinated attack can be of multi-dimensional nature.

5.10 Different Perspectives & Views of IW

Concepts expressed in National Security Agency, USA briefing paper titled "Ensuring Information Superiority for the 21st Century", presented by Lt. Gen. Minihan at NSTAC session, May 1996 are summarized as follows:

- National Security View of IW:
 - Protection of information has intrinsic value - National interest.
 - Cost of compromise is difficult - can be life threatening.
 - Risk avoidance approach is a traditional response.
- Private Sector / Commercial View of IW:
 - Cost of doing business - pass the expense on to the customer.
 - Countermeasures have a definite expected value.
 - "Insurance" approach is the traditional response.
- National and Private Sector Information Security are Now Inexorably Intertwined:

- Zone of cooperation is emerging i.e. where do protection, detection and response responsibilities lie?
- Risk management rather than risk avoidance is preferred

5.11 Systems Vulnerable to IW

The spectrum of targets for IW attack can be very large and diverse and can range from GPS jamming to corrupting of missions, exploitation of emissions, damage, disability or destruction of electronics, corruption of real time data, munitions that can be armed or made inert etc. A consistent IW attack can totally paralyze and incapacitate even a well-formed military force. With large scale computerization and dependence on data banks, the other risk areas where tampering or misinformation can be planted are the medical facilities, logistics, personnel data, cargo, transport, space, finance, trade, general administration, industry etc., categorised as follows:

- Computer Networks and Databases of National Services viz. Satellites, Department of Telecommunications, Railways, Shipping, Oil, Electricity etc.
- Corporate Networks and Databases viz. Finance, Banking, Trading, Industrial Activity etc.
- Government systems viz. Office Records of Revenue, Education, Healthcare, Personnel, Administration etc.
- Defence Information Infrastructure

A typical scene for infrastructure attack as perceived in the report of the US President's Commission on Critical Infrastructure Protection is shown in figure 5.8 [35] .

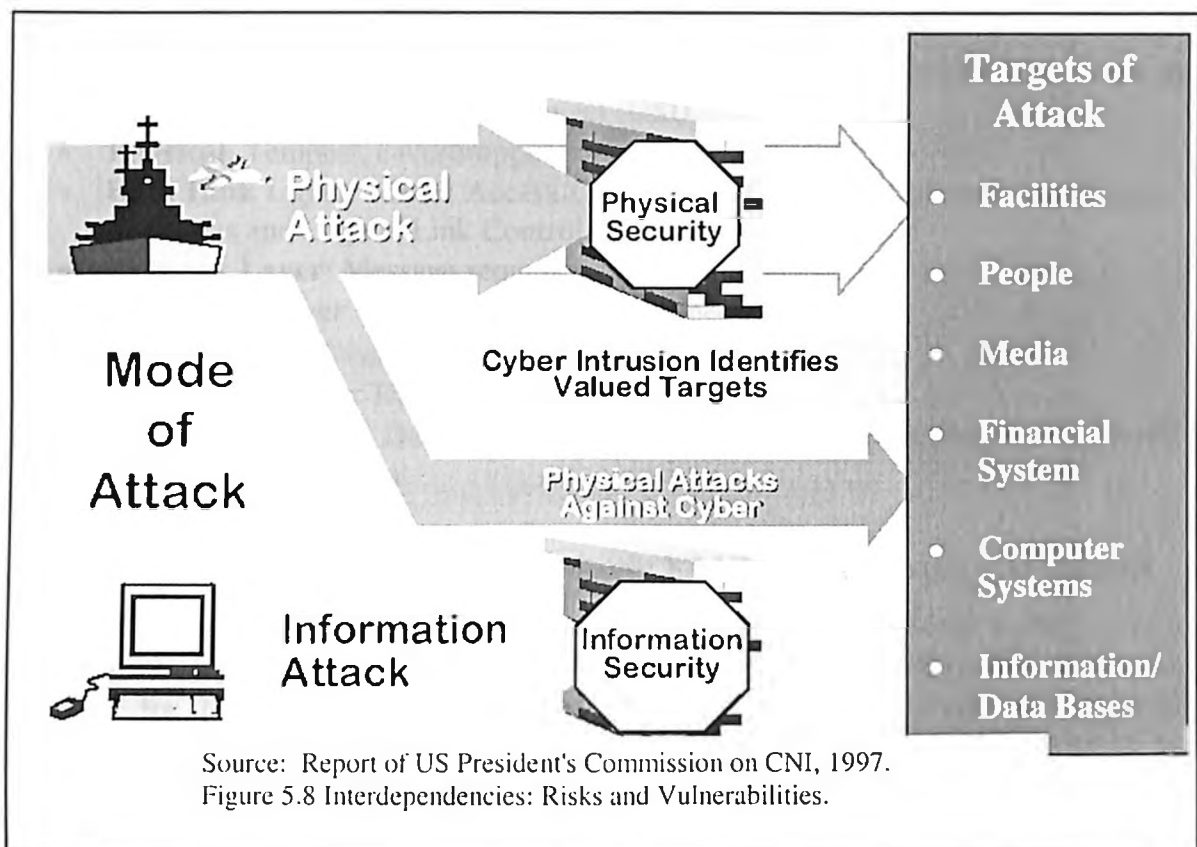


Figure 5.8 Interdependencies : Risk and Vulnerabilities

5.12 Range of Threats & Vulnerabilities

The attacks can be launched at bare machine, computer system and network level as summarized in the succeeding paragraphs [90,150].

5.12.1 Bare Machine level - Hardware Domain Violations

- Alter machine register and flags.
- Alter internal Arithmetic Logic Unit, data bus, control bus and address bus contents.
- Change bootstrap logic to prevent power on self-test routines.
- Change micro program to render it completely non-functional.

5.12.2 Computer Level - System Domain Violations

- **Access Databases:** Delete, overwrite, corrupt, alter, falsify, steal databases
- **Access Directory Services:** Change, delete, falsify, substitute names of users
- **Access Operating System:** Assume super user status and change access rights, execution priorities, user privileges etc.
- **Access Libraries, Support Software:** Change reference identities, computational role, and reusability parameters
- **Application Software:** Alter parameters, change identity, change order of execution, falsify tables and scaling factors
- **Test and Diagnostic Software:** Change configuration tables, interpretation logic etc.

- **Input/Output:** Change reference tables, connectivity matrix
- **Network Level - Protocol Domain Violations:** Enter Protocol Domain at any of the 7 layers of Open System Interconnect (OSI)
- **Physical:** Tempest, eavesdropping
- **Data Link Layer:** Media Access Control (MAC), sharing of media collisions, deny the routes and Logical Link Control.
- **Network Layer:** Message sequences garbling
- **Transport Layer:** Changes end-to-end connectivity
- **Session Layer:** Disable peripherals
- **Presentation Layer:** Data encryption
- **Application Layer:** Decrypting message contents, disrupting program logic and sequence of execution

5.13 IW Attack Tools: Cyberwar vis-à-vis EMP or RF Energy Weapons

The IW attacks on infrastructures at national scale can be conducted through a series of hacker attacks, synchronized in time, combined with physical attacks. The most common choice for physical attacks would be switching stations, communication antennas, pipelines transformers, pumping stations and the cabling systems. The attacks on the information infrastructure can be through network penetration viz. virus attack, spamming etc. These attacks can also be launched through EMP/RF energy weapons to disrupt, disable, damage or destroy the electronics embedded in the IT systems. The mode of attack, availability of attack tools and cost of launching the attacks is illustrated in figure 5.9 [35,80,150].

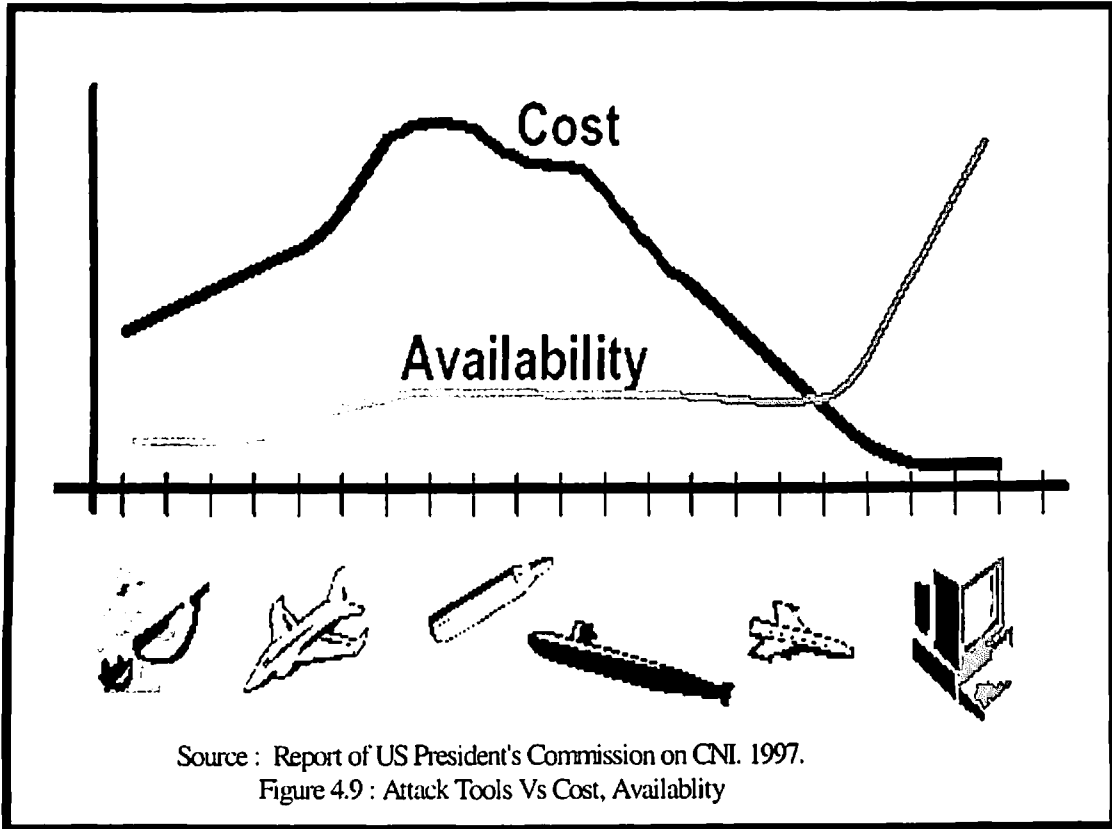


Figure 5.9 Attack Tools Vs Cost, Availability

5.14 IW –Offensive and Defensive Operations

IW involves offensive and defensive operations against information resources of a win-lose nature. The offensive operations acquire, exploit, degrade, disrupt, deny, and destroy information resources. The defensive operations target or exploit weaknesses in human nature/practices, physical environments, technology and how it is used. Both sides in conflict can use offensive and defensive operations as shown in figure 5.10.

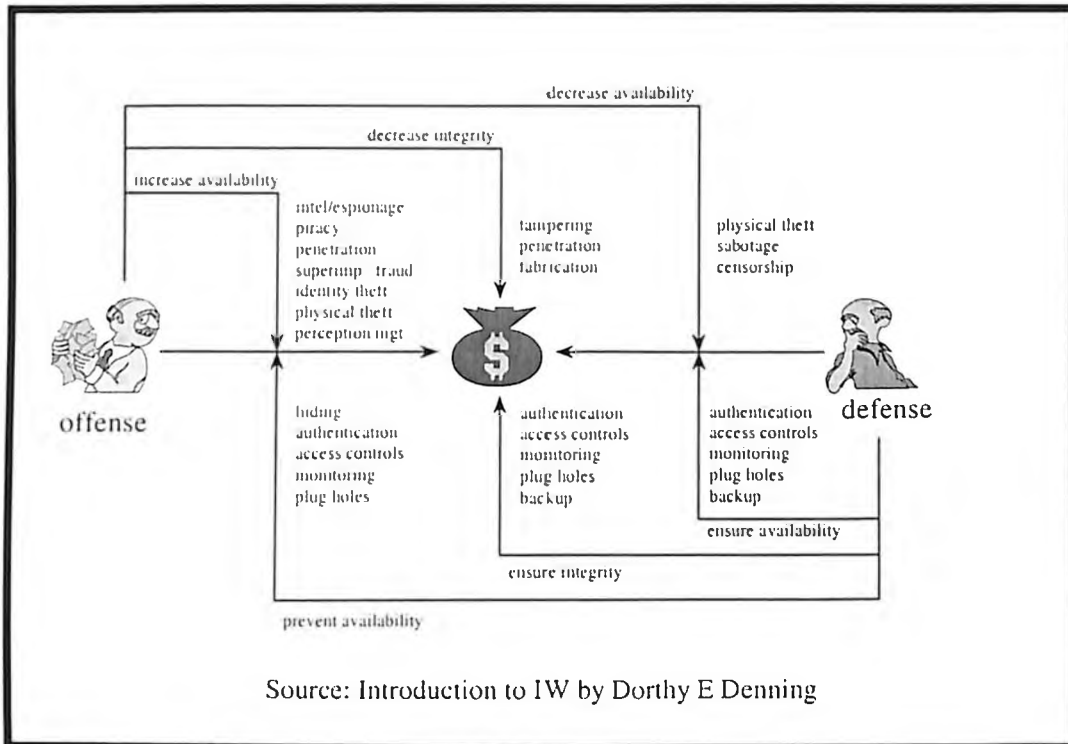


Figure 5.10: IW Offense and Defence

5.15 Levels of Vulnerability and Threat

5.15.1 Vulnerability Of Critical Infrastructure

Vulnerability is a characteristic of a critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat. The typical vulnerabilities are illustrated in figure 5.11[54,204,208]

- **No Vulnerability:** A critical infrastructure, which by designs, implementation, or operation or any combination has no assessable susceptibility to destruction or incapacitation by a threat.
- **Low Vulnerability:** A critical infrastructure, which by designs, implementation, or operation or any combination has a limited assessable susceptibility to destruction or incapacitation by a threat.
- **Medium Vulnerability:** A critical infrastructure, which by designs, implementation, or operation or any combination has a moderate assessable susceptibility to destruction or incapacitation by a threat.
- **High Vulnerability:** A critical infrastructure, which, by design, implementation, or operation or any combination has a extreme assessable susceptibility to destruction or incapacitation by a threat.

<ul style="list-style-type: none"> • Wiretapping and Eavesdropping • Simple Masquerading : Spoofing • Software Piracy • Back Doors • Timing attacks • Trojan Horses • Viruses, Worms • Data Diddling • "Black Windows" • Excessive Privilege, • Distributed Denial of Service • Dumpster Diving Cryptographic Attacks • Information Leaks, Covert + Overt 	<ul style="list-style-type: none"> • Password Cracking • Social Engineering • Router and DNS attacks • Replay Attacks • Key, Sequence Prediction • Denial of Service • Screen Capture • Shoulder Surfing • "Runtime Patching" • Malicious Active - X. • MIME attacks • Malicious Email Attachments • Steganography • Inference and Aggregation • Information Warfare
--	---

Figure 5.11: CNI Vulnerabilities

5.15.2 Threats to Critical Infrastructure

The CNI can be exposed to a large number of IW attacks with varying degree of threats [27,90,93,160].

A foreign or domestic entity may possess both the capability to exploit a critical infrastructure's vulnerabilities and the malicious intent of debilitating defense or economic security. A threat may be an individual, an organization, or a nation or may be a natural or accidental event.

- **No Threat:** No assessable potential for an individual, organization, nation or natural or accidental event or combination possessing both the capability to exploit vulnerabilities and the malicious intent for disruption or destruction of critical infrastructure(s).
- **Low Threat:** - Limited assessable potential for an individual, organization, nation or natural or accidental event or combination possessing both the capability to exploit vulnerabilities and the malicious intent for disruption or destruction of critical infrastructure(s)
- **Medium Threat:** Moderate assessable potential for an individual, organization, nation or natural or accidental event or combination possessing both the capability to exploit vulnerabilities and the malicious intent for disruption or destruction of critical infrastructure(s)
- **High Threat:** Extreme assessable potential for an individual, organization, nation or natural or accidental event or combination possessing both the capability to exploit vulnerabilities and the malicious intent for disruption or destruction of critical infrastructure.

The CNI can be viewed to comprise of various layers viz. terrain layer, feature layer, control layer, technical & application layer and operations layers. Each of

these layers is represented by different systems, which are prone to IW attacks. The potential of these attacks and consequent impact is illustrated in figure 4.12.

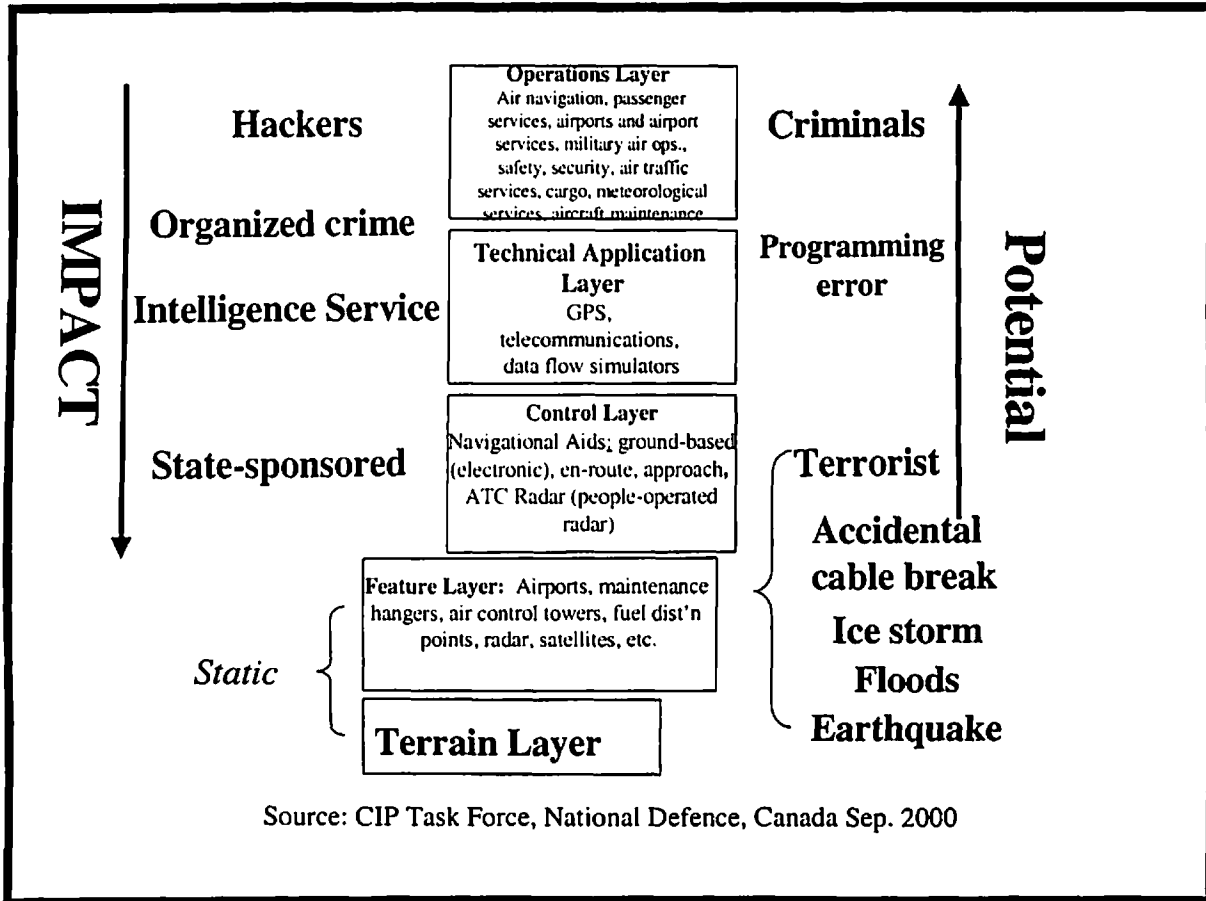


Figure 5.12: CI Threat Layers

5.15.3 Risk To Critical Infrastructure

Risk is a combination of vulnerabilities and threats as illustrated in figure 5.13.

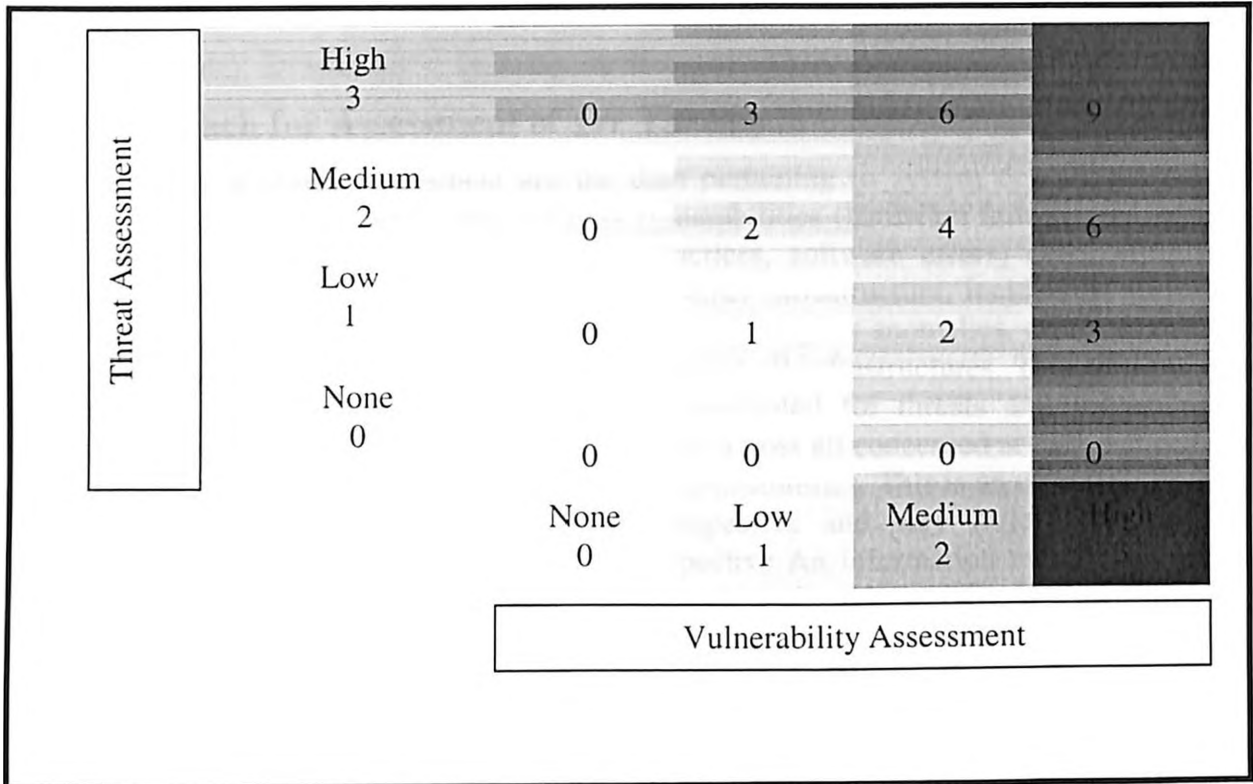
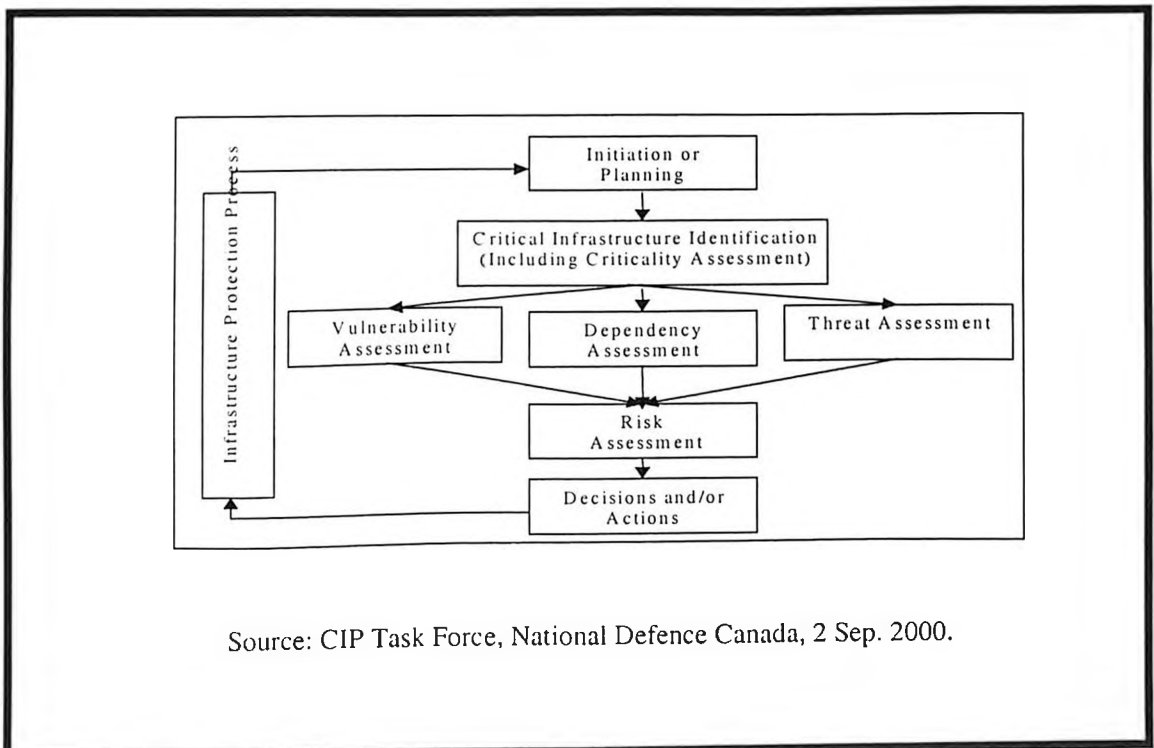


Figure 5.13: Typical Risk Assessment Model

5.15.4 Risk Management

The IW-Defense comprises of efforts and means to minimize or mitigate the risks completely though an infrastructure protection process illustrated in figure 5.14.



Source: CIP Task Force, National Defence Canada, 2 Sep. 2000.

Figure 5.14: Infrastructure Protection Process

5.16 Approach for Assessment of IW Threats

The inputs to threat assessment are the data pertaining to system degradations due to physical acts, cyber based events such as vulnerabilities (hardware failure rates, operator induced malfunctions, poor maintenance practices, software errors) cyber or physical vulnerabilities resulting from dependence on other infrastructure, incident of vandalism, malicious mischief, suspicious activities, physical or cyber anomalies, criminal statistics, threat data, interdependencies etc. available across all infrastructures. This requires to be appropriately collected, collated, processed, evaluated for threats and vulnerabilities, mapped as current or future risks and distributed across all concerned at different echelons in public, private, civil and military areas of responsibilities. This is an extremely complex task from technology and coordination perspective and very little work has been progressed in this direction from an IW perspective. An information model Used by the Defence Science Board Task Force, USA to undertake this activity is shown in figure 4.15.[35]

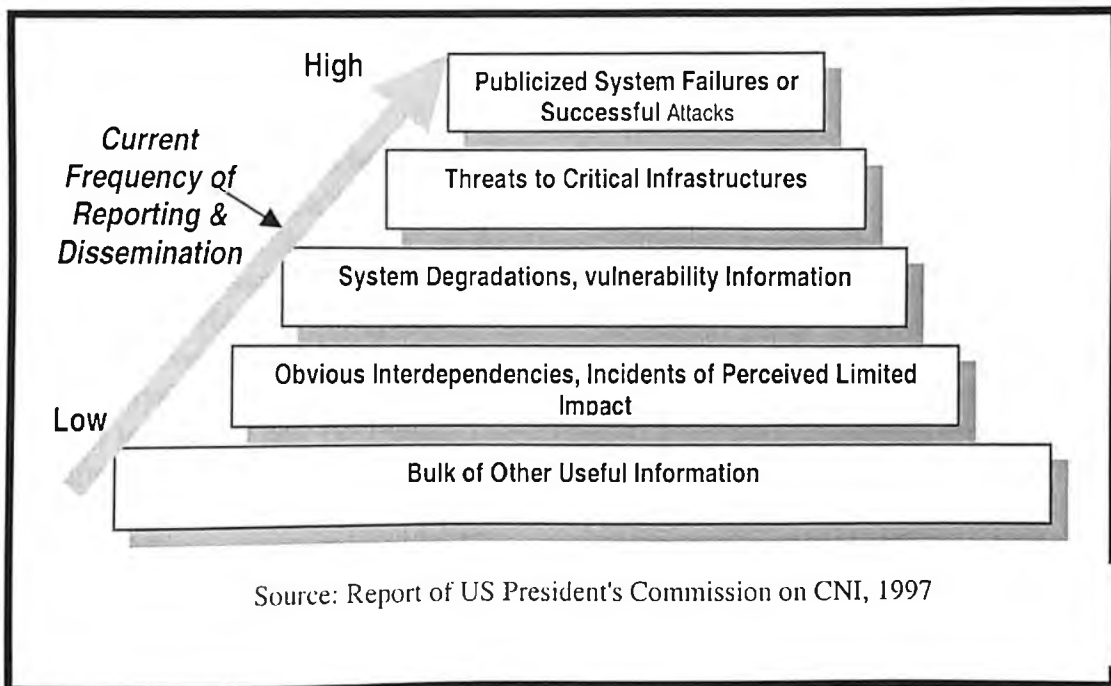


Figure: 5.15 Scope of Useful But Unavailable Information

5.16.1 Measures to Evaluate IW Threats

The Defence Science Board, USA, in its report had recommended a number of measures to evaluate IW- threats so as to build a credible IW- Defence capability. The summary of these recommendations highlighted in DSB, USA report of Mar 2001 are given as follows and considerable efforts are underway to complete actions by the concerned agencies.

- Designate an accountable IW focal point.
- Organize for IW-Defence.
- Increase awareness.
- Assess infrastructure dependencies and vulnerabilities.
- Define threat conditions and responses.
- Assess IW - Defence readiness.
- Assess IW-Defence readiness.
- Raise the bar with high- pay - off, low cost items.
- Establish and maintain a minimum essential information infrastructure.
- Focus on research and development.
- Staff for success.
- Resolve the legal issues.
- Participate fully in critical infrastructure protection.
- Provide resources.

5.16.2 Measures to Minimise or Mitigate IW Threats

The Defence Science Board, USA, has proposed a collective national level effort to establish national structures to facilitate effective partnerships amongst government agencies, infrastructure owners and operators to accomplish national infrastructure assurance policy, planning and programs. This structure is expected to evolve policies, evolve prevention and mitigation strategies, undertake or facilitate information shaping and analysis, incident management, response, restoration and reconstitution across the nation to counter any IW threat. The proposed roles and responsibilities are described in figure 5.16. A similar approach had been evolved by me in paper titled “ Protection of Critical Infrastructure - The Need for National Initiative”, and submitted to the National Security Council secretariat [35,37].

Agency	Roles & Responsibilities
Office of National Infrastructure Assurance	<ul style="list-style-type: none"> - Propose national objectives & strategies. - Propose / promote legislation. - Coordinate federal policies and programs.
National Infrastructure Assurance Council	<ul style="list-style-type: none"> - Include public & private sectors. - Provide forum for national leaders. - Devise awareness and prevention strategy.
Federal Lead Agencies	<ul style="list-style-type: none"> - Coordinate efforts with Assurance Council - Work with owners-operators to fashion policy.
Sector Infrastructure Assurance Coordinators	<ul style="list-style-type: none"> - Provide private or non-profit entity for each sector. - Coordinate with Lead Agency. - Education, awareness & R&D.
Infrastructure Assurance	<ul style="list-style-type: none"> - Facilitate public private partnership.

Support Office	- Assist in coordination of federal policies and programs. - Assess vulnerabilities.
Information Sharing & Analysis Center	- Public & private staff. - Collect & analyze Information - Disseminate findings.
Warning Center	- Provide warning of an attack, physical, or cyber, on Infrastructures.
Source: Report of the US, President Commission on CNI	

Figure 5.16 : Proposed Roles and Responsibilities for National Infrastructure Assurance

5.17 IW Objectives

IW is viewed from national security perspective, threats to civil and military interests and localized activities of institutional hackers, criminals and terrorists groups, with following objectives [39,68].

- Personnel and transport interdiction
- Harassment of opposition
- Communication disruption
- Destruction of Automatic Data Processing (ADP) capability
- Interruption of transport Services
- Sabotage
- Terrorism /Anti Terrorism
- Air land Defence
- Military offensive
- Enemy ordinance activation
- Communication interference
- Electronic component destruction

5.18 IW Threat Spectrum & National Security

The IW threats can be categorized as national security threats, shared threats to civil and military establishments and local threats as illustrated in figure 5.17. For the purpose of my Ph. D research it is proposed to examine IW threats having direct bearing on the national security having military dimension.

Threat Type	Source of Threat	Impact
National Security Threats	Information warrior	Reduces country's decision space, causes chaos and target damage.
	National Intelligence	Information gathering for political economic and military gains
Civil & Military Shared Threats	Terrorists Attacks	Visibility, publicity, Chaos, social, religious. political change

	Industrial/ Economic Espionage	Competitive gains, market dominance
	Organized Crime	Revenge, retribution, financial gains, institutional change
Local Threats	Institutional Hackers, Employees	Monetary gain, thrill, challenge, prestige
	Recreational Hackers	Thrill, Challenge.
Figure 5.17: IW Threats Spectrum		

5.19 Developing IW Capability for India

Traditionally as a part of modernization programs India's (very limited) focus on information warfare had been confined to the struggle between the opposite sides in the information field for the power of possession, control and utilization of information by means of information technology and equipment. However as a result of the development of information networking technology and the continuous research on information warfare theory and practice, information warfare has developed from conducting soft kill types of operations, such as "electronic operations" and "key point sabotage operations" to conducting "paralysis types of operations", such as "computer virus", "directivity beam weapons", and "electromagnetic pulse weapons". Therefore for the future, information warfare is one of the best means of warfare for India to gain regional parity, to achieve the goals of "least damage", "highest efficiency", "rapidest attack" and "fastest decisive victory", and of "winning without fighting and possession and exploitation of resources". India also needs to achieve multiple strategic goals through its IW capability, including political, economic, psychological, and military goals. The IW in this context can be categorized as follows and the IW functional structure can be viewed as shown in figure 5.18 [124, 187,126].

- According to means : Defensive and Offensive
- According to operations : Military and Non-Military
- According to Motive : Political, Social, Economic, Psychological and Military.

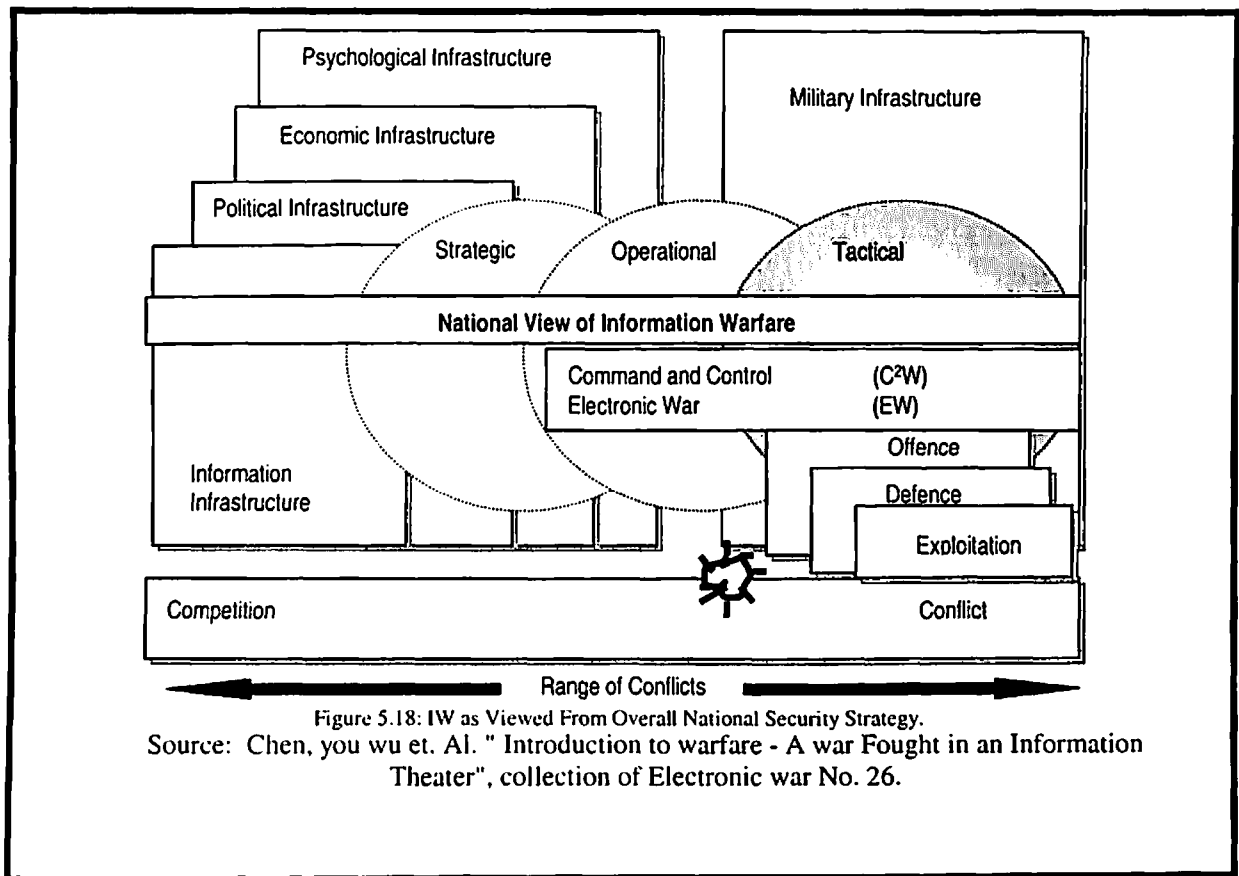


Figure 5.18: IW as Viewed From Overall National Security Strategy.
 Source: Chen, you wu et. Al. " Introduction to warfare - A war Fought in an Information Theater", collection of Electronic war No. 26.

5.20 IW Threats Perception for India

Given India's situation in politics, economy, social psychology, foreign affairs, geography, and military, needs the information and information infrastructure has great impact on the security of the entire country and is vulnerable to information warfare threats. The efforts need to be focused at strategic level on information technology, related infrastructure, tactics and strategic thinking. The focus has to be on winning a "limited war under the condition of high technology". Strategically, the information warfare capability buildup needs to be based on the policy of "limited targets" and "key point highlighting", development of advanced technology, establishment of superior technology conditions, and the foundation of information warfare technology. Tactically, the research on tactics of networking, intelligence collection and space surveillance systems in armed forces, establishing theater and field transparent command and control capability needs to be undertaken. In addition to the Internet offensive and defensive techniques, organizing a new "Internet force", development of "computer virus", logic bomb", and "electromagnetic pulse weapons" needs to be planned. The degree of IW threats, threat spectrum for high value targets involving national security, economy and social structures is presented in the figure 5.19 [134,135,158,159,164,174,175].

Degree of Threat	Threat Spectrum	Threat Value	Potential Targets
Very High Security	<ul style="list-style-type: none"> Strategic EMP Attack Tactical EMP Attack High Power Microwave Pulse Attack 	<ul style="list-style-type: none"> National Security 	<ul style="list-style-type: none"> National Security Council. Defence Headquarters. Ministries of Home, External Affairs & Finance. Apex National Governance Nodes.

			<ul style="list-style-type: none"> • Military Command & Control Nodes. • Weapon Systems.
High	<ul style="list-style-type: none"> • Network Penetration Attacks. • Denial of Service Attacks 	<ul style="list-style-type: none"> • National Governance • National Economy 	<ul style="list-style-type: none"> • Critical National Information Infrastructure Nodes. • Computers & Communication Networks Key National Services. • Industry & Trade.
Low	<ul style="list-style-type: none"> • Computer logic Bomb Computer Virus. • Electronic Information Interference. • Deception and Destruction. • Psychological Communication Threat. • Political Communication Threat. • Media Communication Threat . 	<ul style="list-style-type: none"> • Political, Instability • Social Upheavals • Administration 	<ul style="list-style-type: none"> • National Population • Industry • Business • Public at large
Figure: 5.19 IW Threat to India			

5.21 Proposition for a National IW Framework for India

The research, design and development of all types of IW weapons such as "malicious code", "network penetration" and "EMP / RF energy weapons" is necessary to create national level IW-Defense and IW Offense capability. As brought out above there is a global awakening and concern about malicious code and network penetration attacks and the national level Information Assurance Programs are being conceived and launched by USA, Australia, China and many European countries to safe guard their NIIs. The areas addressed under such assurance programs and the facilities being created are presented in figure 4.16. The global IT and Communication industry is supporting these initiatives and considerable know-how, technology and industry support is available in this area.

The development of EMP and RF energy weapons is localized to few nations viz. USA, Russia, France, UK, Israel, Ukraine, China etc. These weapons are also called "Weapons of Mass Electrical Destruction" due to their potential to disable or damage any solid state electronic device embedded in computers and communication systems. These information warfare weapons have emerged as a serious threat to the National Security and have the

deterrence potential near equivalent to nuclear weapons as signified by the quotes in the figure 5.20 [80,81].

QUOTED BY	STATEMENT
William J Clinton US President 11115 National Security Strategy	"The threat to our military and commercial information systems poses a significant risk to national security and must be addressed"
General John M Shalikashvili Chairman, JCOS Memo. IW Status	"Information in all its forms, information protection, and the increasingly prominent position of information in the attack have become central features in determining the outcome of modern and future conflicts."
President George W. Bush IOWA speech 8 th Jan, 2001	"Our United States and one allias ought to develop the capacity to address the true threats of the 21 st century. The true threats are biological and informational warfare".
Secretary of State, USA, Condoleeza Rice, Mar 22, 2001	"The danger posed by international hack attacks against critical US networks in some ways comparable to the threat Soviet nuclear warheads posed during the cold war".
New MAX.com 26 th Jan, 2002	"In 1999-2001, the PLA was engaged in developing a "shell-less gun" (electromagnetic gun, or EMG). Present efforts are concentrated on developing an anti-tank EMG and an anti-aircraft EMG".
NEWSMAX.com 26 th Jan 2002	"In Oct 2001, Chinese executives from Rosoboronexport made presentations at Lankagwi Int. Maritime & Aerospace 2001 exhibition in Malaysia about Ranets E (a mobile RF defence system against high-precision weapons) and Rosa-E(system designed to break enemy radar systems and ground based military installations)"
Office of the Director Defence Research & Engineering, USA, Memo Jun 28, 2002.	HPC Challenge Project Sr. No. 1 FY 2003 "Directed High Power RF Energy: foundation of Next Generation Air Force Weapons - Air Force Research Laboratory - Keith Cartwright".
Figure: 5.20: National Security Threat and Deterrence Potential of IW Weapons	

The developments in the area of EMP and RF energy weapons are shrouded in secrecy and confined to defence establishments. Very limited open source literature is available except initial investigative research emanating from nuclear EMP tests in 60s & 70's. The figure 4.7 shows that very high value IW capability programs involving military are underway across the globe. Also considering the controversies regarding use of nuclear weapons, most countries in the future will prepare deterrence posture around EMP and RF energy weapons and keep hard kill nuclear weapons as a last option.

I had initially proposed to concentrate my Ph.D research work on the development of National Information Assurance Framework. However in May 02, my supervisor, Dr. Mukal Sinha during a review of the thesis came to the conclusion that development of EMP and RF weapons is a national necessity and there is a need to undertake preparatory work which can be used as a foundation by defense establishments of the country to commence an IW program with national security dimensions. Therefore for the purpose of Ph.D. thesis, I have progressed with the work pertaining to development of EMP and RF energy weapons. In this thesis I have proposed a comprehensive IW capability for India to be built around EMP and RF energy weapons. This work has been documented under the following sub-heads and presented in chapters 6 to 10 of the thesis.

- Effect and Vulnerabilities of EM Energy
- Technology Assessment for Development EM Weapons
- Development of EM weapons
- Packaging, Induction and Deployment of EM Weapons
- Research Needs for Development of EM Weapons.

5.22 Conclusion

- In chapter 4, it had emerged that the military modernization and growing interest in the Revolution in Military Affairs has increasingly attracted international attention. The concept of Information Warfare has emerged as a subject of global interest. The intense discussions and debates within defense community suggest harnessing the political will to devote substantial resources to developing IW doctrines and capabilities to leverage the information revolution. The corresponding IW weapons can range from EMP & RF energy weapons to malicious code, logic bombs and network penetration tools. United States, Russia and China rival each other in analytical work in IW. The concepts and capabilities of IW have seemingly captivated the imagination of futurologists and military planners alike.
- The IW threats exist in three categories viz. national security threats, shared threat to civil and military establishments and local threats affecting social, political economic and military interests.
- In this chapter we have seen that dependency upon resources or infrastructures produce vulnerabilities when these resources are denied or destroyed. Modern industrialized nations including India heavily depend upon their fundamental computing and communication infrastructures, which are vitally important to the smooth operation of our political systems, finance sectors, government bureaucracies, manufacturing industries, road, rail, sea and air transport, and military systems. The computing and communication technologies comprise the foundation of these infrastructures and they share a common attribute, in that they are built with modern high-density semiconductor components.
- We have also seen that this fundamental dependency upon the modern semiconductor devices produces a global and pervasive vulnerability to attack by weapons, which are specially designed to damage or destroy semiconductor components. These EMP and RF energy weapons are now both technically feasible and relatively economical to build, in comparison with established weapons of mass

destruction such as the nuclear weapons. A wide range of existing targeting and delivery techniques can be employed in using such weapons.

- It emerged that the technology of EMP and high power RF in a directed energy role has unprecedented potential for military use, in both offensive and defensive roles. There are many possible applications for this type of technology, from minesweeping to anti-aircraft artillery to unmanned combat aerial vehicles combined with precision attack and air combat capability, which can pose challenge to a most powerful military force. In this chapter we have also examined military tactics and strategy to change with these systems. The aim is to evolve an integrated IW-Defence and IW-Offence operations, to build an IW capability with national security dimension and, a deterrent posture hitherto possible only through nuclear weapons.
- As of now the development of EMP and RF energy weapons is localized to few nations viz. USA, Russia, France, UK, Israel, Ukraine, China etc. These weapons are also called "Weapons of Mass Electrical Destruction" due to their potential to disable or damage any solid state electronic device embedded in computers and communication systems. These information warfare weapons have emerged as a serious threat to India's National Security and have the deterrence potential near equivalent to nuclear weapons.
- The developments in the area of EMP and RF energy weapons are shrouded in secrecy and confined to defence establishments. Very limited open source literature is available except initial investigative research emanating from nuclear EMP tests in 60s & 70's. Very high value IW capability programs involving military are underway across the globe. Also considering the controversies regarding use of nuclear weapons, most countries in the future will prepare deterrence posture around EMP and RF energy weapons and keep hard kill nuclear weapons as a last option.
- We have recognized that traditionally as a part of modernization programs India's (very limited) focus on information warfare had been confined to the actions between the opposite sides for the power of possession, control and utilization of information by means of information technology and equipment. However as a result of the development of information networking technology and the continuous research on information warfare theory and practice, information warfare has developed from conducting soft kill types of operations, such as "electronic operations" and "key point sabotage operations" to conducting "paralysis types of operations", such as "computer virus", "directivity beam weapons", and "electromagnetic pulse weapons". Therefore for the future, information warfare is one of the best means of warfare for India to gain regional parity, to achieve the goals of "least damage", "highest efficiency", "rapidest attack" and "fastest decisive victory", and of "winning without fighting and possession and exploitation of resources". India also needs to achieve multiple strategic goals through its IW capability, including political, economic, psychological, and military goals.
- Given India's situation in politics, economy, social psychology, foreign affairs, geography, and military needs, the information and information infrastructure has great impact on the security of the entire country and is vulnerable to information warfare threats. The efforts need to be focused at strategic level on information technology, related infrastructure, tactics and strategic thinking. The focus has to be on winning a "limited war under the condition of high technology". Strategically, the

information warfare capability buildup needs to be based on the policy of "limited targets" and "key point highlighting", "development of advanced technology", "establishment of superior technology conditions", and the "foundation of information warfare technology". Tactically, the research on tactics of networking, intelligence collection and space surveillance systems in armed forces, establishing theater and field transparent command and control capability needs to be undertaken. In addition to the Internet offensive and defensive techniques, organizing a new "Internet force", development of "computer virus", "logic bomb", and "electromagnetic pulse weapons" needs to be planned. The degree of IW threats, threat spectrum for high value targets involving national security, economy and social structures needs to be examined and identified as suggested in this chapter.

- Development of EMP and RF weapons is a national necessity and there is a need to undertake preparatory work, which can be used as a foundation by defense establishments of the country to commence an IW program with national security dimensions. Therefore for the purpose of Ph.D. thesis, I have progressed with the work pertaining to development of EMP and RF energy weapons. In this thesis I have proposed a comprehensive IW capability for India to be built around EMP and RF energy weapons. This work has been documented under the following sub-heads and presented in chapters 6 to 10 of the thesis.
 - Effect and Vulnerabilities of EM Energy
 - Technology Assessment for Development EM Weapons
 - Development of EM weapons
 - Packaging, Induction and Deployment of EM Weapons
 - Research Needs for Development of EM Weapons

PART- III
EMP AND HPM ENERGY WEAPONS - A NEW
INFORMATION AGE DETERNCE

CHAPTER 6: EFFECTS AND VULNERABILITIES OF EM ENERGY

CHAPTER 7: TECHNOLOGY ASSESSMENT FOR DEVELOPMENT OF
EM WEAPONS

CHAPTER 6

EFFECTS AND VULNERABILITIES OF EM ENERGY

6.1 Introduction

In chapter 5 we have highlighted that high-density semiconductor devices form the building blocks of the modern information and communication infrastructure. It also emerged that Electromagnetic Pulse (EMP) and directed RF energy has devastating effect on these electrical and electronic devices. The EMP and high power RF energy are therefore being recognized for potential use as weapons of "Mass Electrical Destruction" (WMED) to cause disability, denial, damage, or destruction of NII. This chapter examines characteristics of EMP and RF energy, historical background of its origin, effects, and vulnerabilities. It describes mechanisms for coupling this energy into a target electronic system for inflicting damage, susceptibilities and the extant and type of damage it can cause at component, device, system and service level. It also categorizes energy in different frequency bands to evolve a variety of weapons.

It signifies that with the advent of broadband, Internet and wireless technologies, there would be more competing requirements for usage of Radio Frequency (RF) Spectrum. At the same time the military planners are vigorously moving ahead for development of technologies for control of RF spectrum, and the EM weapons are the latest addition to this effort. It describes how supremacy in EMP and RF energy weapons can enable a nation to dominate in the emerging IW scenario at national and global level.

6.2 EMP, RF and Microwave Energy

Electromagnetic Pulse or EMP device is a generic term applied to any device, nuclear or conventional, which is capable of generating a very intense but short electromagnetic field transient. For applications in weapons, this transient must be sufficiently intense to produce electromagnetic power densities that are lethal to electronic and electrical equipment. Electromagnetic (EM) weapons are electromagnetic devices specifically designed as weapons. The terms "conventional EMP weapon" and "High Power Microwave or HPM weapon" have been used interchangeably in the literature. This document will distinguish between "microwave band" and "low frequency weapons". The term "Electromagnetic weapons" or "E-bomb" have been used to describe both microwave and "low-frequency non-nuclear weapons". The other terms used are RF ammunition, EMP bomb, T-bomb [39].

6.3 Historical Background

USA discovered the effects of RF energy on electronic components with the advent of the Electromagnetic Pulse phenomenon associated with the detonation of a nuclear weapon. On July 7, 1962, after the U.S. tested a hydrogen bomb in the skies above a remote Pacific island, scientists felt effects as far away as the Hawaiian Islands, over 1000 miles distant. When the blast went off, 300 street lamps suddenly extinguished, many burglar alarms sounded and a large number of power supply systems failed when their safety switches tripped. Mr. C. L. Longmire developed a theoretical analysis to explain what happened. It

emerged that nuclear blast releases a pulse of energy across the low radio frequency bands (below 1 GHz) that produces transient voltage in electrical equipment, which causes the electrical circuits to overload. Nuclear physicist Edward Teller predicted in 1977, "If an eight-megaton hydrogen bomb were exploded at 500 kilometers above the middle of the United States, at least half of the country's computers and electronic equipment would stop working" [65,183,188].

Both the United States and the Soviet Union devoted considerable effort into categorizing the effects of EMP on various systems [70]. In the process, scientists developed high power radio frequency generators to simulate EMP so that they could test their systems without exploding a nuclear bomb. As time went by, investigations proceeded into the higher microwave frequencies. The former Soviet Union was the first to begin research on applying high power RF / microwave technology to a weapon. In 1979, they achieved a breakthrough in manufacturing an experimental gigawatt-level microwave emission triode, a device critical to controlling the extremely high power levels needed in microwave beam technology. In 1983, they did it again by producing a 100-megawatt millimeter wave band transmitting tube. This was the first tube manufactured that could produce enough beam level power for microwave weapons experiments. Before their collapse, the Soviet Union had a large and diverse RF weapons program and remnants of this work continue today within former Soviet Union countries [151].

The United States did not really begin microwave weapons research in earnest until the early eighties. Since then, scientists working with the High Power Microwave Division of the Air Force Research Laboratory (AFRL) at Kirt Land have made tremendous technical advances in plasma physics, energy storage and fast switching devices, and other technologies for high power RF / microwave weapons development. They have also stepped up efforts to characterize the effects of RF energy in U.S. and foreign systems in order to improve understanding of both target vulnerabilities and protection measures. The technology has now matured to the point that several U.S. operational commands are pursuing weapon demonstration programs using high power microwave devices. The USAF Scientific Advisory Board has predicted that high power microwave weapons would be a well-established technology by the year 2015.

6.4 Effects of Nuclear Detonations: Radiating Fields

The detonation of a nuclear device results in generation of a number of radiating fields, which have varying effects on living matter, structures, electrical and electronic equipment. The characteristics of these fields with respect to time are shown in the Figures 6.1 and 6.2 and the energy produced has distribution shown in Figure 6.3 [44, 70].

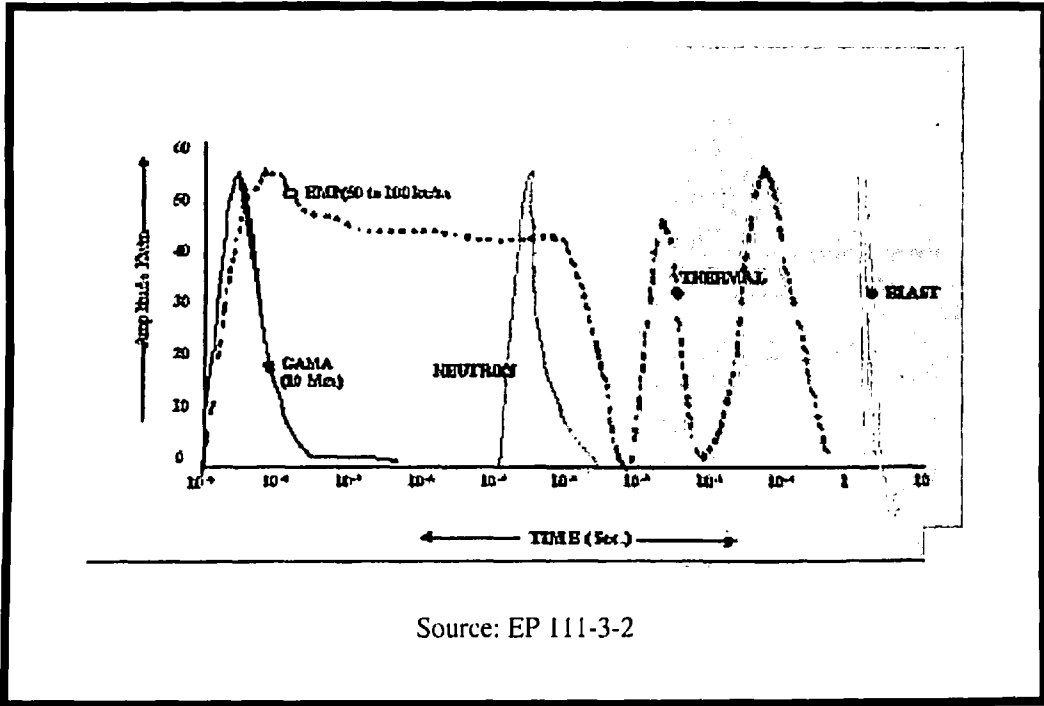
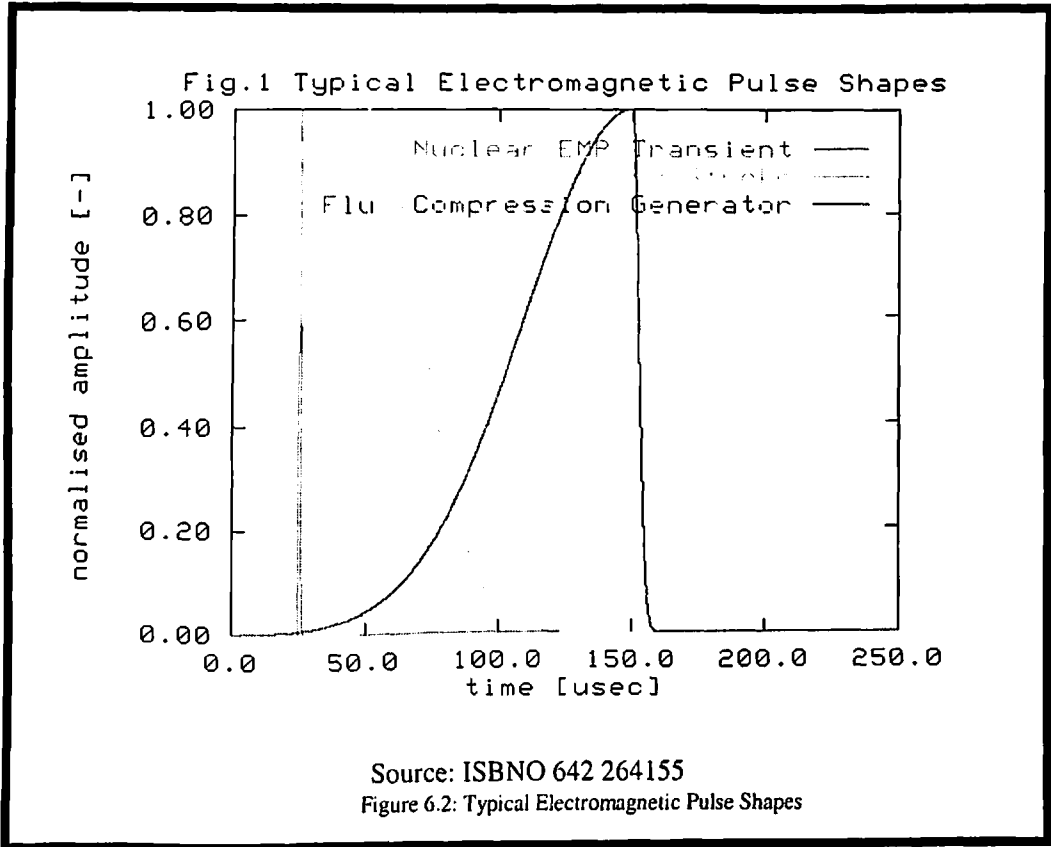


Figure 6.1: Nuclear Burst Effects Relative to Time



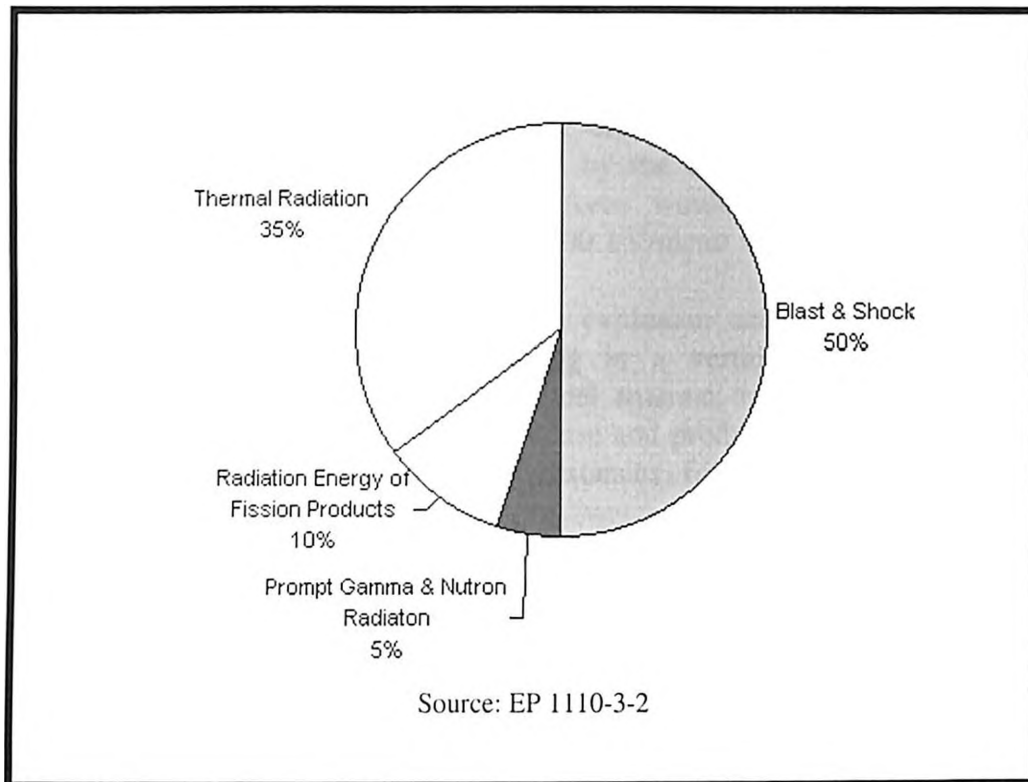


Figure: 6.3 Energy Spectrum from Nuclear Detonation

6.5 Characteristics of Radiating Fields [NUEFSHIP]

6.5.1 Gamma Rays

The gamma rays are of high quantum energy of the order of 50 MeV, travel at the velocity of light and last for several nano-seconds. The gamma ray radiation intensity is so high that it would require shield thickness of 3 mm of lead, 55 mm of steel or 25 mm of aluminum to reduce the intensity by a factor of 50.

6.5.2 Neutron Pulse

The neutron pulse follows the gamma rays and last for few nanoseconds. The neutrons are of similar energy to that of gamma's and being particles, travel somewhat more slowly than the velocity of light. The neutrons require a paraffin or water shield thickness of 20 cm to reduce the flux density by a factor of 50.

6.5.3 Electro Magnetic Pulse (EMP)

Some of the nuclear (and thermal) radiation in the weapon vicinity produces intense ionization, so that high-speed electrons are emitted. This is equivalent to a very large outwardly directed negative electric current with an initial time of the order of 50 nano seconds and gives rise to the following phenomenon, depending upon whether the detonation has taken place in outer space, or on surface of the earth or underwater.

- **Explosion in Outer Space:** If the explosion occurs in the outer space, no direct electromagnetic radiation would be produced, since the current would be spherically symmetrical. However some of the emitted electrons from an exo-atmospheric nuclear explosion would be trapped by the earth's magnetic field. Their spiral motion around the magnetic lines of force' would produce a strong electromagnetic radiation of about 50 kV/meter to 500 kV/meter up to 50,000 miles from ground zero.
- **Explosion near the Surface:** If the explosion occurs near the surface, it would introduce sufficient energy resulting in a vertically polarized electromagnetic radiation. This would act as a vertical antenna transmitting at ground zero. This electromagnetic radiation is very intense and produces field strengths of tens of kilo volts per meter at considerable distances from the explosion. This is called electromagnetic pulse (EMP).
- **Underwater Explosion:** An under water explosion, provided it does not vent through the surface, does not produce any nuclear or electromagnetic radiation at ranges of tactical interest. If it does vent, radiation would occur from the exposed fireball at lower level. The EMP spans the period of gamma and neutron pulse and covers frequency spectrum up to several hundred MHz.

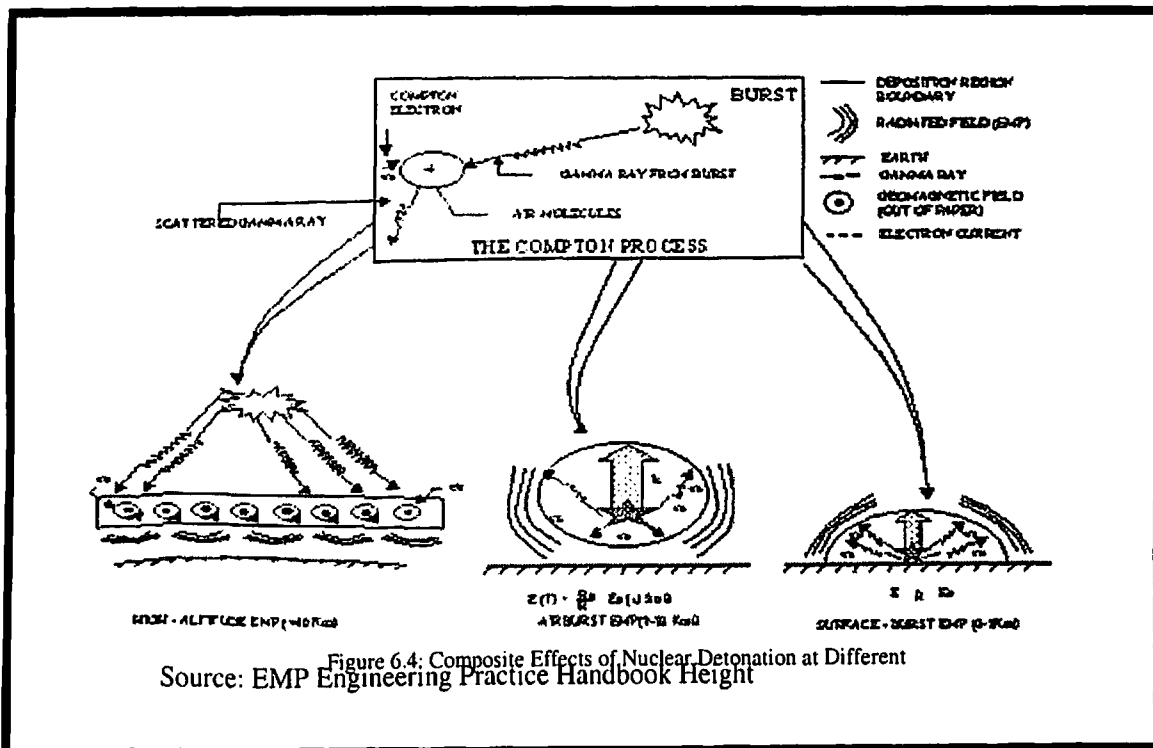
6.5.4 Thermal Pulse

A thermal pulse follows the EMP and lasts for a few seconds. This can generate very high temperature causing differential expansion in structure and overheating.

6.5.5 Blast

It follows the thermal pulse and lasts for several seconds including the normal pressure period.

The composite effect of nuclear burst at different heights is illustrated in Figures 6.4 and 6.5.



No.	EMP Type	Peak Amplitude	Time Frame
1.	HEMP	50 Kv /m	Few n Sec. to 200 n Sec.
2.	Surface Burst (a) Surface Region (b) Radiated Region	Mv/m 10 Kv /m 10 Kv/m	Few n Sec. to 1 u Sec 1 u Sec to 0.1 Sec. 1u Sec. to 100 u Sec.
3.	Air Burst (a) Source Region (b) Radiated Region	Same as Surface 300 v/m at 5 km (Dependent on HOB)	10 n Sec to 100 n. Sec
4.	SGEM	100 Kv/m	few n Sec to 100 n Sec.
5.	Mtn. - EMP	30 v/m	0.1 Sec to 100 Sec.
Source: EMP Engineering Practice Handbook Figure 6.5: EMP waveform Summary			

6.6 Nuclear-EMP Effects on Electronic Devices (Effects of Neutrons)

The electronic components and devices such as diodes, transistors, gate arrays and Integrated Circuits (ICs) are based on pure silicon slice cut from carefully grown single crystals. Their electrical properties depend on the regularity and uniformity of the basic silicon crystal lattice. If the incidence neutron collides with a lattice atom, this is knocked out of place and institutes a collision cascade within which some hundreds of atoms are involved. As a result, a small region is formed where the lattice damage is highly concentrated. The initial total damage is proportional to the neutron influence, but there is a subsequent annealing process during which there is some degree of recovery. Apart from this, however, the damage is permanent (and cumulative if there is more than one nuclear event). It makes no difference whether the device is in working equipment or in a spare unenergised unit in the storeroom except that the annealing process takes longer in the latter case. The mechanism of EMP / RF energy coupling with electronics and communication equipment in a civil or military facility is illustrated in figure 6.6. The practical effects of lattice damage are as follows [78].

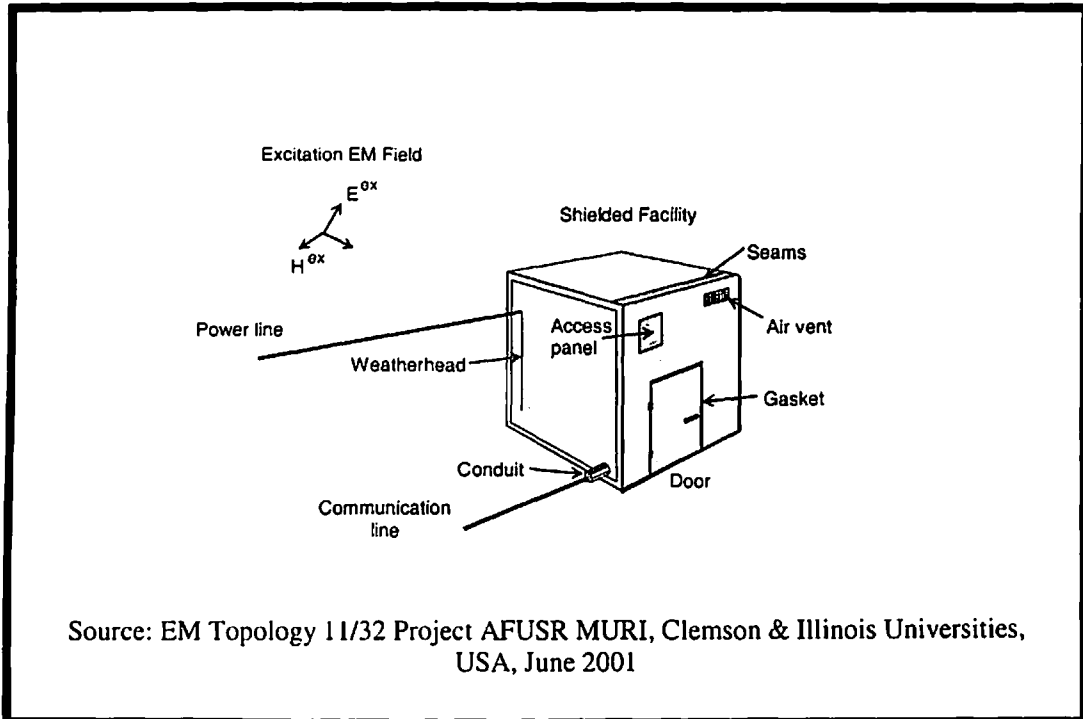


Figure 6.6: Excitation of Electronics by EM field in a Shielded Facility

6.6.1 Bipolar Transistors

Reduction in current gain and increase in collector emitter saturation voltage. It is not difficult to design low power circuits, which can tolerate these effects, but the design of high voltage high power transistor is difficult.

6.6.2 Diodes

In case of diodes, there is a permanent increase in the forward voltage drop, which requires the provision of additional heat sinking for high power devices.

6.6.3 Thyristors

These require higher gate triggering power after neutron irradiation and also suffer from an increase in forward voltage drop and hence increased heat dissipation.

6.6.4 Photo Diodes & Photo Transistors

These are highly sensitive to damage by neutron radiation and latter may suffer a loss in optical sensitivity upto 90%.

6.6.5 Light Emitting Diodes (LED's)

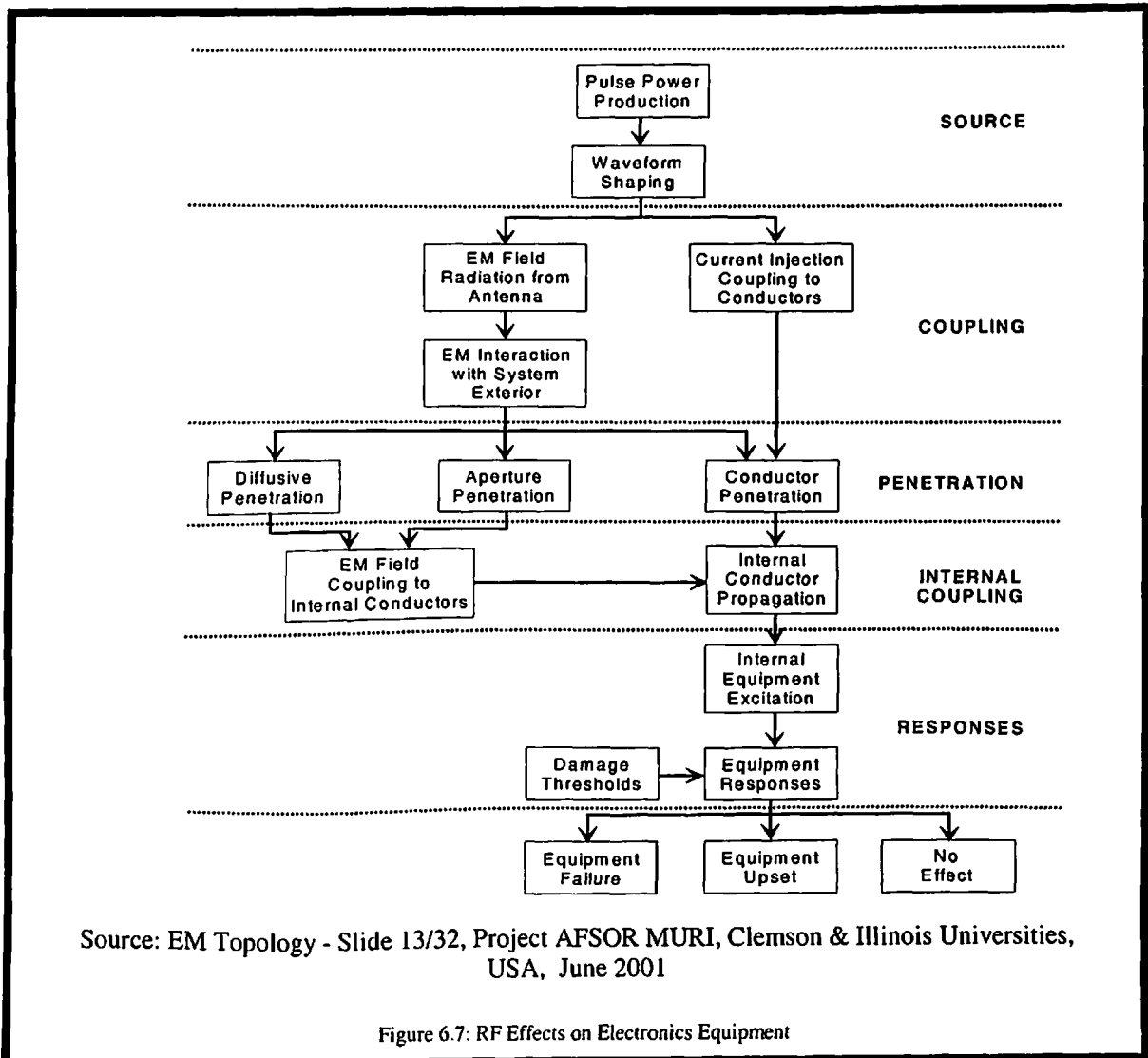
These can suffer degradation in optical output by 50 to 20 percent. The optical isolators consisting of an LED and a phototransistor can therefore suffer a severe reduction in current transfer ratio, which has to be allowed for in circuit design.

6.6.6 Integrated Circuits and Gate Array Devices

MOS, integrated circuits (CMOS, PMOS, NMOS etc) are virtually immune to neutron radiation damage at levels of tactical interest, as are most bipolar digital ICs. However, the bipolar linear ICs such as operational amplifiers are affected in various ways, which must be taken into account during the equipment design.

6.7 Effects of Microwave Energy on Electronics, Materials and Personnel

High power RF / microwave energy can affect anything that responds to electromagnetically induced voltages and currents, which includes electronics, materials and personnel. Two mechanisms described below are at work within objects caught in a high power microwave beam, molecular heating, and electrical stimulation. The schematic representation of a facility housing electronics and communication equipment, when attacked by EM energy is illustrated in the figure 6.7 [78]



6.7.1 Molecular Heating

Molecular heating occurs when powerful sinusoidal waves, produced by narrow band microwave devices cause the molecules of a material to rub together at the frequency of the microwave field. The effect is same as that found in a standard microwave oven. Materials containing liquid or carbon molecules are quite susceptible to this kind of radiation. The idea is that an extremely high power microwave signal directed at a distant target could potentially raise the temperature of fuel above its flash point, prematurely explode the warhead, heat the composite structures to point of failure, or kill the occupants outright by boiling their brains. The power required for doing this, however, is quite large and would require a significant dwell time on target.

6.7.2 Electrical Stimulation

A more efficient mechanism for attack is electrical stimulation. The power levels required to induce transient voltages and currents in electrical devices are much smaller than for molecular heating. This allows for much longer engagement ranges and much shorter dwell times when attacking targets with electrical components. Under electrical stimulation, microwave energy, narrow or wide band, couples with any electrically conductive material in the beam to stimulate electron flow in the material, thereby producing transient currents and voltages. Electrically conductive materials in the target act like little antennae to the high power microwaves in the same way as a normal antenna picks up low power radio waves. Transient currents interfere with the normal operation of electrical components, inducing spurious signals that confuse the system or even damage sensitive components. At sufficiently high power levels, these currents can actually produce electrical arcing or sparks across conductors. Inadvertently leaving a metal or aluminum foil on a package placed in a common microwave oven can present evidence of this phenomenon. It is common knowledge that, sparks are always bad for electronics and could even ignite fuel vapors or explosive warheads. When a beam enters a target, high power RF radiation bounces around inside the container, creating constructive and destructive interference that produces "hot " and "cold " spots (regions of high and low electromagnetic field strengths) within small distances of one another. These hot spots can be many times stronger than the incident field, thereby exposing components situated at these nodes to even higher field strengths. The effects of RF energy on the equipment / systems have been categorised as follows:-

- **Upset:-** This is a temporary alteration of the electrical state of one or more nodes in such a way that they no longer function normally. Once the signal is removed, however, normal function returns with no permanent effects. Jamming is an example of this type of effect, where a sensor might lose lock because of interference.
- **Lockup:-** It produces the same effects as upset, but an electrical reset is required to regain functionality, even after the signal is removed. For example a computer can freeze after exposure to RF and would need to be rebooted.
- **Latch-up:-** This is an extreme form of lockup in which a node can be permanently destroyed or electrical power can be cut off to the node. A fuse blowing or transistors failing on a circuit board due to overloads from microwave radiation are two such examples.
- **Burnout:-** This is the physical destruction of a node. This can occur where the current becomes so high that conductors actually melt. This usually occurs **within**

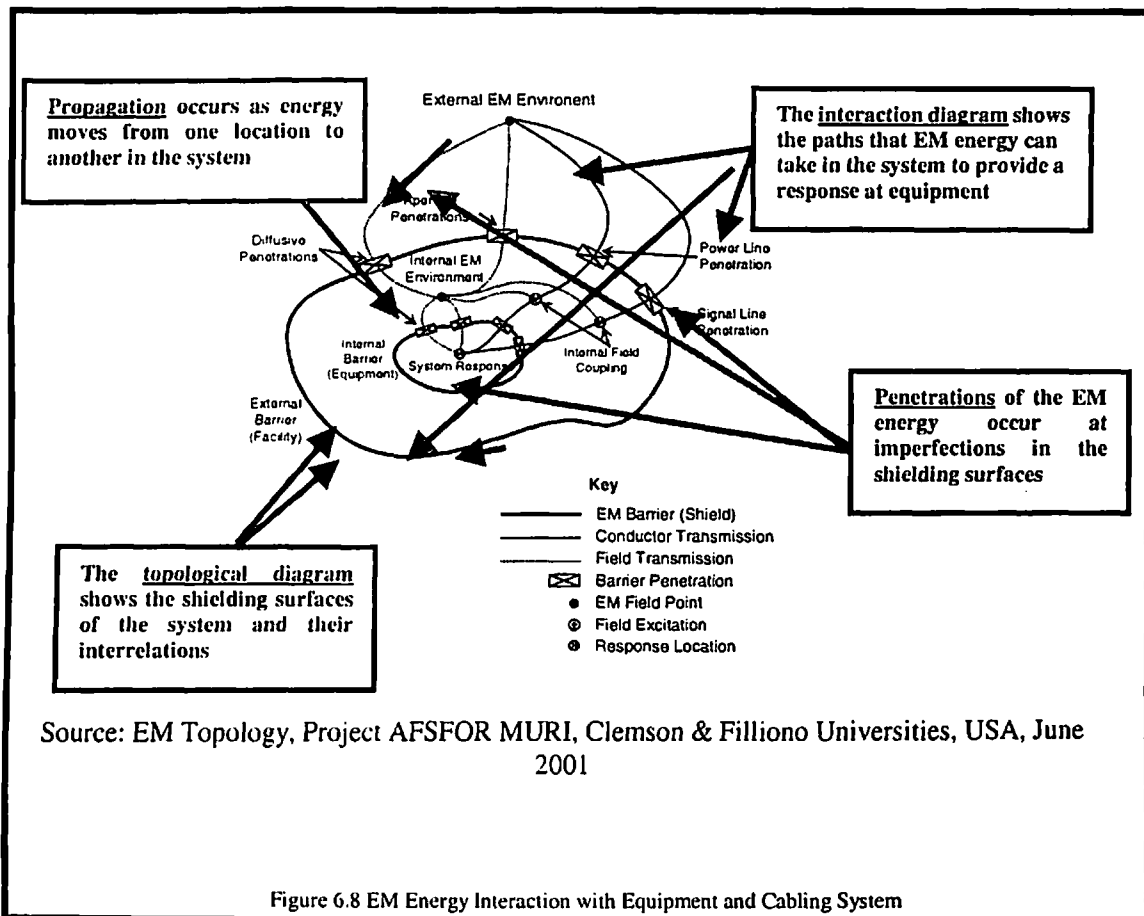
smaller wires or at junction nodes where multiple wires come together and often involve electrical arcing. The damage to household electronics caused by a lightning strike is an example of burnout

6.8 Weaponisation of Microwave Energy

Any of these mechanisms have military utility depending on the mission. In a defense role, lockup, latch-up and burnout can produce the desired effect of thwarting a precision attack by disrupting the guidance system of the weapon. Even upset can be useful in denying navigation signals to a precision weapon to reduce its accuracy. Against reusable platforms like aircraft's, UAVs, the mechanisms of latch-up or burnout are more desirable because they inflict actual damage on the target, which must be repaired if the aircraft or UAVs ever makes it back to home base. This kind of damage can be especially difficult to isolate, because microwave energy can affect every internal component of the system. Lengthy troubleshooting procedures are likely, which can keep the affected systems out of service longer. Finally, significant system wide damage will put a strain on the logistical capability to bring in sufficient spare parts to keep the systems in working order. Therefore weaponisation of EM energy can give high military pay-offs interms of protection of NII against enemy attacks and in an offensive role to inflict damage on the adversary. The process of transforming the EM energy into weapons is described in the succeeding paragraphs [88].

6.8.1 Susceptibility of Equipment and Systems

The rate and degree to which a target NII systems can be affected by microwave energy depends upon numerous factors of both the beam itself (range, frequency, burst rate, pulse width, etc) and the design of the target NII system (shielding, filters, shunts, etc). These factors are extremely complicated, and the detailed discussion is not included. However, a basic understanding of what makes targets vulnerable to high power RF radiation is presented in these paragraphs. In order for and RF signal to affect the internal working of the target electronic or electrical systems, it must first penetrate the external case. A seamless external case, made entirely of conducting metal, with no sensors, apertures or connections to the outside world, would act as a perfect "Faraday cage "and totally shield any internal components from external signals. However, most of the NII components i.e. information systems, data networks and communication systems or even those in armed forces viz. sensors, flight control surfaces and other apertures allow entry of RF radiation. RF radiation uses two mechanisms to enter a target, called front-door coupling and back-door coupling, described below. The sequence and mechanism of coupling of the energy illustrated in figure 6.8. Another important factor that determines how RF radiation will affect a target is the incident power level at the target surface. The higher the power, the more likely it will produce damage.[49,50,78]



- **Front-Door Coupling:** Front-door coupling occurs when RF energy enters the system through a sensor or antenna designed to receive this type of radiation. The radiation may be in-band or out-of-band with respect to the receiving system. In-band refers to radiation that is of the same frequency range as the antenna, meaning that the antenna actually amplifies the signal and passes the energy directly through to the internal components. In-band front-door coupling is the most efficient and destructive coupling method. Out-of-band refers to radiation outside the designed frequency range of the antenna or sensor. The system will usually attempt to filter this type of radiation, although the power levels associated with high power RF beams might still overwhelm its circuits. Narrow-band high power microwave devices are most suited to front-door coupling because all their energy can be focused into the narrow frequency range of the sensor or antenna. Ultra Wide Band microwave devices are not as effective with front-door coupling because most of their energy is contained in the out-of-band frequencies, which systems are designed to filter.
- **Back-Door Coupling:** Back-door coupling encompasses every other way the RF energy can penetrate a system. RF energy may enter through cracks, seams, seals, conduits, cable runs, apertures, solar cells, optical sensors, etc. Ultra-wideband (UWB) radiation is particularly effective at back-door coupling because of the wide range of wavelengths involved, from 5 mm (gigahertz frequencies) to 3 meters (megahertz frequencies), which allows them to penetrate from multiple points. Regardless of the method, once in, high power microwave energy can wreak havoc on electronic components, especially integrated circuits and other microelectronics found in sophisticated weapon systems. Semiconductor design based on Metal Oxide

Semiconductor technology, on which most of critical systems depend, is extremely vulnerable to electromagnetic pulses. Furthermore, as electronics become more densely packed, more energy efficient and operate at higher speeds, they will become even more susceptible to high power RF / microwave radiation.

6.9 Categorization and Frequency Ranges for EM Weapons

6.9.1 Directed Energy Weapons

Microwave weapons fall into a category of directed energy weapons as illustrated in the Figure 6.9. The Microwave weapons are commonly referred to as high power Radio Frequency (RF) devices. Although the RF portion of the electromagnetic spectrum extends from below 3 kilohertz (KHz) to above 300 Gigahertz (GHz) the high power weapon research is generally limited from between 500 MHz to 35 GHz. This is because, moisture in the atmosphere has very little affect on a signal in this frequency range and that is why most communication, navigation and radar devices operate there. [59,69]

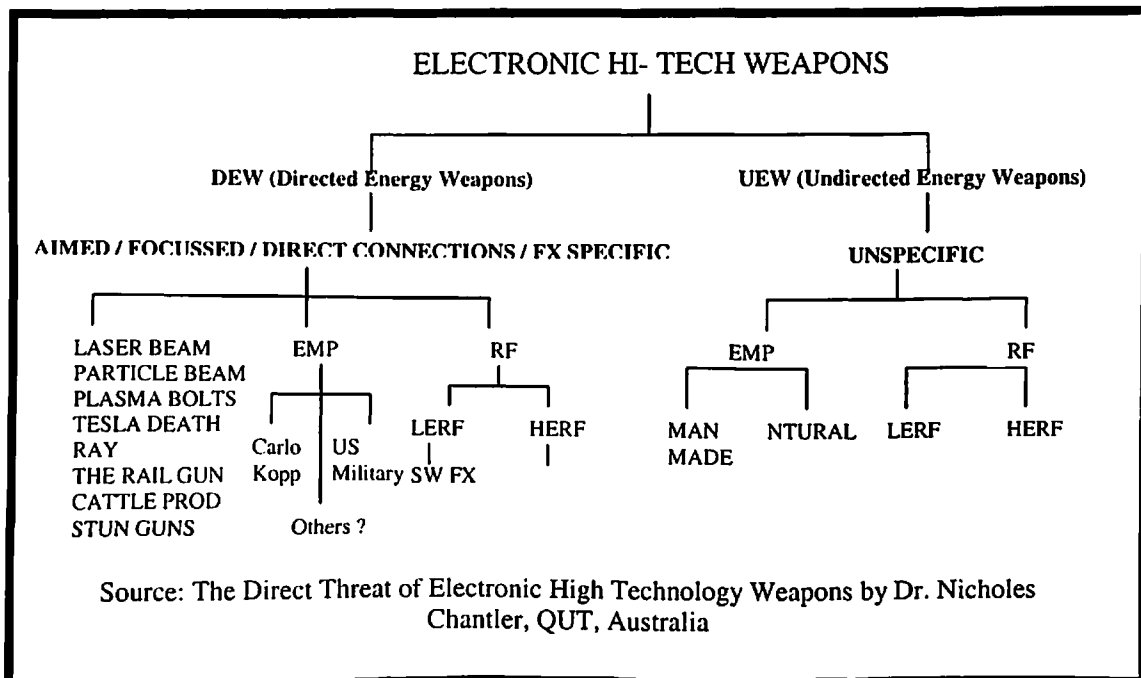


Figure 6.9: Categorization of Weapons

6.9.2 Taxonomy of Electromagnetic Devices

The internationally recognized taxonomy of devices used in directed energy weapons and their frequency ranges are illustrated in the Figure 6.10 and figure 6.11. The United States has conducted extensive research over the years to understand and minimize the effects of electro-magnetic pulse (EMP) from nuclear detonations on the NII [70,142,143]. However, EMP protective measures are not as effective against high power microwave (HPM) and ultra-wideband (UWB) waveforms. This is because EMP frequencies fall mostly below 5 GHz, with pulse widths in the range of 50 nanoseconds to 5 microsecond. The higher frequencies and shorter pulse times of HPM and UWB are

generally inside the response time of most limiters, so RF energy passes relatively unattenuated into the system, thereby causing the disability or damage. [142]

Electromagnetic Devices						
Gamma Rays • Particle Beam Generator	X-Ray • -X-Ray Weapon	Ultraviolet • Lasers Tactical Pulsed Chemical	Infrared • Lasers Tactical Low Energy	Microwave • High Powered Microwave • Maser • Thermal Gun	Radio • EMI • Non -Nuclear EMP • Radio Frequency Weapons	Electrical • Baton • Sticky Shocker • Stun Gun & belt
Source: DoD, USA, Dept. of Non- Lethal Weapons, March 2001. Figure 6.10: Electromagnetic Devices in Different Frequency Bands						

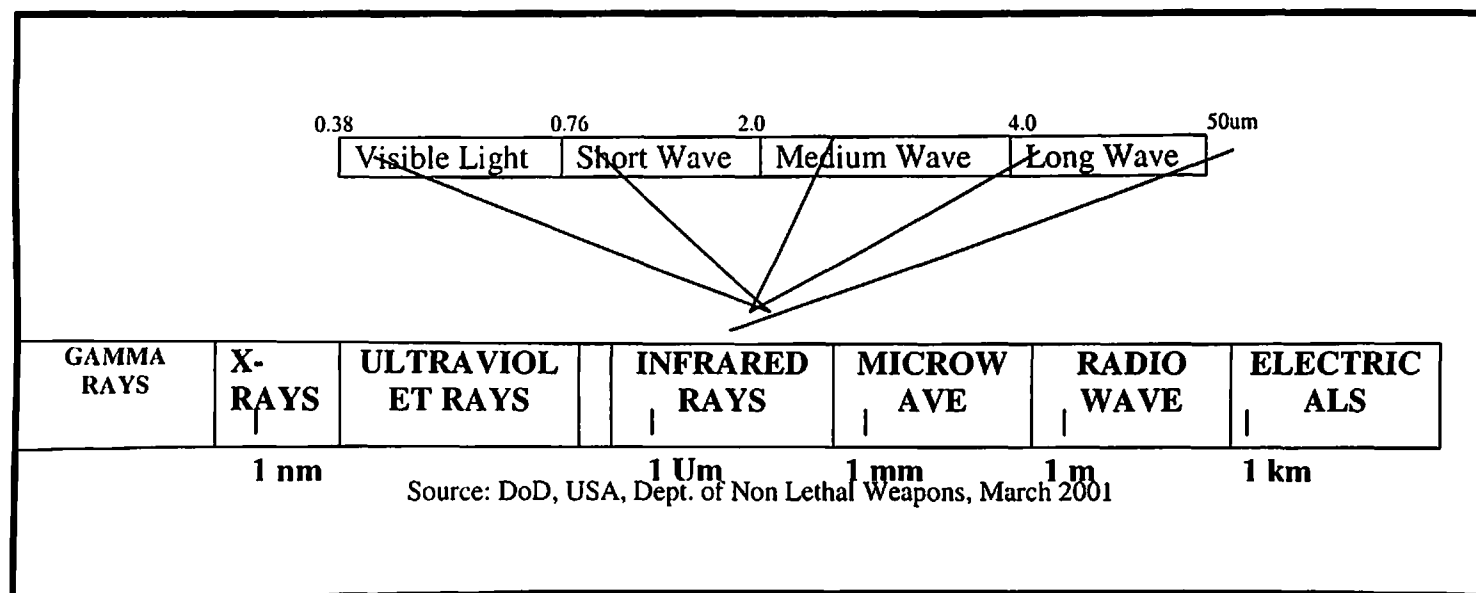


Figure 6.11: Wave Length vis-a-vis Ranges of Energy

6.9.3 Device Categorization

- Ultra Wideband (UWB) Microwave Devices:** The literature categorizes RF weapons according to the type of beams they produce, either wideband or narrowband, and often refers to the whole group under the heading of microwave weapons. Wideband devices generally operate in the lower frequency ranges (50 MHz to 5 GHz) and produce very short pulses (5 to 500 nanoseconds) with wide bandwidths (50% to 500% of the center frequency). These types of devices are called Ultra-Wideband (UWB) weapons.
- Narrowband Devices (NWB) or High Power Microwave (HPM) Devices:** Narrowband devices generate longer pulses (5 microsecond) and produce RF radiation at a single frequency (between 5-35 GHz), with a very small bandwidth (nominally 5%of the frequency). Narrowband devices are also called High Power

Microwave (HPM) weapons, although HPM is sometimes used to describe all microwave weapon technology.

- **Characteristic Parameters:** The parameters used to characterize these systems include frequency, energy, average power, peak power, fluence, bandwidth, pulse width, dwell time and numerous others.
- **Pulsed Beams and Multishots:** Microwave designs can produce continuous or pulsed beams from single-shot or multi-shot systems. Research shows that for an integrated air defense, the best weapons are high frequency, wide bandwidth, pulsed power, multi-shot systems with narrow beam widths to better focus their energy on a distant target. A weapon's range, lethality and rapidity of fire determine how it is to be employed.
- **Deploy-ability:-** The range, lethality and rapidity of fire determine how these weapons are to be deployed.

6.10 Propagation of RF Energy as a Weapon

A fundamental principle of RF energy is that as the distance from the source increases, the energy reaching the target decreases. Normal omni-directional antennae, similar to those used in radio and television, produce steady-state electromagnetic fields that attenuate energy in all directions at a rate proportional to the inverse of the square of the distance from the source ($1/D^2$). Such attenuation is too restrictive for beam to reach large distances. Therefore antenna designs can be made to produce special electromagnetic fields that allow energy to propagate in some directions with less attenuation than in steady-state fields. These fields, called transient-state fields, allow energy to propagate in a beam at a rate of $1/D^2$ where $0 < a < 2$. Transient-state fields, therefore, provide microwave sources with the ability to direct the beam while simultaneously capitalizing on the lower attenuation to extend the range [88]

6.11 Potential of EM Weapons to Damage NII

The EM weapons can cause extensive disability, damage or destruction to the civil as well as military electronics and electrical equipments particularly computers and radio or radar receivers, which constitute the basic building blocks of the NII of the country. Subject to the electromagnetic hardness of the electronics, a measure of the equipment's resilience to this effect, and the intensity of the field produced by the weapon, the equipment can be irreversibly damaged or electrically destroyed. The damage inflicted is not unlike that experienced through exposure to close proximity lightning strikes, and may require complete replacement of the equipment, or at least substantial portions thereof. Commercial electronic equipment is particularly vulnerable as it is largely built up of high-density Metal Oxide Semiconductor (MOS) devices, which are very sensitive to exposure to high voltage transients. What is significant about MOS devices is that very little energy is required to permanently disable or destroy them. Any voltage typically in excess of tens of volts can produce an effect termed as gate breakdown, which effectively destroys the device. Even if the pulse is not powerful enough to produce thermal damage, the power supply in the equipment will readily supply enough energy to complete the destructive process. Wounded devices may still function, but their reliability will be seriously impaired. Shielding electronics by equipment chassis provides only limited protection, as

cables running in and out of the equipment will behave very much like antennae, in effect guiding the high voltage transients into the equipment. Therefore following emerges [44, 88]:-

- Computers used in data processing systems, communications systems, displays, industrial control applications, including road and rail signaling, and those embedded in military equipment, such as signal processors, electronic flight controls and digital engine control systems, are all potentially vulnerable to the EM weapons.
- Telecommunications equipment can be highly vulnerable due to the presence of lengthy copper cables between devices. Receivers of all varieties are particularly sensitive to EMP, as the highly sensitive miniature high frequency transistors and diodes in such equipment are easily destroyed by exposure to high voltage electrical transients. Therefore, radar and electronic warfare equipment, satellite, microwave, UHF, VHF, H.F. and low band communications equipment and television equipment are all potentially vulnerable to the EM weapons.

It, therefore, emerges that military systems as well as all other components of the National Information Infrastructure, particularly the ground segments of satellite systems, telephone exchanges, RF networks, mobile cell phone installations, troposcatter links etc. are extremely vulnerable to EM weapons.

6.12 Evaluation of Electromagnetic -Pulse as Weapon of Choice

EMP is a sudden, high-intensity burst of broad-band electromagnetic radiation. The range of electromagnetic frequencies present depends on the source of the EMP. The high-altitude airburst of a nuclear weapon produces an intense EMP, which, because of the relatively long duration of the explosion, contains strong low-frequency components (below 500 MHz). Conventional EMP devices built with explosively driven, high-power microwave technology produce a less intense, very short (nanoseconds) burst composed primarily of microwave frequencies (500 MHz - 500 GHz). The range of the EMP effect depends on the strength of the source, as the initial electromagnetic shock wave propagates away from its source with a continuously decreasing intensity [4,5].

The gamma radiation produced by a fission or fusion bomb interacts with the atmosphere, creating a large region of positive and negative charges by stripping electrons from atmospheric gasses. The motion of these charges creates the EMP. The pulse enters all unshielded circuits within range, causing damage ranging from circuit malfunction and memory loss to overheating and melting.

Militarily useful EMP can be created by mating a compact pulsed power source (gigawatt range), an electrical energy converter, and a high-power microwave device such as the (Virtual Cathode Oscillator) or Vircator. An advantage of a conventional EMP device is that it can be triggered in a shorter amount of time, thereby putting more output energy into the higher microwave frequencies (above 500 MHz). Since modern electronics operate primarily in these microwave bands, the EMP produced by conventional devices is potentially very effective in shutting down electronics. Explosively pumped EMP devices such as the vircator have another advantage, it is possible to design them to focus their EMP in a particular direction. Even a focused

EMP effect produced by a conventional device will probably have a lethal radius measured only in hundreds to thousands of meters, depending upon the strength of the power source and atmospheric absorption, particularly at frequencies above 20 Ghz.

6.12.1 Effectiveness of EMP as a Weapon

The size of the nuclear EMP effect is related less to the yield of the bomb than to the altitude of the burst. A 500-kiloton burst at an altitude of 60 miles would create damaging EMP over an area equal to entire Indian landmass. At 300 miles, the same burst would create EMP over an area equal to the entire Asia or even more. The gamma burst from a (purely theoretical) microyield nuclear device might be used to create a more manageable EMP effect [70,144].

Electrical devices exposed to an EMP burst experience effects ranging from temporary electronic disruption at the outer edge to destructive electrical over voltages near the center. Modern semiconductor devices, particularly those based on Metal Oxide Semiconductor technology such as commercial computers, are easily damaged by these high-voltage transients. Long ground lines, such as electrical transmission wires, act as enormous antennas for the EMP burst. Power transmission and communication grids are therefore extremely vulnerable and will probably be destroyed by the burst. Any system containing semiconductor electronics, including airborne platforms, would be shut down or burned out by the burst unless it was completely protected with heavy, expensive electrical and magnetic shields, well designed electrical filters, and careful grounding. An extremely effective area weapon, the EMP produced by a nuclear airburst would produce severe damage to the National Information Infrastructure.

A more flexible form of EMP weapon system can employ either a microyield nuclear weapon (yield below two kilotons), a conventional explosively driven EMP device or plasma technology to produce the EMP. Microyield nuclear weapons or conventional EMP devices could be delivered to the vicinity of the target as a bomb or as the warhead of a missile. Given the unpredictable but damaging effect of EMP on electrical and electronic equipment, these EMP explosions can be against enemy platforms and facilities that depend on sophisticated electronics, particularly the enemy's command, control and communications system and air defenses. Missiles equipped with EMP warheads can also be effective weapons to gain air superiority, since modern high-performance fighter aircraft depend heavily on sophisticated, and therefore vulnerable, electronics [41].

The difficulty with the nuclear EMP effect is its indiscriminate nature. The pulse travels in every direction and covers large areas of the planet, potentially damaging friendly assets as effectively as those of the enemy. Another impediment to the use of nuclear-driven EMP weapons is the worldwide aversion to nuclear weapons, particularly nuclear weapons on orbit. Once a nuclear bomb explodes in space, the charged particles produced can easily be trapped in the earth's Van-Allen radiation belts. This would greatly increase the radiation exposure for any satellite passing near the radiation belts, disrupting or destroying poorly shielded satellites. The charged particles would remain

in the radiation belts for an extended period of time, denying the use of space to a friend and a foe alike

6.12.2 Evolving Countermeasures to EMP Weapons

Nuclear-driven EMP is omni directional, spraying large areas with damaging, broadband electromagnetic radiation. EMP created using more conventional technologies is characterized by directionality, relatively short range, and electromagnetic output centered in the damaging microwave frequencies. Arriving at light speed, the broadband nature of EMP makes it extremely difficult and expensive to defend against. Thus, the primary countermeasure for EMP weapons is electromagnetic shielding. Shielding must be provided separately against the electric and magnetic field components of EMP and it must take into account the broadband nature of the pulse. Since a large range of frequencies are present in EMP, the shield against low, medium, and high frequencies are needed. Also protective electrical filters wherever an electrically conductive channel enters electrical systems (e.g., power cables, transmission lines, antenna inputs, etc.) is necessary. Since filters perform differently at different electrical frequencies, this is a difficult task. A single mistake in grounding, filter design, or shielding geometry is enough to provide entry for damaging amounts of EMP, especially in high-speed computer circuitry. If we are able to break a few electrical grounds, shift the output spectrum of EMP attack, or penetrate the shielding at a few critical points, the countermeasure can be neutralized. Once the energy from an EMP effect has entered a region's power grid, communications grid, or computer grid, the entire network can be disrupted for a period of time or even destroyed [88].

6.12.3 Value of EMP as a Weapon

The nuclear-driven EMP weapon is only appropriate in total war scenarios due to its indiscriminate nature. The conventional EMP weapon, on the other hand, shows more flexibility in that it could be directional and its effects could be localized. Both forms of EMP weapons are at least moderate in their timeliness and responsiveness, since an EMP "bomb" could potentially reach its target within 30 minutes after launch by means of a delivery vehicle. The precision of the EMP weapon is relatively low, useful only for area targets e.g., enemy towns, large facilities, or a squadron of enemy aircraft. The survivability and reliability of EMP weapons are moderate to high, particularly if the weapons themselves are ground based. The selective lethality of EMP weapons is low. The effect of an EMP burst on any given electrical system is highly unpredictable, since it depends in great detail on the precise geometry of the engagement, the exact design of the electrical system under attack, and even the current state of the atmosphere. The conventional EMP weapon has very interesting possibilities as a potential future weapon. However, the currently unpredictable lethality, limited flexibility, and questionable precision make it unattractive as the primary component of war effort. This is an area of further research.

6.13 Evaluation of HPM as Weapon of Choice

HPM device also employs electromagnetic radiation for its weapon effect. Not as powerful as nuclear-driven EMP weapons, HPM weapons create a narrower band of microwave electromagnetic radiation by coupling fast, high energy pulsed power

supplies to specially designed microwave antenna arrays. Microwave frequencies are chosen for two reasons, the atmosphere is generally transparent to microwave radiation giving them all-weather capability, and, modern electronics are particularly vulnerable to these frequencies. Unlike most EMP weapons, HPM weapons produce beams defined by the shape and character of their microwave antenna array. HPM beams are broader and do not require extreme pointing and tracking accuracy (500 nanoradian stability and one meter target accuracy are adequate). HPM weapons can be trained on a target for an extended period of time, provided the power supply and HPM circuitry can withstand the internal currents. As a rough point of comparison, HPM systems produce 500 to 5,000 times the output power of modern electronic warfare (EW) systems [5,88].

6.13.1 Effectiveness of HPM as a Weapon

This weapon can fire instantaneously and give light speed which can be understood as a microwave "floodlight" that bathes its targets in microwave radiation. More directional and controllable than EMP, the general effect of this weapon on electrical systems is described above. Unlike conventional EW techniques, the effects of a HPM weapon system usually persists long after the "floodlight" is turned off depending on power level employed

Laboratory experiments have revealed that modern commercial electronic devices can be disrupted when they receive microwave radiation at levels as low as microwatts/cm² to milliwatts/cm². The more sensitive the circuit, the more vulnerable it is. While many electronic devices can be shielded using the same techniques outlined in the section on EMP weapons, most sensors and high-gain antennas cannot be shielded without preventing them from performing their primary functions.

HPM weapons are inherently limited by the fundamental laws governing electromagnetic radiation. An air borne HPM weapon must have an antenna or array of phased antennas with an area measured in acres to point and focus its beam properly on terrestrial targets. The resources necessary to construct such huge structures could be expensive to lift into orbit, and difficult to assemble in the free-fall environment. HPM weapon is a line-of-sight device that must "see" its target before it can fire. These are not practical considerations.

The level of pulsed, electrical power required to produce weapon-level microwave fluxes is now becoming available for ground-based systems. Compact, scaleable laboratory sources of narrow-band, high-power microwaves have been demonstrated that can produce gigawatts of power for 50 to a few hundred nanoseconds. Ultra-wide band microwave sources are less well developed, but research in this area appears promising. A HPM weapon should, however, be able to temporarily disrupt circuits and jam microwave communications at low-power levels.

Air borne HPM system would consist of a constellation of satellites with very large antennas or arrays of antennas. The farther out in space the constellation resides, the fewer the number of satellites required. However, there is a corresponding increased requirement for more power and larger antennas. Another possibility is to overlap "spot" beams from many smaller HPM satellites on each target, gaining the benefit of high

power on centroid at the cost of satellite proliferation. These types of weapons system configurations are hard to produce.

At low powers, the HPM weapon system is fully capable of jamming communications when pointed at the opponent's receiving stations or platforms, in addition to its uses against an enemy's electrical and electronic systems at higher power levels. Since water molecules are also known to absorb certain bands of microwave frequencies, it is also possible that a properly designed HPM weapon system could be used to modify terrestrial weather.

6.13.2 Possible Countermeasures to HPM Weapons

Advances in micro electromechanical devices and nano-technology could eventually result in devices and sensors so small that they are only a tiny fraction of a microwave wavelength in size. These devices, if small enough, could be immune to HPM weapons simply because microwave frequencies cannot couple enough energy into them to cause damage. Advances in optical computing and photonic communications could also be a useful countermeasure. Optical devices are inherently immune to microwave radiation, although the sections of optical circuits where light is converted back into current would still have to be shielded. The countermeasures outlined in the section on EMP weapons are also useful for HPM weapons.

6.13.3 Value of HPM as a Directed Energy Weapon

All-weather characteristics of the HPM make it very attractive for a weapon. Air borne variant, this light-speed weapon would be high in timeliness and responsiveness. However, the flexibility and precision characteristics are similar to the nuclear EMP weapon. In addition, it is limited by line-of-sight restrictions. Moreover, its requirement for large antenna make it impractical for air borne use. The selective lethality is, somewhat unpredictable. If nano-technology is perfected and incorporated widely into electronic systems, this could negate much of the effects of a HPM. Thus, the HPM weapon system is not deemed suitable for space-based applications but holds immense promise for ground and ship borne applications.

6.14 Potential Applications of EM Weapons

Electromagnetic weapons fall into following broad categories in terms of scale of attack and delivered power, illustrated in figure 6.12.

- Special forces and terrorist weapon, which have low emitted power and coverage.
- Strategic and tactical military systems, which are built to destroy, major facilities and sites.
- Electromagnetic strategic weapon, the high altitude airburst nuclear EMP bomb.

The electromagnetic weapons can also be categorized as "Soft Kill" and "Hard Kill". A soft kill is achieved when the weapon causes the target to crash or reset, lose data or get into an unrecoverable state requiring a reboot. Once the electromagnetic weapon ceases to affect the target system, and it is rebooted, normal operation can resume. The effect of soft kill is therefore to disrupt operations, causing downtime and preventing the organization from performing its assigned task.

A hard kill is achieved when sufficient energy is delivered into the target system, such that it is permanently electrically or physically damaged and can no longer perform its function. The objective of a hard kill attack is to inflict attrition upon the target electronic assets. A target system subjected to sustained hard kill attacks will eventually lose the capacity to perform intended functions [40].

6.14.1 Weapons for Special Forces and Terrorists

These are designed to destroy a single machine, workgroup of machines, or disable the networked systems in a single building, are used from very short distances and, do not require direct physical contact with the target. The examples are as follows:

- **HERF and HPM Guns:** These weapons have following characteristics
- The High Energy Radio Frequency (HERF) guns are devices which can emit and focus a high power beam of RF energy. They operate at frequencies above 100 MHz, have power levels to produce standing wave amplitudes of hundreds of Volts on the wiring or interconnecting cables associated with the target systems.
 - The HERF guns operate at microwave frequencies which produce, kilo Watts of peak power, qualify as a High Power Microwave (HPM) weapons and cause damage through back door coupling of standing waves on cabling, or directly coupling into equipment chassis through ventilation holes and poorly secured panels.
 - The Tesla coil is a non-directional equivalent of a HERF gun, operating at hundreds of kilohertz. It can be concealed within the vicinity of a target system, left to operate unattended and used as a series denial weapon
 - The HERF guns can be pulsed or continuous wave, they expose semiconductors to RF voltages to cause breakdown of MOS gates and PN junctions. They are also harmful for living organism.
- **Portable Explosive Flux Compression Generators:** These devices have following characteristics.
 - Explosively pumped flux compression generators are the preferred power source for strategic and tactical military EM weapons. The generator device itself can produce Mega Gauss magnetic flux levels at very short distances.
 - They produce a ramping pulse of up to Mega Amps of current within the generator, lasting several hundred microseconds, which can damage transformers and semiconductors.
- **Tazers and Power Line Spiking:** The Tazer stun gun can be used to damage network interfaces across large numbers of machines, by injecting voltage pulses of kilo Volts of magnitude into network cabling. Any device, which can produce a very rapid short circuit, and then open circuit, can be used to "spike" mains power lines. Such sharp transients traveling along power cables can penetrate power supplies to damage components, as well as damage data communication interfaces through differential earth potentials. Spiking of power lines also requires physical access, although this may be outside the security perimeter of a site.

6.14.2 Strategic and Tactical Military Weapons

Strategic and tactical military electromagnetic weapons are specifically designed to destroy a wide range of electronic equipment over hundreds of meters of diameter. These weapons have been described as the "Nuclear Weapons of the Information Age", and would be used in future military operations, punitive strikes and high caliber terrorist operations. Two technologies are at the core of such weapons. The explosively pumped flux compression generator, capable of producing currents of up to tens of Mega Amps and energies of tens to hundreds of Mega Joules. Alternately, it may be used to drive a High Power Microwave tube and produce a single pulse of tens of GigaWatts. The examples are as follows [39].

- **Low Frequency EMP E-Bombs:** It is an air delivered bomb containing a pure flux generator warhead, termed as LF E-bomb, produces an intense magnetic field in the near vicinity, which inductively couples into wiring, producing a single high voltage pulse, possibly with a ringing transient decay.
- **HPM E-Bombs:** These are air delivered bombs containing a flux generator powered HPM warhead, termed as HPM E-bombs, produce microwave field strengths of between kilo Volts to hundreds of kilo Volts per meter, in a footprint of hundreds of metres of diameter with duration of up to several microseconds. The microwave radiation may be circularly or linearly polarized, and can produce high voltage standing waves on wiring and cables, as well as directly penetrate through holes in shielding.
- **Combined Effects E-bombs:** A Combined Effects E-bomb is a HPM E-bomb which uses an oversized FCG to produce a combination of HPM and LF damage effects. Such a weapon will be effective against any target vulnerable to either HPM or LF weapons.
- **High Power Microwave Directed Energy Weapons (HPM DEW):** These are equivalent of the HPM/HERF guns, can deliver peak powers of GigaWatts and average powers of hundreds of Kilo Watts, and produce damage through high voltage as well as thermal effects. These weapons are also extremely dangerous to personnel and subject to wavelength of operation, they can penetrate many miles of rain or cloud to damage or destroy a target.

EMP & RF ENERGY WEAPONS

TERRORIST / SPECIAL FORCES WEAPONS

- HERF & HPM GUNS.
- PORTABLE EXPLOSIVE FLUX COMPRESSION GENERATOR
- TASERS & POWER LINE SPIKERS

TACTICAL & STRATEGIC MILITARY WEAPONS.

- LF EMP BOMBS.
- HPM E_BOMBS
- COMBINED EFFECT EM BOMBS
- HPM DEWs

Source: The Impact of EM Radiation on computer systems architecture, Karlo Kopp and Ronald pose.

6.15 Conclusion

In this chapter we have seen that the nuclear or non-nuclear Electromagnetic energy can cause devastating effects on civil as well as military information infrastructure. The EMP devices can be used to make weapons for law enforcement internal security and military use. These weapons can disable or damage a target country's information infrastructure at a very large scale and therefore possess deterrence value near equivalent to nuclear weapons. In a military perspective at the same time, there is a need to protect own National Information Infrastructure against the use of EM weapons by our adversaries. Thus there is a need to develop techniques and materials which can resist energy penetration or minimize the disabling effect of energy on our information and communication assets in the civil and military sectors. There is also need to develop protection techniques against large-scale saturation attacks. Considering all these factors EMP and RF energy weapons on a one to one basis can fit into the role of the existing weapons. The EMP and RF energy weapons therefore hold immense promise to form the mainstay of our military capability in regional as well as global context.

In this chapter we have concluded that EMP and RF Energy Weapons are emerging as "Nuclear Weapons of Information Age" and held immense value as tactical and strategic capability in terms of defensive and offensive military posture. They also have equally serious internal security dimension in the context of terrorism and law enforcement. The development of IW capability around EMP and RF Energy weapons is therefore emerging a national security necessity, Based on these inferences, the assessment of technology for development of these weapons has been examined in chapter 7.

CHAPTER 7

TECHNOLOGY ASSESSMENT FOR DEVELOPMENT OF EM WEAPONS

7.1 Introduction

In the previous chapter we have concluded that in order to architect a major EMP and RF energy weapons program, it is necessary to precisely evaluate and assess the underlying technologies. The origin of the EMP has been traced to the detonation of the nuclear weapons and to the simulations through non-nuclear means for testing and verification under laboratory conditions. It emerged that the work is classified and is confined to USA, China, Europe and countries of Russian origin. It also emerged that EM weapons have the potential to cause unprecedented disability, damage and destruction to the NII of a target nation. Therefore IT advanced nations recognize that they are very vulnerable to the use of EM weapons against their respective NIIs and have commenced development programs at national scale. The fear of EM weapons has also resulted in far more serious concerns about the proliferation of these technologies to terrorists or countries not aligned to western political and economic interests. As a result of these apprehensions the developments of protection strategies against the EM weapons are gaining momentum.

It also emerged that considering its social, economic, political and military conditions, development of IW capability around EMP and RF energy weapons by India is a very attractive option. This chapter examines the origin of RF weapon technologies, advances in RF sources and antennas, on going research and developments in RF weapons, RF mitigation techniques and the susceptibility of NII to microwave energy and emerging directions for major weapons programs. The information has been extracted from the testimonies given by scientists and seniors functionaries to Joint Economic Committee of USA, account of interaction amongst American and Soviet Scientists, their exchange visits to Russian laboratories, visits to other countries, continued scientific contacts, research reports, from contracts and test results.

7.2 Historical Background

USA, Russia, United Kingdom, Sweden, and Australia have been exchanging views with Russians through visits to laboratories developing directed energy weapon technologies, pulsed power systems technologies, high power lasers, and space-based neutral particle beams. Dr. I W Merritt of Advanced Technology Directorate (ADT), US Army, during his testimony to Joint Economic Committee (JEC) of the US congress in Feb. 1998 has given a detailed account of these exchanges [151,183,188]. In 1992 his team had visited the Moscow Radio Technical Institute, which was developing high-power microwave sources and which had also a large test facility for performing susceptibility and effects measurements. In 1994, they visited the Kharkov Physico-Technical Institute in Ukraine, where they were developing high power microwave sources, such as the Magnetically Insulated Linear Oscillator (MILO), neutral particle beam sources and prime power systems. They were also performing susceptibility and effects tests. The MILO was invented in the U.S., but as per Dr. IW Merrit, USA

discontinued work on it in the late 1980s. The Soviet Union (SU) picked up the technology and successfully continued its development. Russia also exploited the Magneto Cumulative Generator (MCG) as an explosively driven power supply. Dr. Andrei Sakharov in the SU developed the MCG and the Russians have used MCG power supplies extensively to drive Ultra Wideband and HPM sources, lasers, and railguns. In 1995 they again visited the Kurchatov Institute to discuss laser and high current problems, the All-Russian Electromechanical Institute to discuss high voltage technology, Ioffe Physico-Technical Institute in St. Petersburg to discuss ultra fast switches, and the Institute of Problems of Electrophysics, also in St. Petersburg, to discuss pulse power and plasma technologies.

In 1994 Gen. Loborev, Director of the Central Institute of Physics and Technology in Moscow, distributed a landmark paper at the EUROEM Conference in Bordeaux, France. In this paper Dr. A. B. Prishchepenko, the Russian inventor of a family of compact explosive driven RF munitions, described how RF munitions might be used against a variety of targets including land mines, sea skimming missiles, and communications systems. He further popularized these munitions with articles in Russian naval journals and in other professional journals and magazines.

Dr. IW Merritt revealed that the Soviet Union had a large and diverse RF weapons program and remnants of this work continue today within Former Soviet Union (FSU) countries. The scope and results of the Soviet program are poorly understood, but personnel from the Advanced Technical Directorate (ATD) of Missile Defence and Space Technology Centre of the US Army have been at the forefront of efforts to gather information and to understand it and its accomplishments through Windows on Science and contracts for R&D effort. Their principal objective appears to understand requirements and to identify technologies applicable for RF mitigation. Large uncertainties still exist concerning the status of RF weapon development and associated efforts to mitigate their effects on electronics. In spite of these uncertainties, it is clear that many nations continue to aggressively pursue the development of RF weapons and techniques to mitigate their effects. Air Cmde. C. N. Gosh has emphasized the need for India to pursue EMP Weapons program [14].

7.3 Evolution of High Power Microwave Devices

- The evolution of High power Microwave (HPM) devices during the past 100 years is shown in figure 7.1. It is evident that this technology has reached maturation and is available to construct weapons [9].

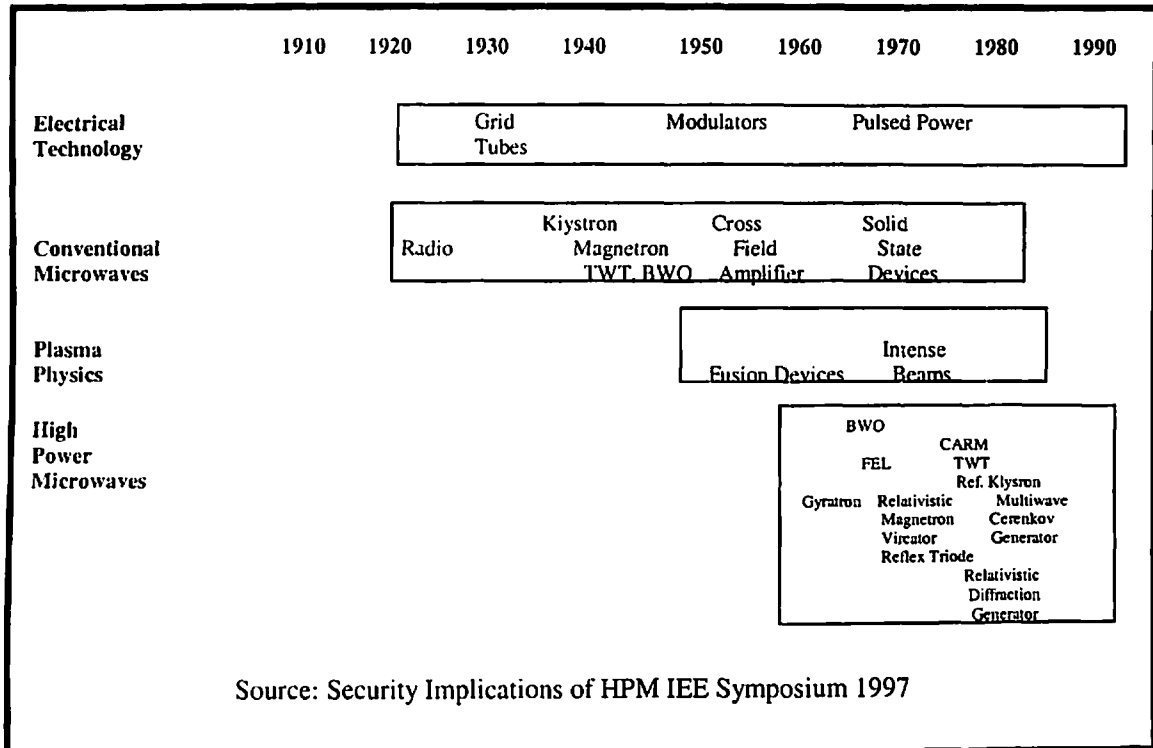


Fig 7.1: Evolution of High Power Microwaves

7.4 Profile of EM Weapons Programs USA

The following details about the on going RD &D work in various countries signifies the volume, complexity and the readiness status of EM technologies for military programs.[4,48,69,79,138,150].

7.4.1 National Security Space Road Map (NSSRM) USA

NSSRM has projected a focused thrust by the USA to develop and transition HPM weapons technology into operational systems. These efforts include technology development and demonstration of advanced HPM weapons and RF hardening techniques. Major milestones have been achieved in demonstrating high power RF sources of a variety of wide and narrow band weapons applications including following 4 mission programs as a major development initiative.

- High Power Microwave (HPM) under the Aircraft Self Protection (ASP) Project.
 - Counter Surface-to-air & Air-to-Air Missile
 - Large Aircraft IR Countermeasures
- HPM Suppression of Enemy Air Defences (SEAD)
- HPM Command Control Warfare/Information Warfare (C2W/IW) for air interdiction of C4I assets, degrading enemy air control, military base operations and hardened target weapons.
- RF Active Denial Technology

The program also covers RF effects and hardening programs for environments, systems responses, RF test and measurement techniques, RF protection techniques, RF standards,

handbooks and design guides, hardness maintenance assurance and planning and execution of system level tests.

7.4.2 Defense Advanced Project Agency (DARPA), USA Program

The DARPA project reports BMDO 96 014 on Diamond Solid state Switch for Pulsed Power and other Applications, BMDO 96- 005 on High Temperature, High Power Fast Plasma Switch et.al describe major thrust on development of basic building blocks of RF weapons.

7.4.3 Defense Technology Area Plan, (Weapons), USA

WE.19.08 HPM Aircraft Self - Project Missile Counter Measures, WE. 22. 09 HPM C²W / IW Technology, WE.23.08 Modern Network Command & Control Warfare Technology projects are targeting developments from the operational perspective.

7.4.4 DoD, USA RDT & E Budget Items

Project 2053, Feb. 2002 for Radio Frequency Weapons (Amongst others) is indicative of budgetary provisions and long term planning by the Depart of Defence, USA.

7.4.5 US Army, Science and Technology Master Plan 1998

Chapter IV K RF Directed Energy weapons, Table IV 23 Electronic Warfare / Directed Energy Weapons Linkages to Future operational capabilities indicates the Service level involvement so that these weapons get seamlessly integrated with the existing systems.

7.4.6 Summary of Research Work

The summary of development underway in the area of EM energy devices across the globe as presented during the 11th IEEE International Symposium on Pulsed Power Conference at Baltimore, Maryland, USA in 1997 is presented in figure 7.2 [179].

S No	Area of R&D & D	Project Specific Development
1	Pulsed Power Systems & Multi Gap Spark Switches	<ul style="list-style-type: none"> Atlas Project. Los Alamos National Laboratory, USA Syrinx Technological Program, Ecole Polytechnique, France
2	High Power Microwaves, Radiation Sources	<ul style="list-style-type: none"> X-Band 3 G W Relativistic BWO Based High Current Repetitively Pulsed Accelerator, Institute of High Current Electronics, Russia Improved Radiation output from Decade Module Swerdrup, Tech, USA High Power ION Beams. National Research Lab, USA 81-7M-01-A Two Beam Accelerator., National University of Defence Technology PRC, China
3	Electromagnetic and Electro Thermal Launchers	<ul style="list-style-type: none"> Setup of Captive 300kJ Pulsed Power Supply System, FMV Defense Material

		<p>Admin, Sweden</p> <ul style="list-style-type: none"> • Test Bed for 5 MW Battery Based Inductive Power Supply
4	Opening Switches	<ul style="list-style-type: none"> • Conduction Time / Current Limitation on the Defence special weapons Agency Decade Module, Naval Research Laboratory, USA • Accelerator for Open Air Beam Injection, PRC Kurchatov Institute, Russia
5	Gas Plasma & Pseudo Spark Switches	<ul style="list-style-type: none"> • Sealed off Switches for Pulsed Power University of Erlangen – Nuremberg, Germany • Low Profile High-Voltage Compact Gas Switch Lawrence Livermore National Laboratory USA
6	Solid State Switches and Photo Connectivity Switches	<ul style="list-style-type: none"> • PFNs Switched with Stacked SCRs at 20k, 500J and 100Hz repetitive rate. Institute for Technical Physics, Germany
7	Diagnostic & Computational Techniques	<ul style="list-style-type: none"> • Pulsed ION beams & Ablation Plumes Exhausted from Targets Irradiated by ION beams. Tokyo Institute of Technology, Japan • Ivory PIC Simulations of the Z – Insulator Stack, Sandier National Laboratory, USA
8	Pulsed Inertial and MHD Generators	<ul style="list-style-type: none"> • High Performance Pulsed Power Generation Systems Using Disk MHD Driven by NPG System. Nagoka University of Technology, Japan
9	Insulation & Dia-electric Breakdown	<ul style="list-style-type: none"> • Vacuum Insulator Coating Development,. Mass. Institute of Technology USA • Electrode Unit for Operating in Liquids with High Specific Conductivity, Institute of Pulse Res & Engg ,Ukraine
10	Magnetic Flux Compression Generators	<ul style="list-style-type: none"> • Study of High Energy Linear Compression in HEL – 1 Experiment, Los Alamos National Laboratory, USA • High Voltage Pulsed Based on Dynamic Plasma Techniques, Air Force Research Laboratory, USA
11	High Current Accelerators & Components	<ul style="list-style-type: none"> • Capacitors for High Power Electronics, Maxwell Energy Products, USA • High Power Super Conducting Delay Line, Lawrence Livermore Laboratory, USA

12	Very Large Pulsed Power Systems	<ul style="list-style-type: none"> • Pulsed Power Performance of PBFAZ, Pulse Science Inc USA • Syrian Project 640 kJ Inductive Energy Generator, ITHPP, France
<p style="text-align: center;">Source : Proceedings of 11th IEEE International Pulsed Power Conference Baltimore, Maryland 1997 Figure 7.2: Summary of RD & D Projects, usable in EM Weapon Programs</p>		

7.4.7 Directed High Power RF Energy: Foundation of Next Generation Weapons (DoD HPC Challenge Projects)

The High Power Microwave Division of the Air Force Research Laboratory, USA is working on three fronts and involving three separate teams. The "Source Development Team" designs the sources that generate the RF pulse. The "Beam Tracking" team is tasked with proper propagation of the RF energy and then directing it towards the target. The "Effects Team" studies the interaction of the RF energy with the target. Intensive modeling and simulation is crucial in all three phases of the project. Magneto-hydrodynamics (MHD) codes are used in the analysis and modeling of the pulsed power; Particle-In-Cell (PIC) codes are used in the modeling and simulation of the source; and Electromagnetic (EM) codes are used in the modeling and simulation of extraction and propagation of the RF and in modeling certain aspects of the effects. These issues are examined separately in chapter 8[45,48].

The teams use a number of parallel first-principle physics codes, developed under previous Air Force R & D projects, to do modeling and simulation on the massively parallel computers at the DoD High Performance Computing (HPC) centers. The design and development of the entire HPM system, including the pulsed power, the source, the extraction and transport, and the effects appear to have been modeled.

7.5 Events in Other Countries

Specific examples of interest in RF weapons and the proliferation of this technology as outlined by Dr. IW Merritt and quoted in other references are as follows [151, 155].

- The French Gramat Research Center has dedicated significant assets to study the effects of electromagnetic energy on electronics and in 1989 Thompson CSF published brochures in which they stated that they were developing RF weapons.
- A 21 January, 1998 newspaper article in the Swedish newspaper SVESNSKA DAGBLADET reported that the Swedish National Defense Research Institute had purchased a Russian "suitcase bomb" that uses high power microwaves to "knock out" computers and destroy all electronics within the radius of its "detonation". The article also reported that this device is being sold commercially and that it has been sold to the Australian military. The price was reported to be several hundred thousand Kroners, or about \$100,000.
- Mr. Carlo Kopp, an Australian professor, who claims to have had a relationship with their military, has his own web site (<http://www.cs.monash.edu.au/carlo>) and has provided detailed papers on the alleged effects of RF weapons and sketches of design concepts.[PUB MS DS] The Applications of High power Microwave

devices for weapon and non- weapon applications are illustrated in figures 7.3 and 7.4, as projected in USAF AF 2025 Submissions [178].

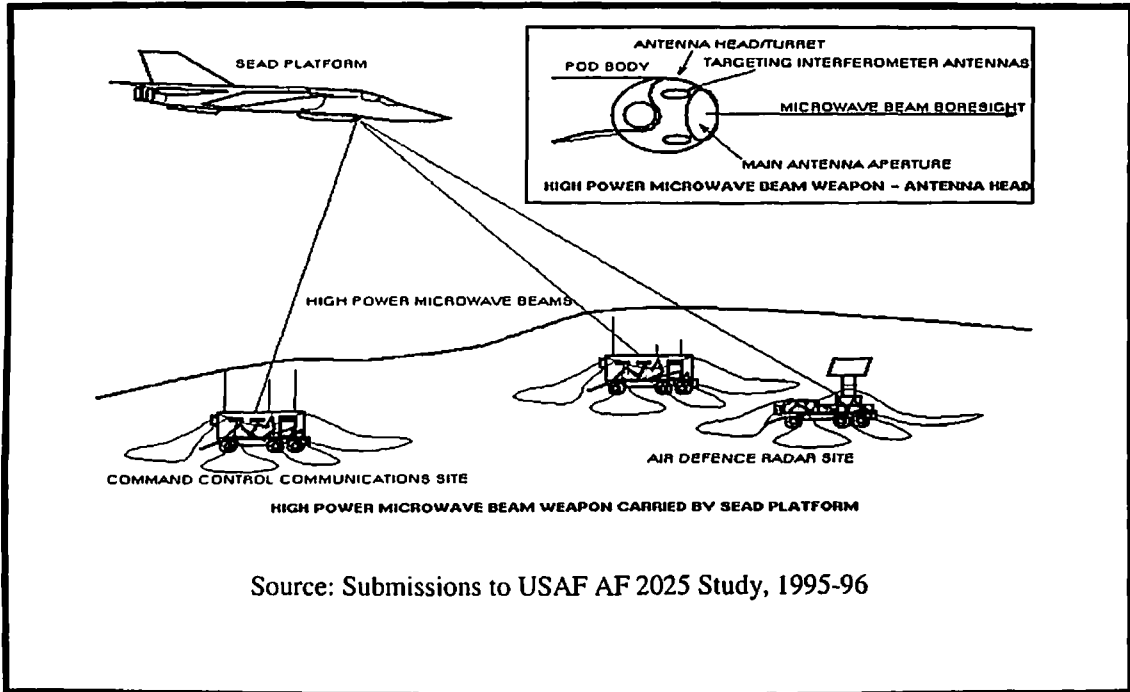


Figure 7.3: High Power Microwave Beam Weapon Carried by Sead Platform (C. Kopp, 95/96)

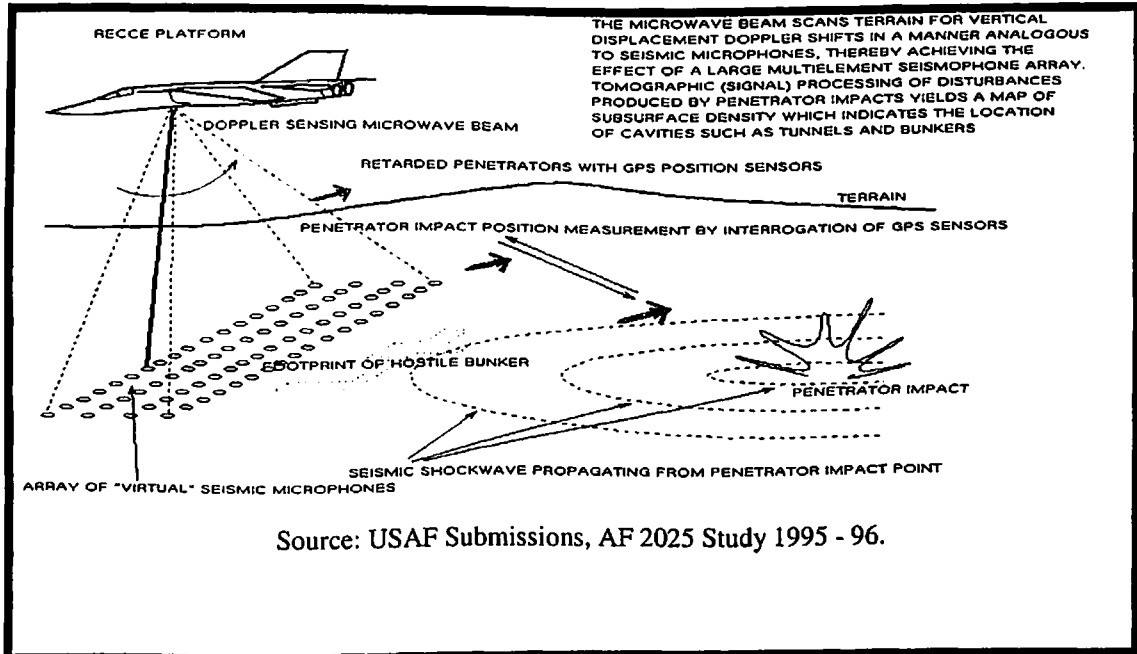


Figure 7.4: Microwave Seismic Sensor Carried by Rece Platform (C.KOPP 10/95)

7.6 Development of Building Blocks for RF Weapons

RF energy sources usable for weapons programs have been classified in several ways, viz. HPM or UWB, pulsed or continuous, single shot or repetitively pulsed, and very short pulse (nanosecond) or long pulse (microsecond to millisecond) devices. In addition, the electrical or explosive power sources have significant effects on the output characteristics of the device. For example, the explosive driven munitions described by Mr. Carlo Kopp and the RF munitions described by Dr. Prishchepenko are single shot devices that convert the chemical energy of high explosives first into magnetic energy, then into electrical energy and finally into microwave energy. This multi-step conversion of energy is inherently inefficient. However explosives are very compact sources of energy. As electronics are not very robust to external sources of energy, the idea is to place the RF energy source/weapon as close to them as possible for inflicting maximum damage. Electrically driven devices have fewer energy conversion steps, but typically they are larger in size and produce less power per pulse. The detailed description of these devices is given as follows.[39,151]

7.6.1 Electrically Driven Devices

The electrically driven (non-explosive) devices require an external power supply and energy storage system, which leads to larger and less self-contained systems than can be produced by explosive-driven approaches. However, two recent technologies that minimize this limitation are the solid state pulsers developed at Ioffe Physico-Technical Institute in St. Petersburg and the RADAN system. These devices are compact and can be powered by small hand-carried energy sources.

As described by Dr. IW Merritt, the Pulsers developed at Ioffe Physico-Technical Institute are based upon very fast (nanosecond and picosecond) solid state "on" and "off" switches developed by Prof. Igor Grekhov and Dr. Alexi Kardo-Syssoev. These switches have been used to generate 10 nanosecond, 10 KHz pulses for a prototype ground penetrating sensor that is now being used commercially in St. Petersburg . This 10 kg portable sensor is said to be used routinely to image to depths of 200 meters with an accuracy of 1% of the depth and it is claimed to be able to image down to 1000 meters with slightly lower resolution [151]. Jammers based upon these switches can be made small enough to fit into a briefcase. A recent version is said to weigh 6.5 kg and delivers fields of 30 kV per meter at 5 meters. This is comparable to high-altitude EMP (HEMP) field strength. An optimized version is said to deliver 100 kV per meter at 5 meters and the pulse width and repetition rate can be tuned to have the maximum effect on the intended target.

RADAN is a compact high-current electron accelerator that is smaller than an attaché case and weighs about 8 kg with its rechargeable 12 Volt battery power supply, but not including its antenna. RADAN can be used to stimulate several outputs including lasers, x-rays, wide band RF and high power microwaves that allow RADAN to be used as a jammer. RADAN output parameters are: total output power 5 MW; repetition rate up to 1 kilohertz; pulse width about 2 nanoseconds; and output pulse bandwidth from 1 MHz to 5 GHz. A directional antenna has been developed and the developer has proposed that RADAN could be used to stop car engines and to destroy the electronic arming and

firing circuits of bombs. Limited testing of RADAN has been conducted in the U.S. and it was found to affect calculators and electronic watches.

The Russian built NAGIRA radar produces short powerful pulses with the following characteristics 10 GHz fixed frequency, 5 nanosecond pulse length, 300 MW peak power, 2 Joules per pulse, 150 Hz pulse repetition rate. NAGIRA was purchased by the UK Ministry of Defence and was delivered to Defence Research and Evaluation Agency (DERA) Frazer, near Portsmouth, in November 1995. Indications are that the UK will use NAGIRA to investigate detection of fast moving targets in sea clutter, to study electromagnetic-pulse penetration into equipment and to measure the effectiveness of front-end protection devices. During initial field trials near Nizhny Novgorod, Russia, NAGIRA was able to track a helicopter at more than 150 km range and at altitudes as low as 50 meters. It is believed that because of electromagnetic interference (EMI) concerns, Russian helicopters were not allowed to operate within several miles of the radar when it was operating at full power.

7.6.2 Explosive Driven Devices

Compact explosive-driven radio frequency munitions being developed by Russia are claimed to range in size from a hand grenade to a 155-mm artillery shell and the output may be either a HPM or an UWB pulse. Since these warheads are part of a projectile, they are intended to detonate very near to their target, so fratricide i.e. possibility of damaging own systems is not a problem as it would be with HEMP.

As testified by Dr. IW Merritt, in June 1997, a U.S. measurements team led by the Advanced Technology Directorate had participated in a joint series of measurements on Radio Frequency Munitions (RFM) at a site near Nalchik, Russia [151]. The purpose of these tests was to verify Russian claims about the output of Dr. Prishchepenko's compact explosively-driven RFM. The test results left Russian claims unconfirmed, since most U.S. measurement equipment was not allowed by Russian authorities to reach the test site and since Dr. Prishchepenko's team claimed that the RFM that were tested radiated in a band that could not be measured with equipment at the site.

From the testimony of Dr. Merritt, it emerges that ATD engineers continue to evaluate RF weapon technologies, to work closely with other countries, and to identify technologies that can be adopted for military applications and commercialization. They maintain relationships with other scientists through direct personal contact at conferences and site visits, through small research contracts, in collaboration with the U.S. Department of State on International Science and Technology Center (ISTC) and Science and Technology Center of the Ukraine (STCU) projects, and through the U.S. Air Force's Windows on Science Program. ATD has been effective in identifying and executing joint projects, such as the joint radio frequency munitions test in Russia and briefings on the solid state pulsers developed at the Ioffe Institute in St. Petersburg. They are now working to bring the underground imaging sensor and its developers to the U.S. to test its ability to detect land mines. Solid state switches developed by the Ioffe Institute are now imported by a U.S. company that produces water purification equipment using Russian pulse power hardware. ATD has cooperated in hosting many

scientists under the Windows on Science Program, including a scientist from Loughborough University in England, the only university that designs, tests, produces and markets inexpensive MCGs.

Many source and antenna technologies can be used to produce devices with very different output characteristics. For example, Russia reports that its cylindrical shock wave source generates a single Gigawatt pulse about a nanosecond long. However, susceptibility tests in the former Soviet Union and U.S. suggest that irradiating a target with a train of nanosecond pulses is more damaging than a single pulse, since multiple pulses lower the damage threshold of the target. As a result, Russian emphasis has been on devices that produce a train of pulses. Some designs are said to generate 50 to 100 pulses, each about a nanosecond long, in a burst of pulses about 10 microseconds long.

7.6.3 Transient Electromagnetic Devices (TEDs)

There is a new type of directed energy called Transient Electromagnetic Radiation (TED). Instead of generating a train of smooth sine-waves, as the conventional narrow-band systems do, it generates a single spike-like form of energy. This spike-like burst of potential does not have "cycles" or waves and it may be only one or two hundred picoseconds (psec) in length. 100 psec is the time that it takes light to travel 1.2 inches and often these short time duration pulses are described in "light-inches" [183]

It is very similar to the type of signal that occurs when you rub your feet on the carpet on a dry day and then touch your computer keyboard. An electrostatic discharge (ESD) occurs when you do this. The electrostatic charge on your body discharges onto the computer and a very brief amount of very high current flows quickly from your finger into the computer circuits causing a momentary break in the normal flow of signals and bits of information. Because of this momentary break in the "bit-flow" the ESD may cause the computer to crash and in some cases it may cause sensitive electronic circuits to be actually damaged to the point where they are non-functional and must be replaced. This vulnerable item may be a single semiconductor diode in an integrated chip in a circuit on the motherboard. It is often economical to replace a whole circuit board of components rather than trying to find the one specific circuit and replacing just it. This type of new weapon source, a transient electromagnetic device (TED), is actually a system that radiates an ESD-like signal that is intended to cause a similar response, as just described, to the targeted system.

7.6.4 Comparison Between Narrow Band & TED HPM Systems

There are differences between narrow-band (NB) and TED HPM systems. The NB systems generate sine waves, the TEDs don't. The NB systems are very complex, the TEDs are simple in construction, the NB systems generate very high average powers (microwave heating), the TEDs generate very high peak powers (and are poor RF heaters). They both use an antenna and the larger it is, the more power they can radiate, in a narrow focused beam, at the target.

In a narrow-band HPM device, high technology vacuum tubes are used which is similar to those used in high-powered TV or FM stations and radar systems. They require large

amounts of primary power and cooling system. All this complexity requires complex engineering and development, and considerable manufacturing time and cost.

TEDs use simple spark-gap switches, either in oil or in pressurized gas pulse storage lines. The power supplies are relatively small in size and much lower in average power and cost than for the NB systems. The engineering and mechanical issues are small in comparison to the narrow-band devices. The technology is well described in the various professional Pulse Power references. The development, engineering, and manufacturing costs are small in comparison to narrow band. Most of the technology is available and is an outcrop of the nuclear and flash x-ray work done in the past.

As described by Mr. David Schriener "NB systems operate at a given frequency with a small bandwidth, and you will find them at one spot on the radio dial. The TEDs do not even have a definable frequency but instead, because of their short time duration, they occupy a very large spectrum space, and you will find it everywhere on every radio dial. When a TED pulse is generated it will have the ability to excite responses in systems designed to receive at any frequency from as low as 100 MHz up to several GHz, from the FM band up to the lower microwave bands. A NB system would excite only those systems that were operating at its frequency, say 2.345 GHz, so a narrow band system must be "tuned" to a given target's known soft spot but a TED system would go after any soft spot of the target platform, back-door or front door."

7.6.5 Potential of TEDs Being Used as Weapons

Simplicity of TED systems make them attractive for RF terrorists. The literature survey reveals that there is a possibility of building a TED source using "back-yard" methods, a Radio Shack Terrorist RF weapon. Such a system would have to have sufficient power, with some degree of probability, cause detrimental effects to common infrastructure items such as financial institutions (banks, ATMs, and stores), medical facilities, airport facilities, general transportation items (auto engine controls, ABS, air-bags, etc.), utility facilities (telephone exchanges, power grid controllers), and other infrastructure entities. This type of source is imagined to be what a criminal, terrorist, or prankster could develop or build in a reasonable time, with reasonable tools and materials and with open literature or reference material. Mr. David Schriener has testified following to the JEC w.r.t. the fabrication of a TED device in an environment directly controlled by him: [183].

- The models made in his home laboratory/workshop used off-the-shelf materials and open-source references.
- The laboratory tests of this hardware were made in a controlled environment with the proper security in place.
- The results of these tests, the data capabilities, and the target set identities are kept in a facility cleared for classified storage.
- The Development of any of this hardware is reported on a regular basis to those with whom he relates at a classified level to assure that they are informed at the work and are able to apply this to their interests and efforts if necessary. Any of this hardware can be used by them for any determination of utility to military interests.
- A standalone briefcase size object to be placed closer to a target.

- An unsuspecting looking gadget to be installed in a vehicle with an antenna.
- A variant suitable for positioning at a remote target location.
- A variant, which can be, fitted in a place suitable to fire at flying objects viz airliners.

7.7 Live Testing

US has conducted Joint Live Fire (JLF) Tests with the three Military Departments to assess the effects of radio frequency weapons. The JLF tests examine the survivability of systems to such weapons. The source was a transient electro-magnetic broadband threat, making potentially susceptible a much wider range of equipment than the more traditionally tested narrow band systems. The tests were conducted outside, rather than the vast majority of other testing, which has been done at short range inside enclosures. The tests were done against a fully operational Army's Huey Cobra Gunship as the candidate platform to gain insights into the first order effects and learn to test such systems to these threats. The intent in testing such an older and less sophisticated platform was that it would be less costly and available for destructive testing. Also to conclude that if such an unsophisticated platform were to be vulnerable to such threats, then newer, more computer dependent platforms could also be, the results are however classified.

7.8 Damage Potential of RF / Microwaves Weapons

The effects of EMP and RF energy on the semiconductors have been examined in chapter 5 in detail. Some of these are critical for design of weapons for specific operational needs vis-à-vis existing military systems. These are summarized as follows [33, 162]

- Semiconductors are vulnerable to the effects of radio frequency energy as semiconductor features become smaller and smaller. Commercial microelectronics make heavy use of metal oxide semiconductor devices which fail when subjected to voltages that exceed the dielectric strength of the component or when the device melts as a result of heating from currents induced by the RF pulse [HPRF WPN 99].
- High Power Microwave and ultra wideband signals differ in their pulse length and frequency content. The HPM sources produce short, very high power, narrowband pulses, often billions of watts (gigawatts) in billionths of a second (nanoseconds). If HPM waveforms are in-band, they can efficiently couple energy into the target and cause damage to sensitive "front door" components that are connected to antennas. If the HPM frequency is not in-band, the energy must enter through a "back door" and coupling to the target is generally poor. In this case, much less energy enters the target to disrupt or to cause damage.
- Ultra Wide Band, sources generate a much wider band of frequencies than HPM sources. This ensures that at least some energy is at a frequency to efficiently couple to the target. However, since the energy is spread across a wider band, the power spectral density is lower and the amount of energy available in a wideband is also much lower. As a result, an UWB device is more likely to disrupt than to destroy a target, except at very close range. UWB sources can be repetitively pulsed and therefore can continue to disrupt the target as long as the source is functioning and within effective range. Many systems tend to be susceptible to disruption or damage at specific, sometimes unpredictable, frequencies. As a result, weapons designed

with UWB devices are well suited to exploit these susceptibilities, since they produce significant energy over a wide range of frequencies. This area has been aggressively researched by the Soviet Union, Russia.

- Extensive work has been conducted to understand the effects of high-altitude nuclear EMP (HEMP) on systems and components, but these data are mostly for frequencies less than 1 GHz and for pulse widths in the range from 50 nsec to 1 usec. The shorter pulses characteristic of HPM and UWB waveforms are significant because current methods for protecting electronics from HEMP, and other anticipated sources of disruption, will not be effective against pulses from RF weapons designed using HPM and UWB devices.
- High-altitude nuclear EMP does not have significant energy above a few tens of megahertz, whereas HPM spectra are typically in the few gigahertz to tens of gigahertz range and UWB spectra may contain energy in the frequency range from hundreds of megahertz to a few gigahertz. There is extensive information on the effects of lightning and nuclear EMP on electronic devices, but these pulses are significantly longer than the pulses from HPM and UWB sources. Since HPM and UWB pulses tend to be shorter than the response times of most limiters, their RF energy can pass largely unattenuated into the target and cause upset or damage before the limiter can turn on.
- Tests over the last 10 years have produced data on component responses to pulse widths in the range from 1 to 50 nsec. However little information is available that describes electronic responses for incident pulses having sub-nanosecond pulse widths. Testing is needed to establish effects of the following general waveforms: very short (nanosecond and sub-nanosecond) single pulses, multiple closely-spaced very-short pulses, and long (millisecond) pulses.
- Much of the existing effects data is from direct drive tests. Such tests produce the most repeatable indication of whether or not the pulse in question will upset or damage the device being tested. However these tests do not help clarify the issue of whether or not the RF waveform in question will actually couple through the walls, openings, filters, cables, and wires that separate components at risk from the external environment. This uncertainty creates a situation in which even the best analysis must be based upon significant assumptions. As a result, the commercial and military systems may be much more, or much less, susceptible to upset or damage than we now assume. As a result, characterization of representative components and circuits and the effects of physical configurations are needed for very short pulses.
- A 1996 paper by Bludov, et al from the Kharkov Physico-Technical Institute, Ukraine described HPM and UWB testing on electronic components and biological systems. The paper identified three levels of damage: temporary upset, permanent upset, and burnout. It appears that Ukraine has a systematic program to characterize the effects of HPM and UWB waveforms on electronic components.

7.9 Emerging Directions

Global interest in RF weapons has increased significantly in the last few years. It has emanated from the collapse of the Soviet Union. This is probably the most significant factor contributing to this increase in attention and concern about proliferation. A recent

study of open source literature dealing with RF weapons clearly documented the worldwide interest in RF weapon technologies. A few of the report's key issues as testified by Dr. IW Merritt, Lt Gen Robert Schweitzer and others to JEC, USA are as follows [151,155,188,189,190,191,192,193,194,195,197,199,200,201]:-

- "...construction of effective explosively-driven Flux Compression Generator devices is entirely feasible for established military powers such as Russia, China, France, Germany, et cetera,..."
- "there are programs underway addressing assessments and survivability, electromagnetic effects and hardening, RF source components and weapons applications".
- "There is no confirmed evidence of employment of such a device to date available in open sources".
- "Modern Metal Oxide Semiconductor technology, on which most of our critical national infrastructures depend, unless deliberately protected or "hardened", is extremely vulnerable to even low-power electromagnetic pulses..."
- "...it is well understood that the IT advanced nations are disproportionately more vulnerable to RF attack than the less developed nations."
- Following Russian origin devices are known to be capable of being used for RF weapon purposes
 - Magneto Hydrodynamic Generator of Frequency (MHHDGF)
 - Explosive Magnetic Generator of Frequency (EMGF)
 - Implosive Magnetic Generator of Frequency (IMGF)
 - Cylindrical Shock Wave Source (CSWC)
 - Spherical Shock Wave Source (CSWS)
 - Ferromagnetic Generator of Frequency (FMGF)
 - Superconductive Former of Magnetic Field Shock Wave (SFMFSW)
 - Piezoelectric Generator of Frequency (PEGF)
 - Superconducting Ring Burst Generator (SCRBG)
- The schematic arrangement of packaging an EM weapon is shown in the figure 7.5 [41].

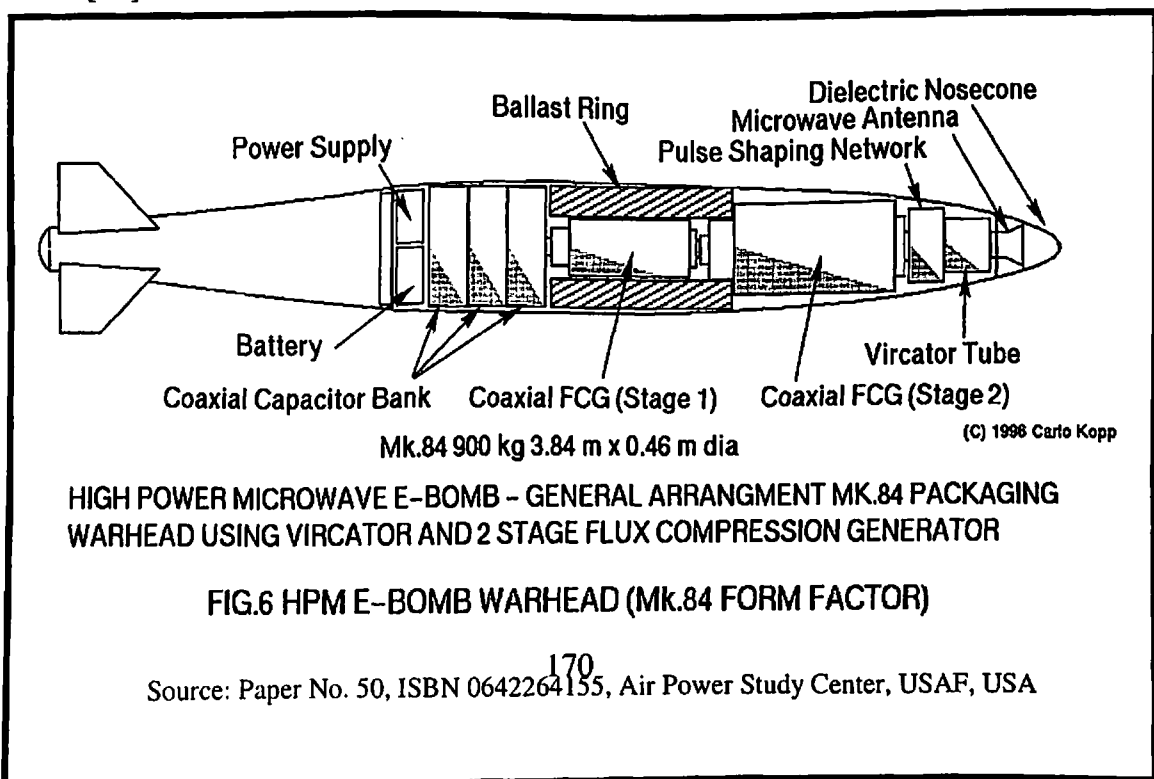


Figure 7.5: HPM E-Bomb Warhead (MK. 84 Form Factor)

- The EM weapons believed to be packaged as deliverable payloads by DOD, USA are shown in figure 7.6.

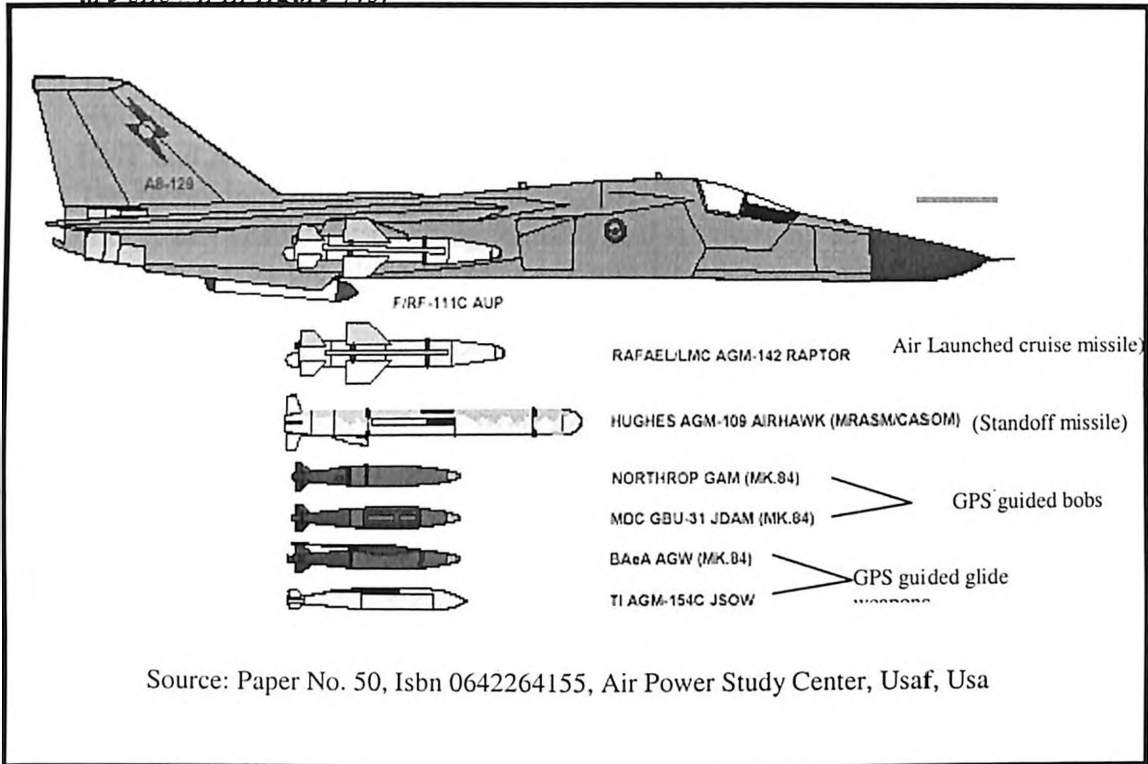


Figure 7.6: Comparison Of Standoff, Free-Fall And Glide Weapons

7.10 Conclusion

In this chapter we have concluded that high power EM device technology in a directed energy role has immense potential for military use, in both offensive and defensive postures. Its applications can be developed for missiles, artillery, unmanned Aerial Vehicles (UAVs) etc. The high power microsystems can become effective defense against stand off cruise missiles and stealth technology. The device technology, systems engineering, packaging and support process framework for large-scale weapon program exists with USA, Russia, China and some other countries. The operational systems are expected to enter services by 2015.

It has also emerged that there is an increasing variety of equipment capable of generating very short RF pulses that are capable of disrupting sophisticated electronics. These pulses are not addressed by current design standards and will challenge existing front-end RF protection and other forms of EMI protection. New capabilities are needed to reject high-power, very-fast RF pulses and to minimize their effects on systems. Also the common EMI and EMP mitigation techniques hitherto available will not provide adequate protection against nanosecond and sub-nanosecond pulses generated by future radio frequency weapons, since active mitigation device response times are typically several nanoseconds to microseconds. Faster solid-state devices do

not have the high power capability needed to protect systems from RF weapons pulses. Therefore as of now it is not possible to precisely quantify the risk presented by radio frequency weapons. But it is clear and certain that the risk is growing. Through the research efforts we can respond to this risk by developing near-term, low-cost, broadly applicable mitigation techniques. These techniques can reduce susceptibility to radio frequency weapon environments and thereby reducing the risk to NII.

The analysis in chapter 6 & 7 has further established the following:-

- The embedded electronics in computing, networking and communication systems in civil and military are extremely vulnerable to disability, damage or destruction by EMP and RF energy weapons
- The technology underlying the design, development and production of EMP and RF energy devices is fast reaching maturity and is emerging as the core of EM weapons program across the globe. These EMP and RF energy weapons are being recognized as "the Nuclear weapons of Information Age" and have national security dimensions for all countries across the globe.
- Several high power microwave technologies have matured to the point where they are now ready for transition from engineering and manufacturing development to deployment in strategic and operational missions for the Armed Forces.
- Microwave weapon systems offer prospect of significant offensive and defensive capabilities and are unique to possess "D5" capabilities viz deny, disrupt, damage, destroy and defend, They offer distinctly a new method of war.
- Microwave weapons don't rely on exact knowledge of enemy, they leave persisting and lasting effects on victim systems, affect enemy systems even when they are turned off. The enemy must harden the entire system to ensure protection against microwave weapons.
- Considering India's economic, social, political and military interests in the context of internal as well as national security, the development of IW capability with EMP and RF energy weapons is inevitable.
- Based on the above analysis, EMP and RF energy weapons development requirements, strategy and program is presented in chapter 8.

PART- IV
DEVELOPMENT OF IW CAPABILITY AROUND EMP
& HPM ENERGY WEAPONS

CHAPTER 8: DEVELOPMENT OF EM WEAPONS

CHAPTER 9: PACKAGING INDUCTION AND DEPLOYMENT OF EM WEAPONS

CHAPTER 10: RESEARCH & DEVELOPMENT NEEDS OF THE EM WEAPONS PROGRAM

CHAPTER 8

EVELOPMENT OF EM WEAPONS

8.1 Introduction

In the previous chapters we have examined the vulnerability of electronic and electrical systems when they are exposed to nuclear or non-nuclear EMP and RF energy. Over a wide range of frequencies we have also examined the techniques of coupling the EMP and HPM in to different types of target sets such as computing resources, communication systems, power lines etc. to cause maximum damage. We have seen how EM energy can be packaged as a weapon for various roles. We have examined the work underway globally for the development of EMP and RF energy weapons. It has emerged that microwave technologies have matured to a point where they are now being transitioned into operational systems in USA, Russia and China. We have also analyzed that given India's situation in politics, economy, social psychology, foreign affairs, geography and military needs, its information and information infrastructure has great impact on the security of entire country and is extremely vulnerable to attacks by enemy using these EMP and RF energy weapons. The conclusion therefore is that development of IW capability around EMP and RF energy weapons by India is inevitable.

This chapter examines the threat perception in the emerging cyber world, the operational requirements of EM weapons to counter it, mapping EM weapons into existing systems of the Armed Forces and development of technology to realize them. It is also examines the basic building blocks of EM weapons, their constructional features, packing into deployable configurations and linking to various roles in defensive and offensive postures. It also presents an approach to pool together existing infrastructure in the Armed Forces, Defence Research and Development Organisation (DRDO), institutions and the industry to draw up a comprehensive IW capability. It suggests that India possesses IT infrastructure and software expertise, which should be leveraged for simulation, virtual prototyping and testing of EMP & RF weaponry concepts, doctrines, IW force structures to cut down effort, expense and time, so that we can be in league with the developed world in this vital area.

8.2 Threat Perception

The economic and military superiority in future would be based on microelectronics since they form the core of our National Information Infrastructures including the offensive and defensive systems of the Armed Forces and other national security agencies. To prevail against us, an adversary must cripple, destroy or deny access to these microelectronics based systems. Can an adversary do so? Very likely, as we have discussed in previous chapter. The military doctrines being evolved for the Information-Age-Warfare foresee extensive use of sophisticated electronics and communication systems to ensure information dominance and overwhelming battlefield success. Because the battlefield success and the well being of the civilian economy are so dependent upon the microelectronic-based systems, we need to fully understand any technology that might be used to defeat these systems. This is particularly true of the newly emerging threat of EMP and RF energy weapons. And even more importantly, we need to develop

countermeasures before such weapons are used against us. The opportunity window to develop such a capability lies from now to the year 2015. This intent is supported by the HPM initiatives of USA [45].

There are two ways, the EM Weapons can invade us. An EMP pulse generated in the event of a nuclear exchange and detonation of a non-nuclear EMP device in the frequency ranges of interest. As a practical matter, a piece of electronic gear on the ground, in a vehicle, ship or plane does not really care whether it is hit by a nuclear magnetic pulse or a non-nuclear one. The effect is the same. It burns out the electronics. The same is true of the computers in every part of the NII. There is another way these weapons can be delivered to a target, military or civilian. Here the term, EM munitions, or EFM is used. These are called RF weapons. These small munitions contain high explosives that produce radio frequency energy as their primary kill mechanism. These munitions can be hand grenades, mortar rounds, or large artillery shells or missiles. They produce a short but very intense pulse. Thus EMP and RF energy weapons put together pose a very serious threat to our national security.

8.3 Scoping of the Solution Strategy

As we have seen in the previous chapters, target of these attacks can be the national telecommunications systems, power grid, air, surface and sea transportation systems, mass media, oil and gas control and refining infrastructure, manufacturing industry, public works, civil emergency services, finance and banking systems, health care, insurance etc.

As of now, we neither fully understand nor control EM technology. We have not yet begun to work on defenses, especially for our information vulnerable infrastructures. We need to first scope the problem, determine susceptibilities and vulnerabilities, and then test. All of this, including hardening of existing components, which will take considerable effort and expenses need to be addressed. There are other courses of corrective action, but all will take time to acquire and apply. The first step will be to bring together our expertise in Electromagnetics from Department of Defence Research & Development (DRDO), Department of Defence, Indian Space Research organisation (ISRO), Department of Atomic Energy (DAE), Power sector RD & D units and the research community from institutions and industry. The Armed Forces need to examine the entire issue in strategic and tactical context, taking into account threat perception of next 25 years, major development programs underway and the shape, size of our deterrence posture, integration of IW as a new element of warfare in and access the force structure. The internal security agencies, civil deference organizational critical infrastructure protection agencies etc. need to step in from their perspective. Targeting the humans with Directed Energy Weapons is an extremely critical issue for containing terrorism, therefore law enforcement should be involved deeply. In this thesis the EMP and RF energy weapons are being examined only from a national security perspective. However this analysis is equally applicable to internal security issues. This will help us to gauge the problem and identify solutions and directions. The analysis in this and previous chapter provides the baseline inputs for scoping the solution strategy.

8.4 Operational Requirements

As far as possible the EMP and RF energy weapons should offer one to one replacement features for the existing conventional weapons so as to seamlessly integrate them into our existing inventories and support infrastructure. At broad level these capabilities pertain to countering artillery fire, ship defense against missiles, self-protection of air craft and similar other platforms, suppression of enemy integrated air, surface and sub surface defense systems, air space control, counter-proliferation, denial, disability, disruption, destruction and defence of command and control infrastructure. The systems should be developed with focus to exploit following added advantages offered by the EMP and RF energy weapons [5,68]

- Instantaneous engagement times and effectiveness on detonation at speed-of-light
- All-weather attack capability on the enemy electronic systems
- Area coverage of multiple targets with minimal prior information on threat characteristics
- Ability to launch surgical strikes (disable, damage, disrupt, degrade, destroy) at selected levels of combat
- Non-lethal and / or less lethal to human beings. Therefore offering minimum collateral damage in politically and socially sensitive environments
- Simplified pointing and tracking
- Reusable and deep magazines. The weapon should be able to fire or pulse as long as there is power in the generator
- An unfailing defence against enemy attacks using EMP and RF energy Weapons at our military and civil information infrastructures
- Suitable for deployment in covert operations. The firing of EMP and RF energy weapons should not leave any signature so that their use can be denied in the event of certain geopolitical situations
- Difficult to detect. Silent when used without explosive devices
- Low operating costs and simplified logistics
- The US Airforce Research Laboratory had Commissioned a study in 1998 which identified precision -guided munitions, large aircraft shield for self protection, small aircraft shield for self protection and unmanned Compact air vehicles as focus areas in phase - I, which were further studies. The core-operational competencies projected by the US Air Force using HPM weapons is shown in figures 8.1 we need to examine our requirements keeping similar perspective in view

Core Competencies	Advantages to Microwave Weapons
Air Space Superiority	<ul style="list-style-type: none"> • Deny, degrade, and destroy enemy electronic systems. • Provide rapid force deployment. • Neutralize enemy response.
Global Attack	<ul style="list-style-type: none"> • Speed of light, all-weather electronic attack. • Enable dynamic force employment. • Enhance security of operations.
Rapid Global Mobility	<ul style="list-style-type: none"> • Improved air and ground force protection. • Non-lethal, long range denial option. • Aircraft self-defence capability.
Precision Engagement	<ul style="list-style-type: none"> • Precise / selective electronic attack. Minimum collateral damage and casualties. • Non-lethal weapon force protection.
Information Superiority	<ul style="list-style-type: none"> • Deny enemy situational awareness. • Protect friendly systems.
Agile Combat Support	<ul style="list-style-type: none"> • Protect deployed forces with minimal logistics. • Light-weight systems and small fuels requirements.
<p>Source: OP11, Feb 2000, Air University Alabama, USA, by Col. E M Walling. Figure 8.1: USAF Core Competencies and High Power Microwaves</p>	

8.5 Building Blocks and Technology Base for EMP and RF Energy Weapons

To construct a non-nuclear EMP and RF energy weapon, the basic requirement is to build a device capable of generating very large amount of EM energy very quickly and deliver it to a set of targets. Following types of devices form the basic building blocks for a weapon program [68,167].

- Explosively Pumped Flux Compression Generators (FCG). They serve as a power source.
- Explosive or Propellant Driven Magneto-Hydrodynamic (MHD) generators; also to serve as power source.
- A range of High Power Microwave (HPM) devices, the foremost of which is the Virtual Cathode Oscillator or Vircator for conversion of low frequency power into microwave energy.
- Antenna System

A Development Roadmap for development of operational applications, and hardening of equipment vulnerable to EMP and RF energy weapons is outlined in the succeeding paragraphs.

8.6 Construction of EM Weapons

Typical narrowband HPM devices have three components: a pulsed power source that releases stored energy as a fast (~ nsec to msec) applied voltage, a beam/cavity interaction region where the beam's kinetic energy is transformed to microwave radiation, and an antenna that directs the radiation. These components are distinct in their density of charged particles. Specifically, pulsed power devices often involve high-density plasmas, beam/cavity sources have a low density of charged particles, and antennae ideally have no charged particles.

The design of an HPM device that provides the required power and effectively radiates EM waves presents difficult challenges. Complex and expensive experimental efforts are more timely and cost-effective if they are guided by theoretical and computational modeling. The required modeling is based on Maxwell's equations, the Navier-Stokes compressible fluid equations, and the Lorentz Force law. Analytical solution of the resulting system of nonlinear partial differential equations is intractable. Furthermore, numerical solution requires fine-grained resolution in both time and space. Thus, modeling and simulation, which is critical to timely development, is computationally intensive. Such computations are made tractable by viewing the device as a system consisting of a pulsed power source, a microwave source, and an antenna as shown in the figure 8.2. Each of these components has an important, distinguishing characteristic that facilitates its simulation using the software [66].

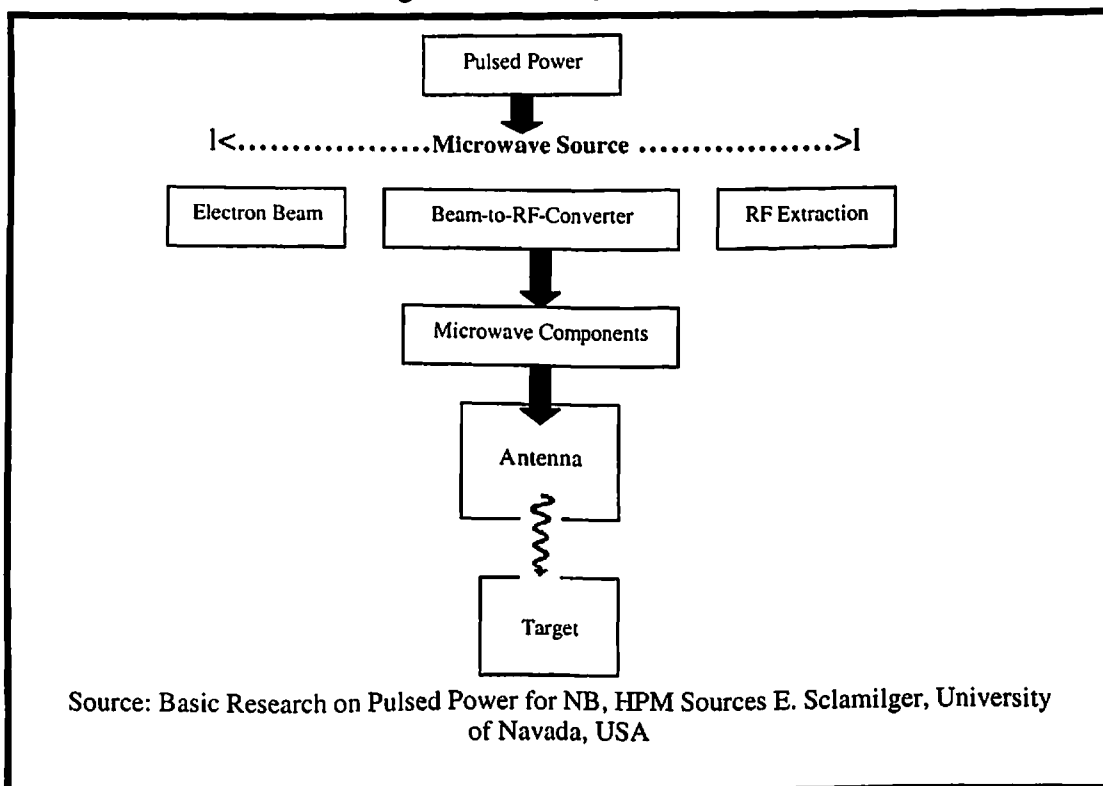


Figure 8.2: Components of EM Weapons

8.6.1 Pulsed Power Source

- The pulsed power source converts low power stored energy into a high power electrical pulse as shown in figure 8.3.

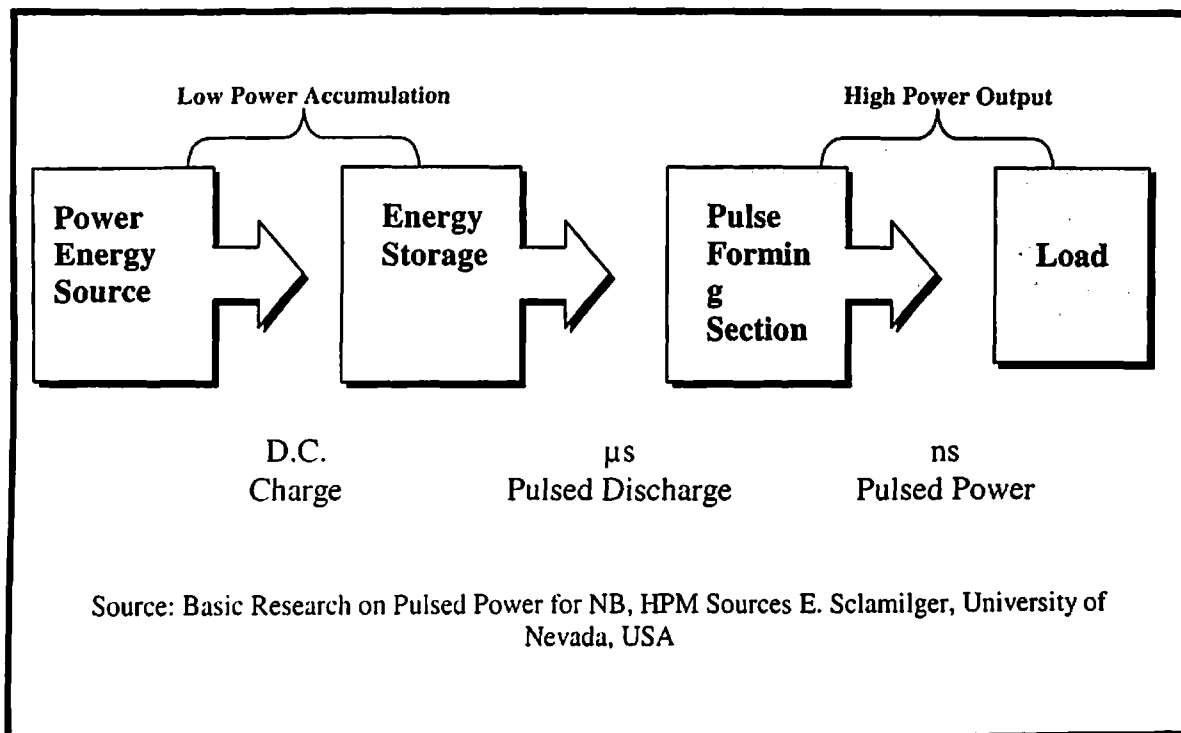


Figure 8.3: Generation of High Power Pulse.

- Stored energy can be as high as a kiloJoule, with power in the gigawatt range. The typical pulsed power needs projected by the DoD, USA for the EM weapons are shown figure 8.4 and they vary from 10KJ electrical energy to 100 MJ which corresponds to peak power in megawatts to gigawatts range [67].

S.No.	System Types Parameters	Electrical Energy	Pulse Length	Peak Pulse Power	Burst avg. power
1.	High power microwave	10 kj	100 ns	100G W	100 kW
2.	(Ultra Wideband HPM systems)	10 j	1 ns	10 GW	10 kW
3.	(Practical beam self-protect)	100 j	1 us	1 GW	10 kW
4.	Electro - thermal chemical gun	1 MJ	10 ms	0.1 GW	1 MW
5.	Dynamic armor	1 MJ	1 ms	1 GW	1 MW
6.	Electromagnetic gun (rail and coil)	100 MJ	10 ms	10 GW	100 MW
7.	Electromagnetic launch and recovery	100 MJ	1 s	100 Mw	1 MW

Source: Slide 5, CP3, MURI Program. University of New Mexico, USA, Oct. 02.

Figure 8.4 : Pulsed Power Needs for DoD, USA

- The concept used in several designs is explosively driven magnetic flux compression. One device based on this concept is the helical magneto-cumulative generator (MCG). In this device, a modest initial magnetic field is compressed by high explosive. Because of the conservation of magnetic flux (magnetic field integrated over a surface area), the magnetic field increases as its cross-sectional area decreases. Thus, the kinetic energy of the explosive material induces a fast-rising electrical pulse in an attached load. The efficiency of the process increases with reduced flux losses (e.g. magnetic diffusion, geometrical detachment, and electrical breakdown), which typically requires increased geometrical complexity.

8.6.2 HPM Source

The electrical pulse created by the pulsed power source is applied to a diode to create a high energy (~400 kV), high current (70-60 kAmp) beam of electrons. Although the configuration for the diode region varies widely from source to source, the principle is the same. The beam of electrons created in the diode region then interacts with the structure of the cavity and energy is transferred from the kinetic energy of the beam to EM energy in the existing modes of the cavity (preferably in a single desired mode). Finally, the beam is collected in a beam dump and the microwaves are extracted from the cavity. The HPMs sources most commonly described in the open literature and used for configuring RF energy weapons are referred as Flux Compression Generators (FCG), Magneto Hydro Dynamic (MHD) Generator and High Power Microwave (HPM) Devices. Their constructional details and features are described in the succeeding paragraphs.

8.6.3 Flux Compression Generators (FCG)

- In principle, any device capable of producing a pulse of electrical current of the order of tens of kilo Amperes to Mega Amperes will be suitable for end use in EMP weapons. The FCG's falls under this category.
- The central idea behind the construction of FCG's is that of using a fast explosive to rapidly compress a magnetic field, transferring most of the energy from the explosive into the magnetic field. A start current produces the initial magnetic field in the FCG prior to explosive initiation. The start current is supplied by an external source, such as high voltage capacitor bank (Marx bank), a smaller FCG or a MHD device. A number of geometrical configurations for FCGs have been published. The most commonly used arrangement is that of the coaxial FCG. The coaxial arrangement is of particular interest in this context, as its essentially cylindrical form factor lends itself to packaging into munitions. The X-Ray image of FCG constructed under the MURI project at Texas University, USA is shown in figure 8.5 [67].

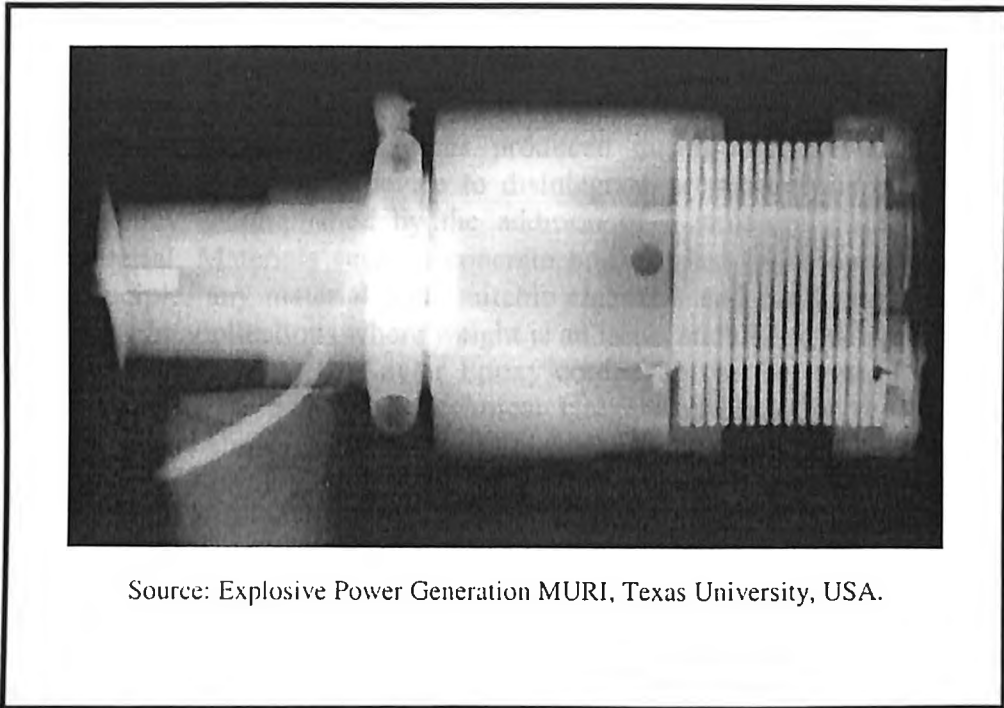


Figure 8.5: X-ray image of Flux Compression Generator

- In a typical coaxial FCG, a cylindrical copper tube forms the armature. This tube is filled with a fast burning explosive. A number of explosive types have been used, ranging from B and C-type compositions to machined blocks of PBX-9507 used by US forces. The armature is surrounded by a helical coil of heavy wire, typically copper, which forms the FCG stator. The stator winding is in some designs split into segments, with wires bifurcating at the boundaries of the segments to optimize the electromagnetic inductance of the armature coil. The construction details of a FCG (as described by Carlo Kopp and in a number of IEEE papers) are given in Figure 8.6 [39,41].

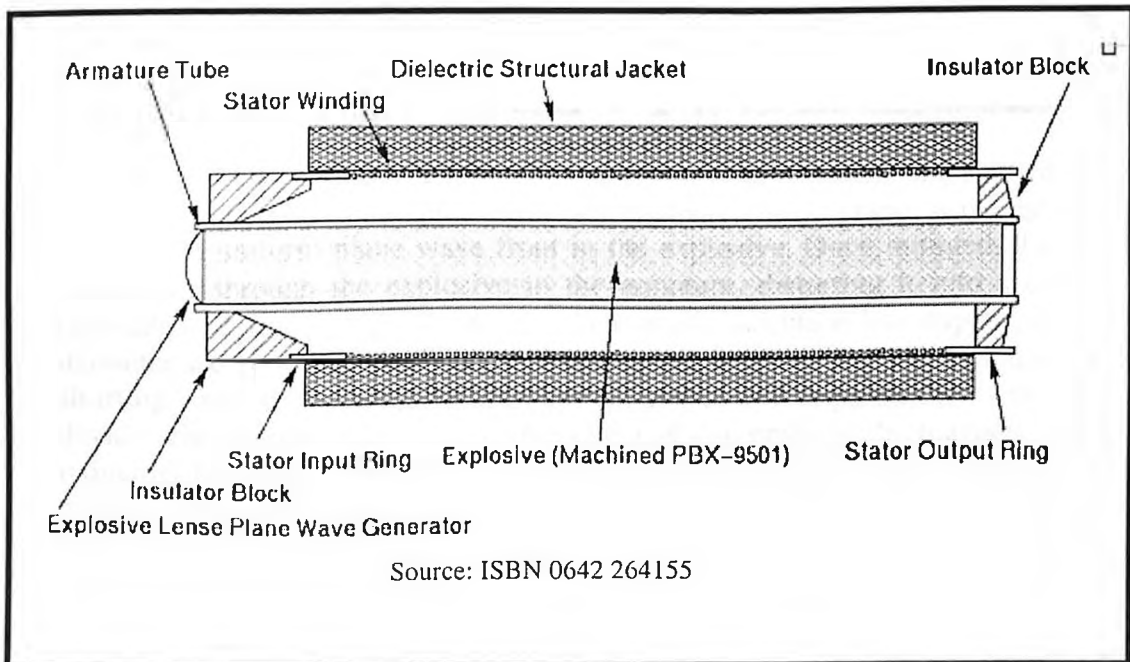


Figure 8.6: Constructional Details of FCG

- The intense magnetic forces produced during the operation of the FCG can potentially cause the device to disintegrate prematurely if not dealt with. This is typically accomplished by the addition of a structural jacket of a non-magnetic material. Materials such as concrete or fiberglass in an epoxy matrix are used. In principle, any material with suitable electrical and mechanical properties could be used. In applications where weight is an issue, such as air delivered bombs or missile warheads, a glass or Kevlar Epoxy composite can be used. The details of a FCG developed by the Texas Technical University, USA for the DOD, USA project MURI are shown in figure 8.7 [67].

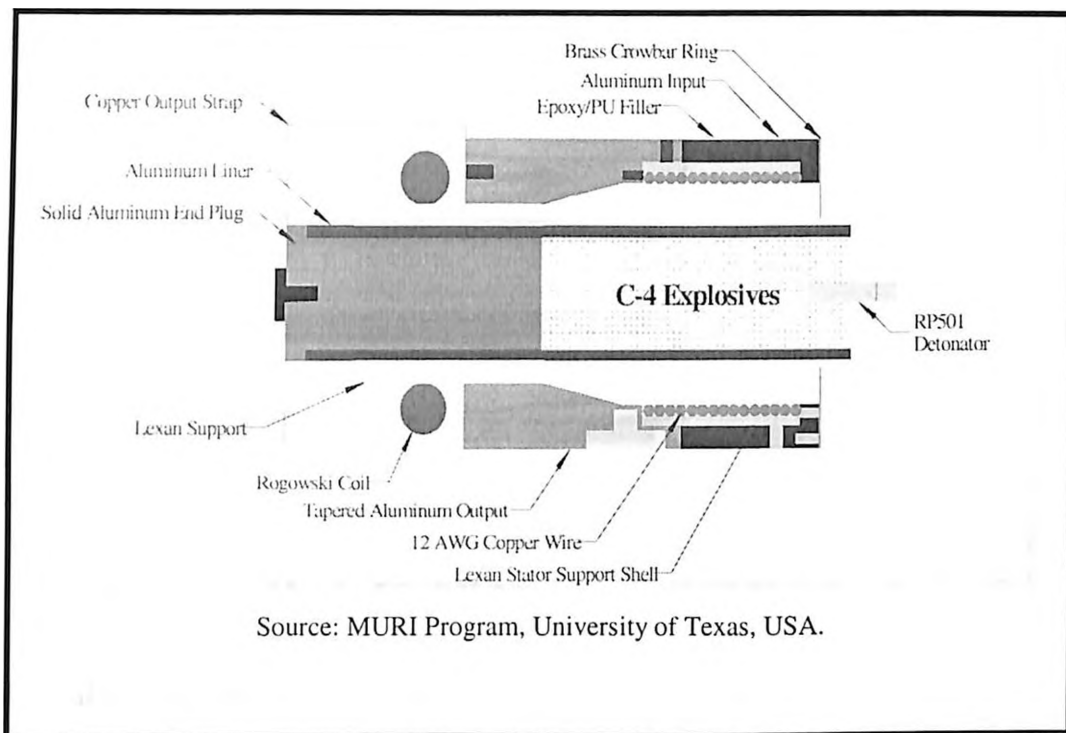


Figure: 8.7 Components of a FCG

8.6.3.1 Principle of Operation of FCG: The explosive is ignited when the start current peaks. This is usually accomplished with an explosive lens plane wave generator that produces a uniform plane wave front in the explosive. Once initiated, the wave front propagates through the explosive in the armature, distorting it into a conical shape (typically 72 to 74 degrees of arc). Where the armature has expanded to the full diameter of the stator, it forms a short circuit between the ends of the stator coil, shorting and thus isolating the start current source and trapping the current within the device. The propagating short has the effect of compressing the magnetic field, whilst reducing the inductance of the stator winding. The result is that such generators will produce a ramping current pulse, which would peak before the final disintegration of the device. Published results suggest ramp times of tens to hundreds of microseconds, specific to the characteristics of the device, for peak currents of tens of Mega Amperes and peak energies of tens of Mega Joules. The Sequence of Flux compression is as follows and is also illustrated in figure 8.8:

- External start current applied to FCG winding

- When start current peaks, explosive lens is fired which in turn initiates burning of explosive charge.
- Armature expands due to explosive pressure and creates moving short circuit
- Moving armature compresses magnetic field resulting in a pulse

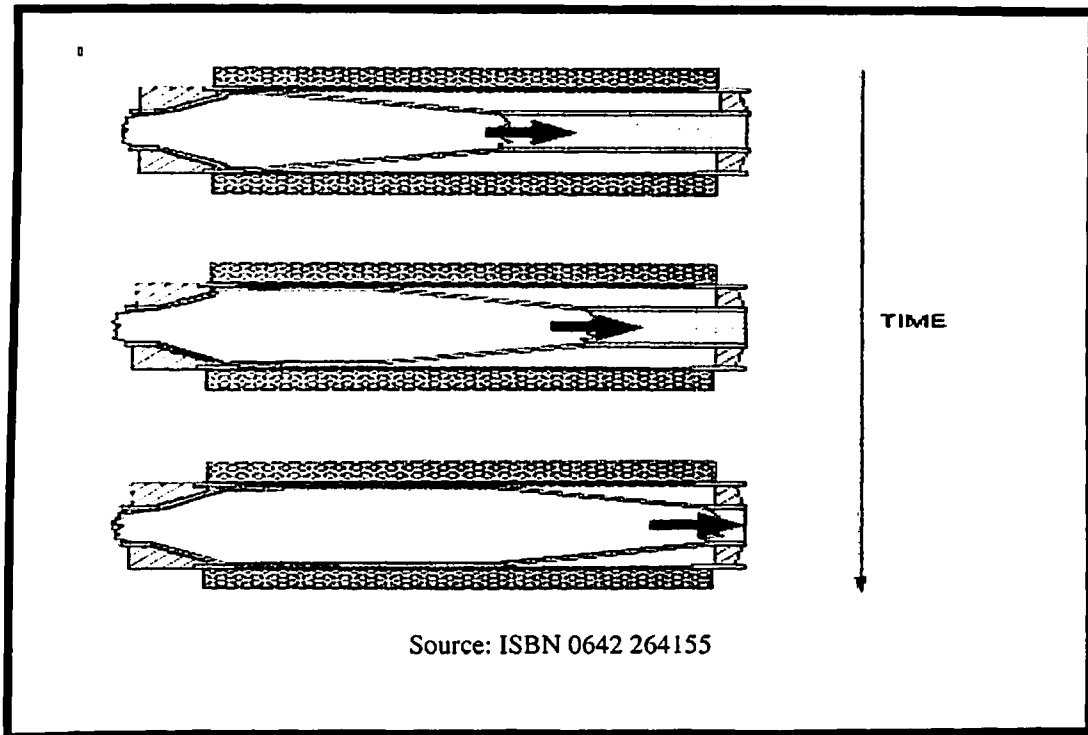


Figure 8.8: Sequence of Flux Compression

8.6.3.2 Amplification and Pulse Shaping: The current multiplication (i.e. ratio of output current to start current) varies with designs, but numbers as high as 60 have been demonstrated. In a munitions application, where space and weight are at a premium, the smallest possible start current source is desirable. These applications can exploit cascading of FCGs, where a small FCG is used to prime a larger FCG with a start current. Experiments have demonstrated the viability of this technique. The electric model of the above mentioned FCG developed is shown in figure 8.9 and its computed and measured current ratings are shown in figure 8.10. The Texas Technical University, USA, under the MURI project has successfully developed these FCGs and validated their designs through simulation studies.

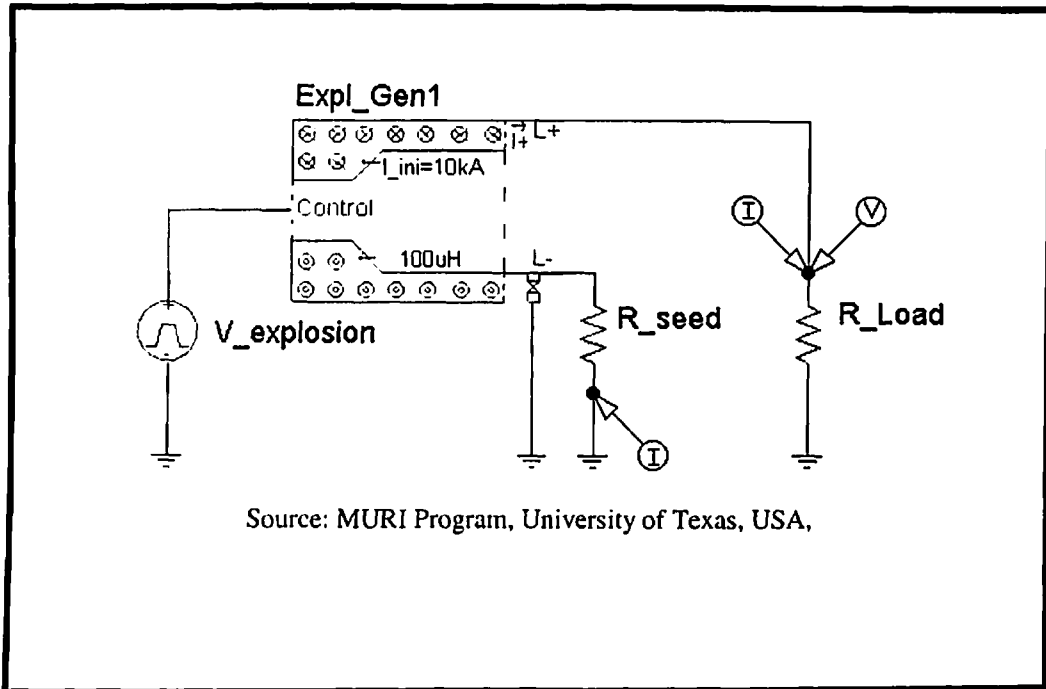


Figure 8.9 Electric model of Flux Compression Generator

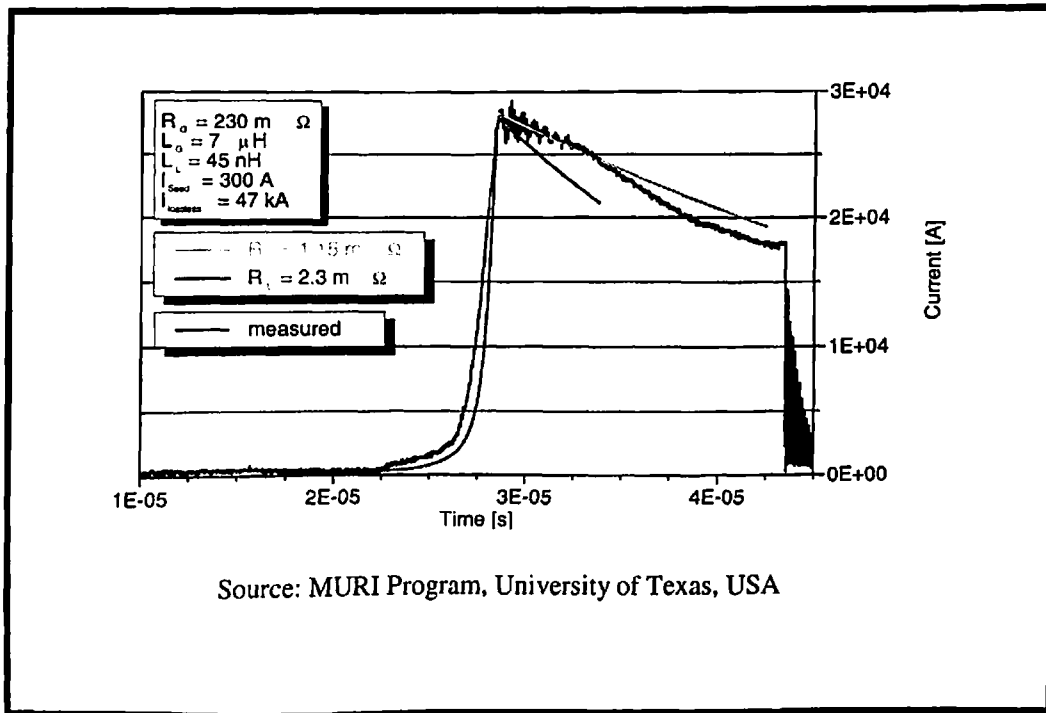


Figure 8.10: Generator current output, measured and calculated

8.6.3.3 Adapting FCG to EMP Weapon Program: The technical issues in adapting the FCG to EMP weapons applications lie in packaging, supply of start current, and matching the device to the intended load. Interfacing to a load is simplified by the coaxial geometry of conical FCG designs. This geometry is convenient for weapons applications, where FCGs may be stacked axially with devices such a microwave Vircators. The demands of a load such as a Vircator, in terms of waveform shape and

timing, can be satisfied by inserting pulse shaping networks, transformers and explosive high current switches. This can make it potentially viable for making laser-guided bombs, missiles in different variants, torpedoes etc. In India, the agencies under the aegis of Integrated Guided Missile Development Program (IGMDP) have the potential to adapt this type of FCG's for EM weapon program. Similarly, the Naval Scientific and Technological Laboratory (NSTL) can examine it for use in under-water applications where torpedoes for anti-ship role or targeting electronics of oil platforms etc. can be used.

8.6.3.4 Limitations of FCG: The literature suggests that pulses generated by FCGs are in the frequency spectrum of 7MHz and below. An EM weapon built around such devices cannot be used against a large spectrum of targets, even if power levels are enhanced. Secondly, the energy spread is too large. However this is an area where more refinements and directed research need to be undertaken

8.6.4 Magneto Hydrodynamic (MHD) Generators

- The fundamental principle behind the design of MHD devices is that a conductor moving through a magnetic field will produce an electrical current transverse to the direction of the field and the conductor motion. In an explosive or propellant driven MHD device, the conductor is a plasma of ionized explosive or propellant gas, which travels through the magnetic field. Current is collected by electrodes, which are in contact with the plasma jet.
- The electrical properties of the plasma are optimized by seeding the explosive or propellant with suitable additives, which ionize during the burn. Published experiments suggest that a typical arrangement uses a solid propellant gas generator, often using conventional ammunition propellant as a base. Cartridges of such propellant can be loaded much like artillery rounds for multiple shot operation.
- The design of explosive and propellant driven Magneto-Hydrodynamic generators is much less mature than that of FCG design. Technical issues such as the size and weight of magnetic field generating devices required for the operation of MHD generators suggest that MHD devices will play a minor role in the near term. In the context of this discussion, they are suitable for start current generation for FCG devices.

8.6.5 High Power Microwave (HPM)

The physics of the HPM devices or Vircator tube is substantially more complex than those of the FCG and MHDs. The fundamental idea behind the Vircator is that of accelerating a high current electron beam against a mesh (or foil) anode. Many electrons will pass through the anode, forming a bubble of space charge behind the anode. Under proper conditions, this space charge region will oscillate at microwave frequencies. If the space charge region is placed into an appropriately tuned resonant cavity, very high peak powers may be achieved. Conventional microwave engineering techniques may then be used to extract microwave power from the resonant cavity. Because the frequency of oscillation is dependent upon the electron beam parameters, Vircators may be tuned or chirped in frequency, where the microwave cavity will support appropriate modes. Power levels achieved in Vircator experiments range from 770 kilowatts to 40

GigaWatts over frequencies spanning the decimetric and centimetric bands of frequencies. The typical spectral energy density of radiation is shown in figure 8.11.

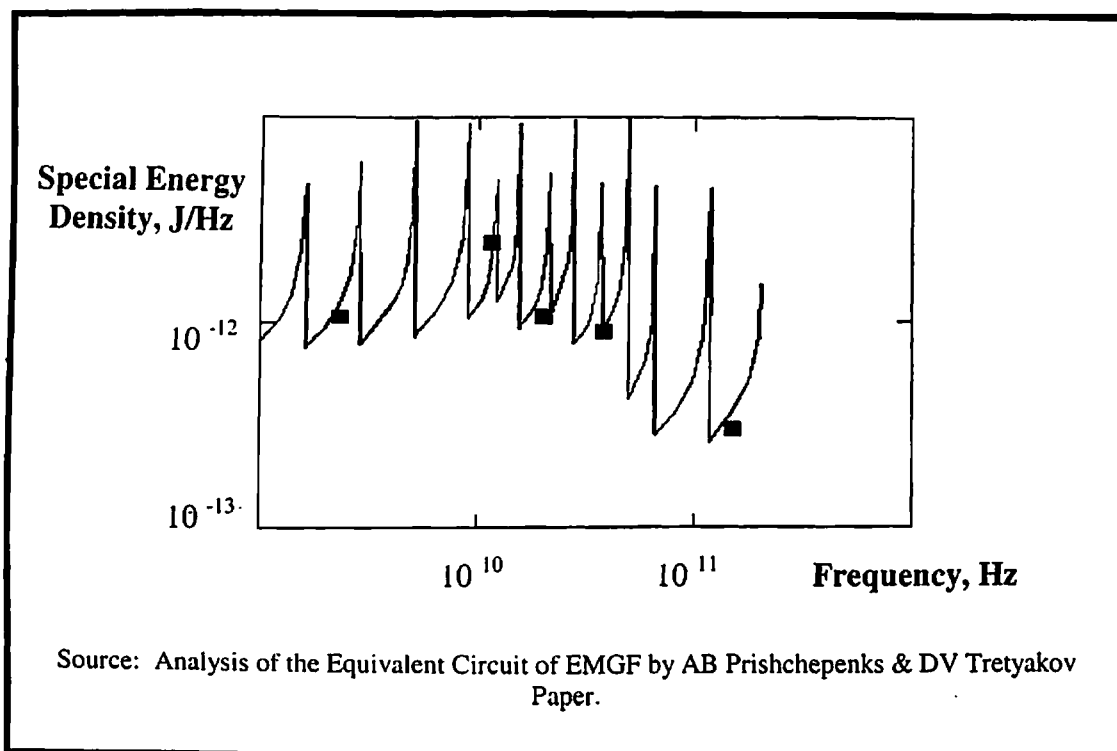


Figure 8.11: Spectral Energy Density of Radiation.

8.6.5.1 HPM Sources - The Vircator

These are all examples of the available technology base. From the perspective of a bomb or warhead designer, the device of choice will be at this time the Vircator, or in the nearer term a Spark Gap source. The Vircator is of interest because it is a one shot device capable of producing a very powerful single pulse of radiation, yet it is mechanically simple, small and robust, and can operate over a relatively broad band of microwave frequencies. The principle of operation and characteristics of a Vircator are summarized as follows:-

- Conductor moving in magnetic field produces an electrical current
- Direction of current is transverse to the direction of field or motion
- Relativistic electron beam punches through the foil mesh anode
- Virtual Cathode function
- Peak power in Giga Watts
- Anode melts down 0.7 micro sec approx.
- Simple construction
- Cost effective
- Chirping of oscillations due to wide band-width

8.6.5.2 Types of HPM Devices Developed

Some of the HPM devices known to exist in the market are as follows:-

- Relativistic Klystrons
- Magnetrons
- Slow Wave Devices
- Reflex Triodes
- Spark Gap Devices and Vircators

8.6.5.3 Construction of HPM Device

The two most commonly described configurations for the Vircator are the Axial Vircator (AV), and the Transverse Vircator (TV). The Axial Vircator is the simplest by design, and produce best power output in experiments. It is typically built into a cylindrical wave guide structure. Power is most often extracted by transitioning the waveguide into a conical horn structure, which functions as an antenna. AVs typically oscillate in Transverse Magnetic (TM) modes. The Transverse Vircator injects cathode current from the side of the cavity and will typically oscillate in a Transverse Electric (TE) mode. Figure 8.12 and 8.13 show schematic arrangement for AV types of HPM devices and their pulse generation [39, 205].

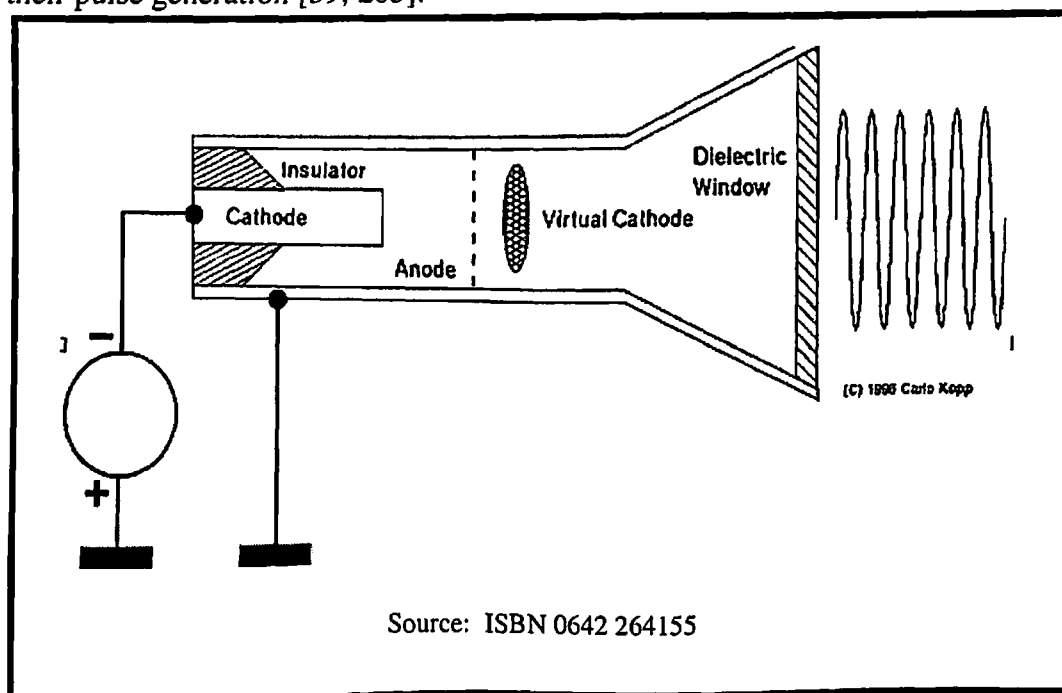


Figure 8.12. : Constructional Details of Axial Vircator

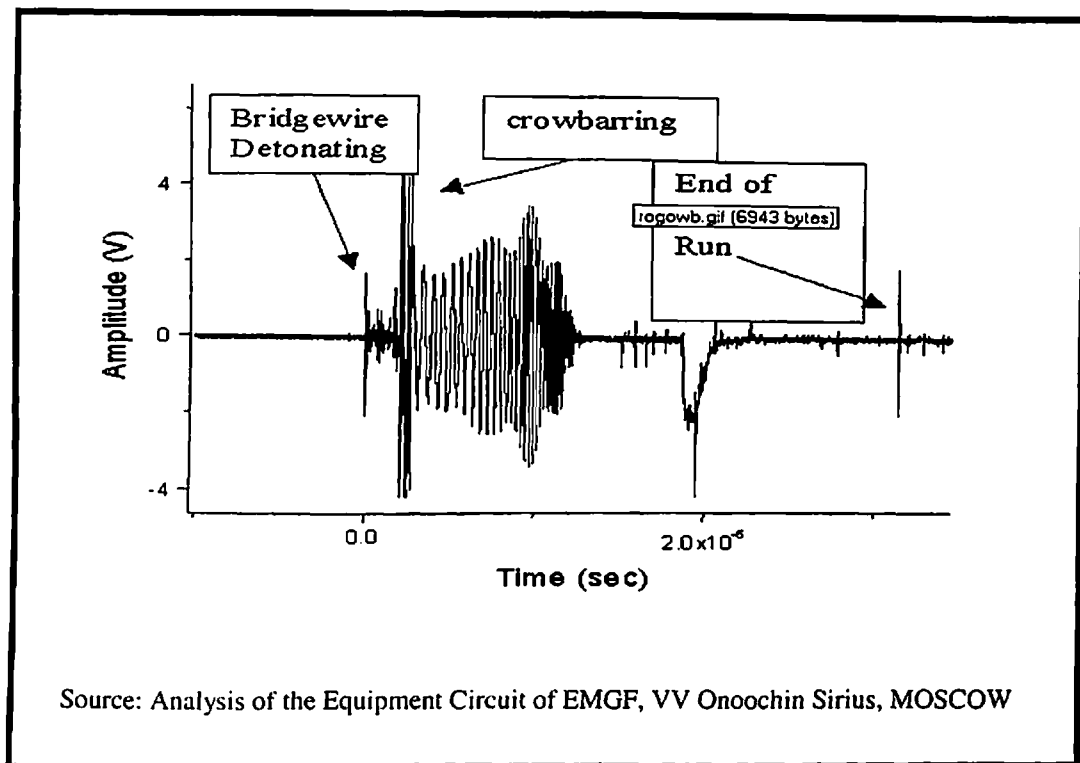


Figure 8.13: Current in the Coil of the EMGF

8.6.5.4 Design Issues

The technical issues in Vircator design are as follows:-

- **Output Pulse Duration:** This is typically of the order of a microsecond and is limited by anode melting.
- **Stability of Oscillation Frequency:** This is often compromised by cavity mode hopping.
- Low conversion efficiency
- Less power output
- There are difficulties in coupling power efficiently from the Vircator cavity in modes suitable for a chosen antenna type. This is because of the very high power levels involved, which can cause electrical breakdown in insulators.

8.6.6 Suitability of FCG's and HPM Devices for EMP and RF Energy Weapons

Whilst FCGs are potent technology base for the generation of large electrical power pulses, the output of the FCG is by its basic physics constrained to the frequency band below 7 MHz. Many target sets will be difficult to attack even with very high power levels at such frequencies. Moreover, focusing the energy output from such a device will be problematic. A HPM device overcomes both of the problems, as its output power may be tightly focused and it has a much better ability to couple energy into many target types and therefore emerges as a preferred choice for making EM weapons. The details of development of HPM based systems in USA under the following programs are given in the notes 1,2,3.

- WE.19.08 HPM Aircraft Self - Protect Missile Countermeasures
- WE.22.09 HPM C2W / IW Technology
- WE.23.08 HPM Modem Network Command and Control Warfare Technology

8.7 Development Objectives & Time Frames

Technology development and demonstration should be oriented to establish a short, medium and long term, mature and comprehensive program for development and integration of microwave sources, pulsed power supplies and antenna systems. A suggested development profile is presented in figure 8.14 [39, 45,150].

Weapon System	Mid-term (4-6 years)	Long-term (7-10 years)
Point Defense System against missile threat.	Demonstration of live fire cable-car. Field demo of high average power narrowband source.	Demonstration of Ship-self-defense system. Demonstration of Counter munition.
Command & Control Warfare / Information Warfare	Field trials.	Airborne trials.
System for Disabling Air Defences.	Explosively driven single pulse device demonstration.	Multiple-pulse device trials.
System for Control of Air Space.	Modeling and simulation for concept development.	Field trials.
Source: Defence Technology Plan, DoD, USA Chapter 10 (Weapons) Figure 8.14: Suggested Development Roadmap		

8.8 Scope of Basic Research and Technology Demonstration

Basic research efforts for high power microwaves should emphasize the fundamental understanding of the limitations of microwave technology and its applications, and investigation of promising new approaches and concepts. Efforts should be devoted to develop RF sources, antennas, and pulsed power systems and investigation of RF effects on microelectronics.

8.9 Development Program

The organizations within the ministry of defence should have primary responsibility for the development and application of EMP and RF energy weapons technology. The private sector efforts can complement military programs. The Department of Atomic, certain power sector agencies and defence PSUs have development and testing programs, which can directly support Services efforts, while the private sector can evolve both independent and cooperative RF effects testing programs. Programs should be initiated to develop and transition improved techniques for measuring

electromagnetic interference. The electronics industry as a whole should work closely with the Services to ensure compliance with new international standards for electromagnetic protection.

In executing the program for development of EMP and RF energy weapons, focus should be maintained on specific technology demonstrations, in order that the technology effort at the component level can also be focused. The investments among the various technology demonstration and technology development efforts should be allocated in accordance with their potential payoffs to the Services needs and their relative contribution to achieving the goals.

8.9.1 The Demonstrations of Mission-Oriented Concepts

The USA defence services have pursued development programs for aircraft self protection, anti-ship missile defense, and counter munitions (EW Electronic Attack - degrade/neutralize enemy defenses); and Lethal Suppression of Enemy Air Defenses (SEAD) and C2W/IW (Precision Force, MOUT, and IW). Potential payoffs include generic protection against a wide variety of missile/ munition threats (IR, EO, RF, laser-guided), improved effectiveness and lower attrition rates of friendly systems, and negation (permanent damage, long-term disruption, and temporary degradation) of enemy command, control, and general information systems. The, electronic protection techniques are being developed under the HPM program and are continuously transitioned to users in order to harden NII systems against hostile HPM weapons or inadvertent EMI/EMC. Joint development and test projects to demonstrate the maximization of investments to meet individual Service requirements have been pursued. It is suggested that India should structure its EMP and RF energy weapons development program on these lines keeping local conditions in view.

8.9.2 Technology Development

Following should constitute the basic building blocks from the technology development perspective.[45,82,89].

8.9.2.1 Compact, High Power HPM Sources

Following specifications are being aimed under the US Programs

- Power exceeds 700 MW(> 700 GW possible).
- Pulse length (Cm-mm waves, 700 MHz-700GHz). This amounts to six-fold increase in narrow band pulse length as compared to existing devices available in USA. The narrow band tunability should be achieved up to an octave as compared to existing systems in conventional microwave industry based on solid-state electronics.
- Weight should be ~500 lbs and volume ~7.5 cu ft (exclusive of antenna and pulse power).
- The projected power rating, weight and frequency of devices to meet different end needs as projected by US, DoD are summarized in figure 8.4.

- 8.9.2.2 Compact, High Power, High Gain, Ultra-Wide Band Antennas:** 78 inch antenna diameter with approximately 75 - 20 db of antenna gain.
- 8.9.2.3 Compact, Efficient, High Power Pulse Power Drivers:** Development of compact (~500 lbs in less than 70 cu ft), high peak power (>50 GW) packages.
- 8.9.2.4 Study and Assessment of HPM Effects and Lethality:** This would includes the following: -
- RF testing of a wide range of air, sea, land, and air borne assets.
 - RF effects database development to provide reliable prediction of RF effects to permit extrapolation to other systems.
 - Development of innovative countermeasure techniques and incorporation of HPM into accepted military weapon engagement models.
 - Assessment of biological effects necessary to establish safety thresholds for personnel protection.
- 8.9.2.5 Integration with Existing Programs:** This would encompass integration of EMP and RF energy weapons into platforms such as fixed-wing and rotary wing aircraft, naval combatants, land vehicles, aircraft pods, unmanned aerial vehicles and munitions. The main components will be the pulse power drivers, HPM sources, and output antennas
- 8.9.2.6 Low Impact Hardening of Systems Against Hostile and Self-Induced EMI:** This will include following
- Transitioning EM hardening to users in response to existing EMI/EMC problems and projected threats.
 - Identifying susceptibilities in air, land, sea and other militarily critical systems, medical electronics, industrial controls and other components of critical NII.
 - Developing hardening countermeasures, which minimally impact system performance, cost or maintainability.
- 8.9.2.7 Evaluation of Additional Applications:** Based on effects assessments and technology development efforts, following should be undertaken
- Air Surveillance for Missile Defence (ASMD)
 - Counter-proliferation.
 - Counter-munition, and air space control

8.9.3 Technology Demonstration

- Platform Self Protection can pertain to existing air crafts, strategic and tactical nuclear assets, Light Combat Aircraft (LCA), Advanced Light Helicopter (ALH), Main Battle Tanks (MBT), Air Craft Carriers, supply ships or equivalent platforms to meet the needs of there Services.
- Command and Control Warfare/Information Warfare demonstration can include networking components (Switches, Routers, Servers, Command Shatters)
- Suppression of Enemy Air Defenses Demonstration.

8.9.4 System Level Development

In support of weapon system development or product improvements, there is a need to provide capability to perform weapon system analysis in the context of a realistic battlefield environment to include dynamic terrain, weather, obscuration (man-made

smokes, vehicular and high explosive dust, etc.), Command Control and Communications (C³) and Counter Measures (CM) and Counter Measures (CCM).

- Conduct weapon system munition configuration effectiveness/value-added analysis.
- Conduct weapon system-sensor mix effectiveness/value-added analysis.
- Conduct direct-fire / indirect-fire lethality, delivery accuracy effectiveness / value-added analysis.

For example using virtual simulation, it is possible to investigate system effectiveness of a tank with a smart target activated fire and forget EM weapon round.

8.9.5 Technology Development and Evaluation

There is a need to provide the Armed Forces with an engineering level-simulation to evaluate Service level systems and subsystems to include the individual end user for current, future needs of virtual prototypes.

- Perform weapon systems “what if” value-added analysis
- Perform countermeasure “trade-off”/ value-added analysis
- Perform sensor technology “what-if”/ value-added analysis
- Perform lethality “what-if”/ value-added analysis
- Perform survivability analysis

8.9.6 Tactics and Doctrine

There is a need to provide capability to support development and evaluation of tactics and operational concepts for the three Series at all echelons.

- Conduct weapon system force mix analysis
- Determine tactics, techniques and products for optimum employment of weapon systems/technologies.
- Determine which configuration is more effective. For example a unit of 4 LCAs where 2 can serve as reconnaissance vehicles can be a typical mix in order to draw a practical operational doctrine or 3 ALHs and 2 Jaguars serving as the reconnaissance vehicles. The reconnaissance vehicles can establish and maintain contact with the opposing force, identify the main axis of advance, provide situational awareness, and report the activity back to the appropriate command and control center.

8.9.7 Test and Evaluation

In support of the acquisition process, there is a need to provide capability to augment the testing for hardware/prototypes and conceptual models to full fill the following requirements.

- Serve as Command, Control, and Communications (C3) driver to stress information handling systems and networks
- Evaluate sensor to shooter capability of system of systems
- Expand scope of operational tests beyond live participants
- Rehearse large scale tests
- Replay large scale tests
- Provide synthetic test environment and stimuli

For example in support of a live training exercise, it is possible to serve as Command, Control, and Communications (C3) driver to stress information handling systems and

networks. In particular, simulated intelligence data gathered from aircrafts, UAVs and radars can be passed to common processing center.

8.9.8 Force Modernization

In support of the Services modernization objectives, there is a need to provide the user capability to support horizontal technology integration initiatives, digitization of the battlefield, infrared sensor and battlefield decision support system.

- Conduct survivability/value-added analysis
- Serve as Command, Control, Communications (C3) driver
- Augment operational synthetic battlefield
- Supplement analysis of alternatives

For example using virtual simulation, it is possible to investigate the value-added to a battlefield decision support system integrated on a main battle tank.

8.10 Protection and Assurance Program

The EMP and RF energy weapons are expected to form established inventory of western nations by 2015 and may proliferate equally fast to South and East Asia. It is therefore imperative for India to equip herself to mitigate or minimise the risks to NII against the use of these weapons. This will require creation of a comprehensive assurance program along with a framework for protection of NII. The outlines of this program are as follows [64,70,150].

8.10.1 EMP Vulnerability Assessment

Goals of the vulnerability assessment efforts should be to perform operability, survivability, vulnerability, and connectivity assessments for current and proposed systems in combined nuclear and non-nuclear EMP and microwave energy effects environments. The identification and capture of relevant system data should be the starting point for these assessments.

8.10.2 Electromagnetic Hardening Technology

Its goals should be to develop and demonstrate innovative and affordable technologies and methodologies for integrated hardening and testing of critical NII systems against high-power microwave (HPM) and High-altitude Electromagnetic Pulse (HEMP) effects. Specific technology objectives should include protection tools as a generic and simple-to-install hardware "kit" for hardening COTS computers, attack detectors and complete development of a unified EMP/HPM protection and test methodology.

8.10.3 Hardening of Battlefield Environment

It is anticipated that integrated hardening against multiple battlefield threat environments i.e., HPM and HEMP will reduce hardening cost, size and weight, reduce procurement costs (design and test time), and provide residual protection against other EM threats (e.g., indirect lightning). Hardening cost reductions of up to 30% can be achieved if composite shielding materials become realizable. Cost savings of 20-25% over the life of a system are also expected with the improved testing and maintenance/surveillance methodologies developed under this program. Development of field-expedient methods

for characterizing COTS immunity to EMP and HPM environments should be taken on priority. As India does not possess a sizeable manufacturing base for microelectronics, the cost of such a program can be prohibitively high. It would therefore be necessary to collaborate with strategic industry or government-to-government partner overseas.

8.10.4 Electronic System Radiation Hardening

Develop enabling technology to support the fabrication of radiation-hardened electronics and photonics and develop test/design protocols to validate system survivability using above ground tests. The payoffs from this program can include hardened electronics and cost-effective protocols to support system hardening and survivability verification. In USA a similar program has demonstrated radiation hardened 0.5 micron silicon-on-insulator microelectronics for a 4X reduction of weight and power.

8.10.5 Protection of Communication & Power Lines

The objective is to identify, develop, and demonstrate low-cost techniques to protect military and critical civil infrastructure systems with long power and communication lines from the effects of MHD-EMP. The EMP is a wide area event that can be caused by high altitude detonation of nuclear weapons. The energy they impart on transmission lines and electronic equipment is similar to certain natural phenomena. EMP can inflict serious damage on the national infrastructure and therefore there is a need to have tailored programs to address the hardening of commercial equipment against a broad spectrum of potential electromagnetic and RF threats. There is a need to take measures to ensure that the critical command and control structures of the nation respond to such an event and are resilient to these threats. There is a concern that a combination of commercial power grids, telecommunications, networks and computing systems will remain vulnerable to widespread outages and upsets due to EMP. Detailed analyses of critical civil systems would be needed to better understand the magnitude of this problem [70].

8.11 Development of Alternative Technologies for Risk Mitigation Against EM Weapons [62,63,64]

8.11.1 Fiber Optics and Shielding Technologies

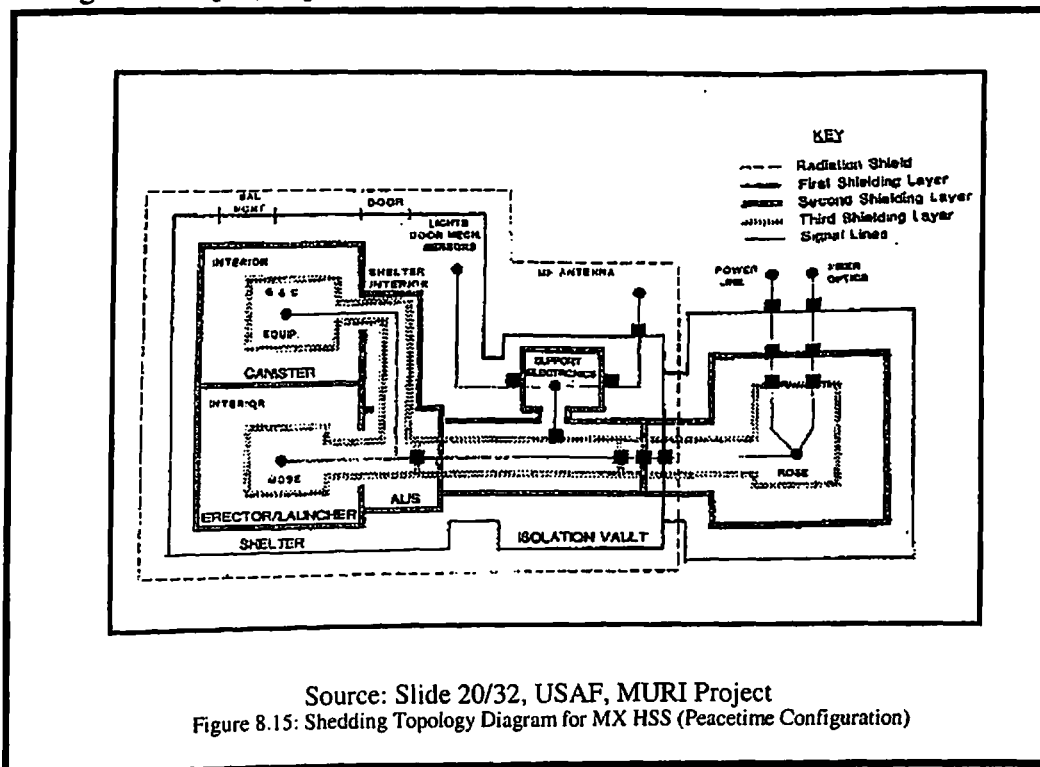
Commercial technologies can contribute significantly to the hardening of the NII. The two most significant developments are the widespread use of optical fibers and the general electromagnetic shielding of commercial electronics against spurious signals. The evolution of telecommunications cabling from copper wire to silicone and plastic fibers not only provides the added speed and capacity the modern communications demands, but these 'light pipes' are inherently immune to interference from electromagnetic pulse. Unlike copper cables, long fiber cable runs do not act like antenna to collect electromagnetic field strength and route EMP to sensitive devices. As electronic environment becomes more complicated, equipment manufacturers are forced to take defensive actions to protect equipment operation and consequently much of the electronic equipment is being manufactured today to tighter tolerances, which permit operations in electronically noisy environments. Particularly for industrial quality and

medical and laboratory equipment, off-the-shelf electronic equipment can be purchased and installed to meet the toughest electromagnetic environments that can be found in medical imaging, radiology, and high frequency welding environments. In fact, the move towards the digital environment has demanded a certain level of shielding to prevent interference to vulnerable transmission lines

8.11.2 Built in Protection at Design Stage

A surge suppressor can protect expensive and delicate electronics from unintended spikes on the electrical power grid. While in the normal case these transients are caused by natural phenomena such as lightning strikes, switching or transient loads, these devices can "filter out" the transients induced by EMP up to their stated ratings and built-in engineering margins. In many cases, these surge suppressors will also provide protection for equipment attached to telephone lines such as wireless telephone instruments, facsimile machines, and data communications devices. By blocking the out-of-the-ordinary signal levels, these surge suppressors can provide some measure of protection from EMP-like events.

EMP protection is affordable, if provided for at an early stage in system design and development. For military systems of tactical interest and an anticipated threat environment at the low-to-moderate end of the threat spectrum, the cost can be as little as one percent of the total development investment. For strategic systems, where the worse possible threat environment must be protected against, the cost can go up to five percent. The typical engineering approach is to provide necessary filtering of the expected EMP energy frequency on wirelines that are connected to the device and to shield the sensitive components from the direct effects of EMP energy. The arrangement for ground-up design of the Peace Keeper (MX) Missile System of DoD, USA is shown in figure 8.15 [70, 78].



Source: Slide 20/32, USAF, MURI Project
Figure 8.15: Shedding Topology Diagram for MX HSS (Peacetime Configuration)

8.11.3 Improved Packaging of Electronics

State of the art commercial semiconductor processes are designed primarily for performance factors other than EMP. Many of today's semiconductor technologies are highly vulnerable to relatively low levels of electromagnetic field strength. Protection of these devices requires designs and packaging techniques to prevent effects of EMP.

The infrastructure is rapidly evolving into a complex system of networks. At present, there is limited understanding of the implication of EMP and RF vulnerability on these complex systems. For example a large system of systems will only be as resilient as its weakest link. However large networks frequently have multiple, redundant paths and failure of an individual component may have little or no effect on the overall performance of the network. These aspects need to be examined.

To capitalize on leading edge technologies, military systems are increasingly using COTS equipment that has not been specifically designed to mitigate the effects of an EMP environment. The USA DoD has set forth a goal to transition from a 25% COTS / 75% MILSPEC equipment ratio in military systems to 75% COTS / 25% MILSPEC. This has several ramifications. There will be fewer DoD investments in built-to-specification military systems to meet unique DoD requirements. At the same time, with growing dependence on commercial-of-the-shelf technologies, the concerns for robustness in an electronically noisy environment must be addressed in the equipment we purchase and these improvements will be available to other hardware purchasers.

8.11.4 EMP Hardening Schemes

Life cycle maintenance of EMP protection needs to be addressed so that the highest levels of protection can be assured. This means that modifications, inspections, repair actions, and operations must take into account the EMP integrity of the individual equipment and the networks they serve. A requirement is to determine behavior of the digital circuitry to EM excitation and know the vulnerabilities as shown in figure 8.16. Based on this a system that is engineered, installed and initially tested to guarantee its protection. The hardness must be periodically re-tested and put under continuous surveillance to ensure that day to day operations and maintenance have not left it vulnerable to electronic attacks. A model suggested by FM Tesche, under the DoD, USA project, MURI is shown in figure 8.17. This EMP hardness surveillance and hardness maintenance process must be built into the system design. This additional operations and maintenance burden need to be addressed whenever a decision is made to protect against EMP vulnerabilities [70,78].

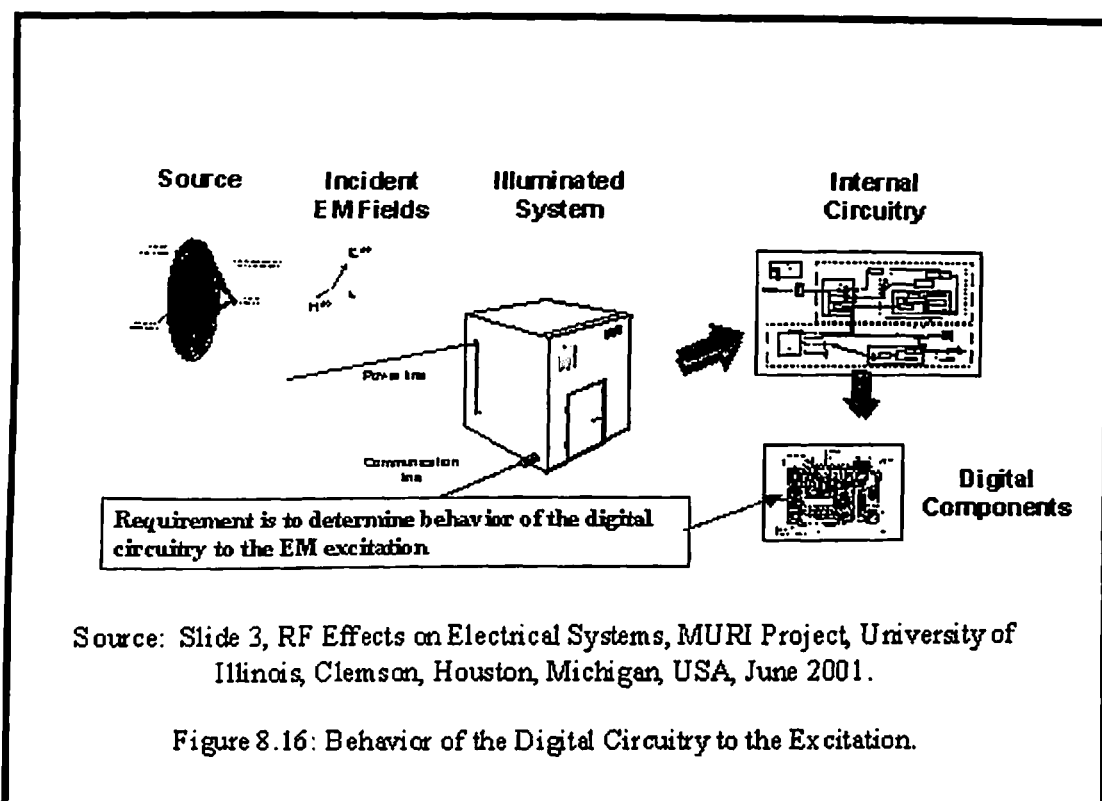


Figure 8.16 Behavior of the Digital Circuitry to the Excitation

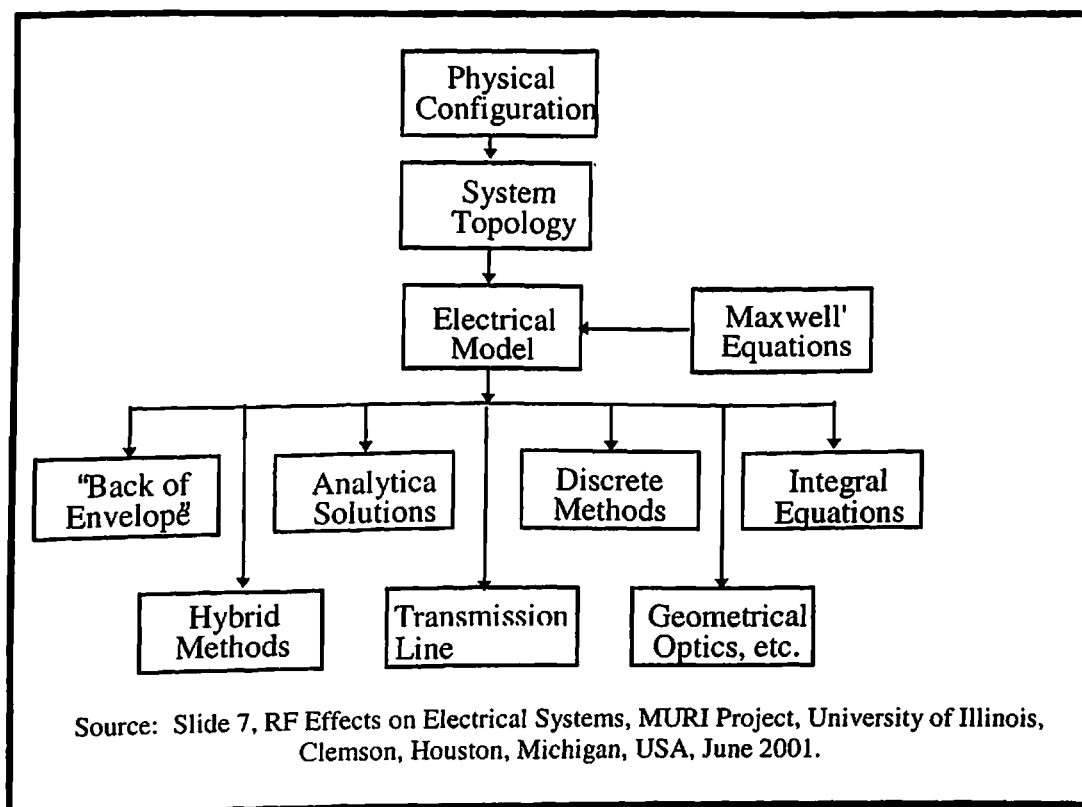


Figure 8.17: Modeling for EM Vulnerability Analysis.

8.12 Suggested Approach for India

India needs to develop its IW posture in consonance with emerging threats in the foreseeable future, match her global role and deterrence potential. This would require development of an institutionalized IW framework, creation of new organizations and institutions to support this program, pool together expertise available within the country, and if necessary enter into collaboration with strategic partners overseas. In specific terms, following steps are extremely necessary [150,206,207].

- Institutionalize IW policy framework (**Institutional Decision Making, Funding Support**)
- Create Institutes of Information Technology & Information Warfare (**Academic Support**)
- Create Laboratories and work centers for Information Warfare. (**Technologies, Solutions, System Engineering, Weapon Development, Implementation**).
- Create National Information Infrastructure Authority (**Regulation, Control, Protection**)
- IW Operations (**Armed Forces, Civil Defence, Internal Security**).

8.12.1 Proposed Information Warfare Organizations at National Level

A national level IW organization to undertake the following tasks is proposed [150,206,207].

8.12.2 Following two project organizations under a National IW Board are proposed.

Project Organization 1: IW Weapons Development Program. A suitable Project Organization to undertake the following tasks is to be created.

- Develop IW Conceptual Framework in consonance with national security goals.
- Identify requirements and scope of EMP and RF energy weapons to meet security goals.
- Evolve EMP and RF energy weapons development framework and program.
- Evolve System Engineering models.
- Identify building blocks for development of IW weapons.
- Create development and testing infrastructure.
- Task laboratories with Services specific developments, involve industry for production.
- Create System Engineering organizations to undertake system integration and induction.
- Interface with Service Head Quarters.
- Create funding and other support infrastructure.
- Interface with project organizations responsible for development and implementation of security overlays for the National Information Infrastructure to dovetail both the programs.

8.12.3 Project Organization 2

National Information Protection Program. This project should be tasked to undertake the following:

- Develop Protection Framework in consonance with national security goals including EMP and RF energy protection.
- Identify requirements and scope of NII security to meet the above mentioned goals.
- Evolve National Information Assurance Program for development of security technologies and soft infrastructure.
- Evolve security models for national emergencies and dovetail them with National Civil Defense vis-à-vis cyberwar emergencies.
- Interface with Armed Forces and other Critical National Information Infrastructure agencies to create building blocks for the security of critical information infrastructure of core sectors of economic activity and functional hubs of national governance.
- Create and task laboratories, work centers and industry to develop/customize root technologies for NII security.
- Create System Engineering Organizations to under take systems engineering and integration of IW components in civil and military domains.
- Interface with national agencies engaged in development of IW weapons to dovetail solutions for IW - Defense.
- Funding, control and monitoring on project basis.

8.12.4 Proposed Roles of Armed Forces

- Develop IW Concepts in consonance with IW goals of respective Service.
- Create IW System models.
- Dovetail EM weapons with conventional weaponry.
- Identify changes in force structure and pursue implementation.
- Training and post deployment support.

The integrated infrastructure for national IW program is illustrated in Figure 8.18.

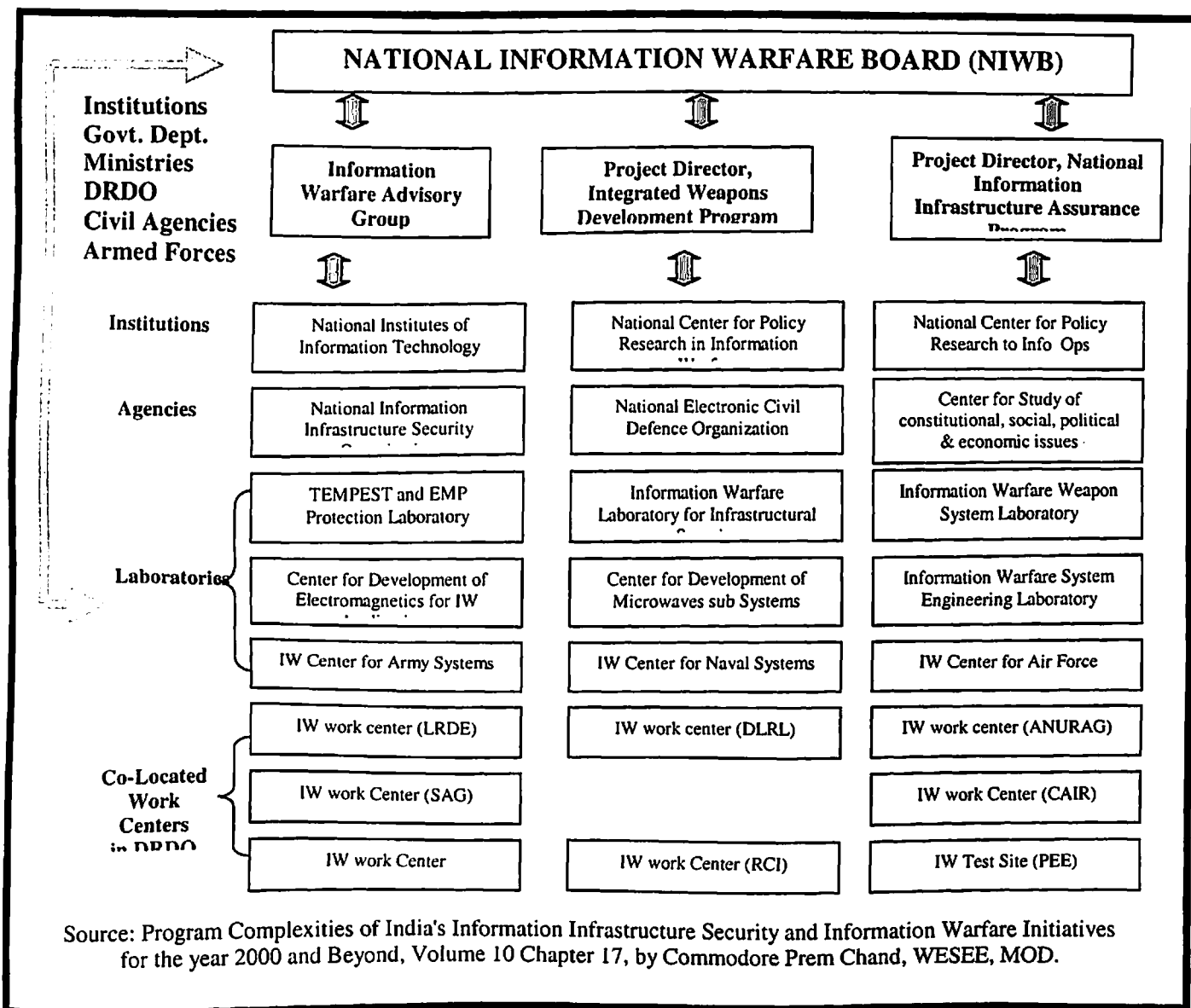


Figure 8.18: Infrastructure Framework for National Information Warfare Program.

8.13 Conclusion

This chapter concludes that EMP and RF energy weapons offer the prospect of very significant IW offensive and defensive capability for India. The operational requirements for an all weather IW weapons capability has been suggested. The building blocks of these weapons and their constructional details as available for the ongoing the programs across the globe have been presented with mid term (4 to 6 years) and long term (7 to 10 years) perspective in view. The blueprint for research design and development encompassing technology assessment, HPM effects and lethality, integration with existing programs, hardening schemes technology demonstration, tactics and doctrines, testing

and evaluation, force modernization, protection program, assurance strategies, risk mitigation strategies have been presented.

The outlines of National Information Warfare Board, project organizations for development of IW weapons and NII Assurance Framework, along with institutions, government agencies, work centers, laboratories with in the defence establishment and their appropriate interface with other national agencies, industry and academia have been suggested.

In summary this chapter constitutes the blueprint for development of India's IW capability. The packaging, induction and deployment aspects have been presented in chapter 8.

Note 1: Source:

WE.79.08 *HPM Aircraft Self-Protect Missile Countermeasures*. The goal is to develop and demonstrate ultra wideband (UWB) high-power microwave (HPM) technology to provide robust protection of large aircraft against the rapidly proliferating infrared, EO, RF and laser-guided missile threat. Ongoing missile susceptibility tests are defining the most effective and efficient kill mechanisms: disruption of seeker, guidance, or fuze electronics. Modeling and simulation tools are nearly complete and will be used to support/enhance RF effects tests and to analyze engagement scenarios. As of September 1996, the source technology selected for this effort is an array of individual laser-triggered solid-state sources which produces a narrow, electronically steerable beam. An UWB HPM brassboard (consisting of source, antenna, and power conditioners) will be developed in FY97 and built in early FY98. The brassboard will be packaged for a field demonstration in the fourth quarter of FY98 in conjunction with the DoD infrared countermeasures program. A significant parallel effort explores the EMI/EMC issues relating to the host aircraft. Aircraft hardening and HPM antenna backlobe and sidelobe suppression methods are being developed and demonstrated. HPM is a non-expendable, generic counter-measure capable of defeating a large variety of missiles without a priori knowledge of specific threat parameters

Note 2: Source:

WE.22.09 *High-Power Microwave C²W/IW Technology*. This DTO develops and demonstrates high-power microwave (HPM) technology to disrupt, degrade, and destroy electronics in communication and information systems to support command and control/information warfare (C²W/IW) and suppression of enemy air defense (SEAD) missions. Adversaries will be denied use of electronic information processing and communications systems by using high-peak (damage) and high-average (disruption) power wideband sources packaged for an air-deliverable bomb, submunition, man-portable device, or unmanned aerial vehicle (UAV). Nonlethal or lethal technology will initially concentrate on man-portable (short-range) or heavy transportable weapons and SEAD applications, followed by airborne weapons on UAVs or as submunitions, as prioritized by user needs and technical maturity. Ongoing susceptibility/effects testing on information processing and communications systems of military interest will define specific HPM source and antenna requirements by FY99. In FY00, the first brassboard system will be used in a critical experiment to demonstrate feasibility to the user. With user-defined metrics and measures of effectiveness, the first-generation ATD will be

conducted in FY07. This effort exploits generic HPM effects on information and communications systems without a priori knowledge of specific target parameters. Specific details are classified and can be provided to appropriate agencies upon request.

Note 3: Source

WE.23.08 *Modern Network Command and Control Warfare Technology*. The objective is to develop and demonstrate multiple synergistic capabilities to intercept and attack or counter advanced, global, military communication/navigation/information networks from ground and airborne platforms. In FY98, the program will demonstrate unmanned aerial vehicle (UAV)-based electronic support (ES) and real-time relay to ground and air components of the Intelligence EW Common Sensor (IEWCS) System. By FY00, the program also will demonstrate ES and EA strategies to counter emerging modern complex communication formats, conduct a joint test with WE.46 for evaluation of SEAD, and demonstrate a tenfold increase in HF wideband power generation in a comparable package volume. The FY07 goal is to demonstrate non-fratricidal electronic attack (EA) techniques versus communication/ navigation systems. By FY02, it will demonstrate ES/EA capability against a low-probability-of-intercept/-detection (LPI/LPD) class of specific communications links characterized by featureless, time-division, and code-division multiplexing formats. By FY02, the program will also provide the capability to selectively influence an adversary's use of or confidence in information, processes, systems, and computer-based networks through the use of offensive deceptive techniques to manipulate the information or information sources which support them. By FY03, the program will show a 7,000 times improvement in effective use of available transmitter power, and a 7,000 times improvement in EA spatial selectivity for jamming strategies. Achievement of this DTO will enable joint forces to wage proactive, offensive information warfare against an enemy's command and control information infrastructure and delay/deny effective enemy defense versus U.S./coalition strike forces.

CHAPTER 9

PACKAGING INDUCTION AND DEPLOYMENT OF EM WEAPONS

9.1 Introduction

The EM weapons would need to coexist with the current conventional weapons. This would require that sensors, command & control systems, launch and delivery systems are made compatible with them for maximum effect. This chapter examines possible targets and the lethality considerations for use of EM weapons. It also presents packaging, integration, delivery and launch options. The chapter also maps the weapon capabilities to combat roles, effectiveness, and doctrines for exploitation by all the three Services. It signifies that EM weapons can map into the role of artillery ammunition, missiles, platform protection and attack systems covering strategic as well as tactical operations. There is a one to one replacement of conventional weapons by EM weapons possible in the foreseeable future.

This chapter presents doctrines for exploitation of EM weapons in strategic tactical roles whereby information flow within the NII structures can be served effectively. The strategy to attack information processing and communication elements for high payoffs in terms of paralysis and disorientation has been suggested by mapping the warden's combat model to military and Civil Components of NII. The doctrine encompasses the electronic combat operations, maritime operations, land battle, defensive counter operations, graduated response strategy and defence against EM weapons. A protection strategy and hardening program has also been suggested.

9.2 Identification of Targets

Following can be targeted effectively using EM weapons [68].

9.2.1 Geographically Fixed Targets

Buildings housing government offices, computer equipment, production facilities, military bases, known radar sites and communication nodes are all targets which can be readily identified through conventional photographic, satellite imaging, radar, electronic reconnaissance and human intelligence operations. These targets are typically geographically fixed and thus can be attacked provided the aircraft can penetrate to weapon release range. With the accuracy inherent in Geographical Positioning System (GPS) / inertially guided weapons, the EM weapons can be programmed to detonate at the optimal position to inflict maximum electrical damage.

9.2.2 Mobile and Camouflaged Targets

Mobile and camouflaged targets, which radiate overtly, can also be readily engaged. Mobile and relocatable air defence equipment, mobile communication nodes, mobile command shelters and naval vessels fall in this category of targets. When these targets radiate, their positions can be precisely tracked with suitable Electronic Support Measures (ESM) and Emitter Locating Systems (ELS) carried either by the launch

platform or a remote surveillance platform. In the latter instance target coordinates can be continuously data linked to the launch platform. As most such targets move relatively slowly, they are unlikely to escape the footprint of the electromagnetic bombs during the weapon's flight time.

9.2.3 Mobile and Hidden Targets

Mobile and hidden targets, which do not overtly radiate may present a problem, particularly when conventional means of targeting are employed. A technical solution to this problem does however exist, for many types of target. This solution is the detection and tracking of Unintentional Emission (UE). UE has attracted most attention in the context of TEMPEST surveillance, where transient emanations leaking out from equipment due to poor shielding can be detected and in many instances demodulated to recover useful intelligence. Termed "Van Euck" radiation after its inventor, such emissions can only be suppressed by rigorous shielding and emission control techniques, employed in TEMPEST rated equipment.

Whilst the demodulation of Van Euck can be a technically difficult task to perform well, in the context of targeting by the EM weapons this problem does not arise. To target such an emitter for attack requires only the ability to identify the type of emission and thus target type and to isolate its position with sufficient accuracy to deliver the weapon. Because the emissions from computer monitors, peripherals, processor equipment, switch mode power supplies, electrical motors, internal combustion engine ignition systems, variable duty cycle electrical power controllers, super heterodyne receiver local oscillators and computer networking cables are all distinct in their frequencies and modulations. A suitable Emitter Locating System can be designed to detect, identify and track such sources of emission.

9.3 Delivery Systems for EM weapons

Following features are unique to EM weapons.

- Multi component warhead consisting of a battery, FCG (2 or more stages) and a vircator or, deflector and antenna.
- The missile, launch & delivery platform needs to be equipped with priming source.
- The non-missile weapons (free fall or guided bombs) need pre charging before launch from a platform viz. ship, aircraft or submarine.
- EM-weapon payloads for missiles contain priming power packs and therefore are heavy. Comparatively free fall projectiles are pre-charged; light weight and hence more lethal.

As with explosive warheads, electromagnetic warheads will occupy a volume of physical space and will also have some given mass (weight) determined by the density of the internal hardware. Like explosive warheads, electromagnetic warheads may be fitted to a range of delivery vehicles. Some of the potential possibilities are examined in the succeeding paragraphs [41].

9.3.1 Cruise Missile

A possible application involves fitting an EM warhead to a cruise missile airframe. The choice of a cruise missile airframe will restrict the weight of the weapon to about 340-kg, although some sacrifice in airframe fuel capacity could increase the size. A limitation in all such applications is the need to carry an electrical energy storage device, e.g. a battery, to provide the current used to charge the capacitors used to prime the FCG prior to its discharge. Therefore the available payload capacity will be split between the electrical storage and the weapon itself. In wholly autonomous weapons such as cruise missiles, the size of the priming current source and its battery may impose following limitations on weapon capability.

- A missile borne EM warhead installation will comprise of the electromagnetic device, an electrical energy converter, and an onboard storage device such as a battery. As the weapon is pumped, the battery is drained. The electromagnetic device will be detonated by the missile's onboard fusing system. In a cruise missile, this will be tied to the navigation system; in an anti-shipping missile to the radar seeker and in an air-to-air missile to the proximity fusing system. The warhead fraction (i.e. ratio of total payload (warhead) mass to launch mass of the weapon) will be between 15% and 30%.
- An electromagnetic bomb warhead will comprise an electromagnetic device, an electrical energy converter and an energy storage device to pump and sustain the electromagnetic device charge after separation from the delivery platform. Fusing could be provided by a radar altimeter fuse to airburst the bomb, a barometric fuse or in GPS/inertially guided bombs, the navigation system. The warhead fraction could be as high as 85%, with most of the usable mass occupied by the electromagnetic device and its supporting hardware.
- Due to the potentially large lethal radius of an electromagnetic device, compared to an explosive device of similar mass, standoff delivery would be prudent. Whilst this is an inherent characteristic of weapons such as cruise missiles, potential applications of these devices to glide bombs, anti-shipping missiles and air-to-air missiles would require fire and forget guidance of the appropriate variety, to allow the launching aircraft to gain adequate separation of several miles before warhead detonation.

9.3.2 Aircraft Delivered EM Weapons

Aircraft delivered bombs, which have a flight time between tens of seconds to minutes, could be built to exploit the launch aircraft's power systems. In such a bomb design, the bomb's capacitor bank can be charged by the launch aircraft en route to target, and after release a much smaller onboard power supply can be used to maintain the charge in the priming source prior to weapon initiation. This in turn can give comfortable trade-offs for enhanced lethality. An electromagnetic weapon delivered by a conventional aircraft can offer a much better ratio of electromagnetic device mass to total bomb mass, as most of the bomb mass can be dedicated to the electromagnetic device installation itself. It follows therefore, that for a given technology an electromagnetic bomb of identical mass to a electromagnetic warhead equipped missile can have a much greater lethality, assuming equal accuracy of delivery and technologically similar electromagnetic device

design. Lethality of air launched weapons at lower and higher detonation height is illustrated in figure 9.1 [39].

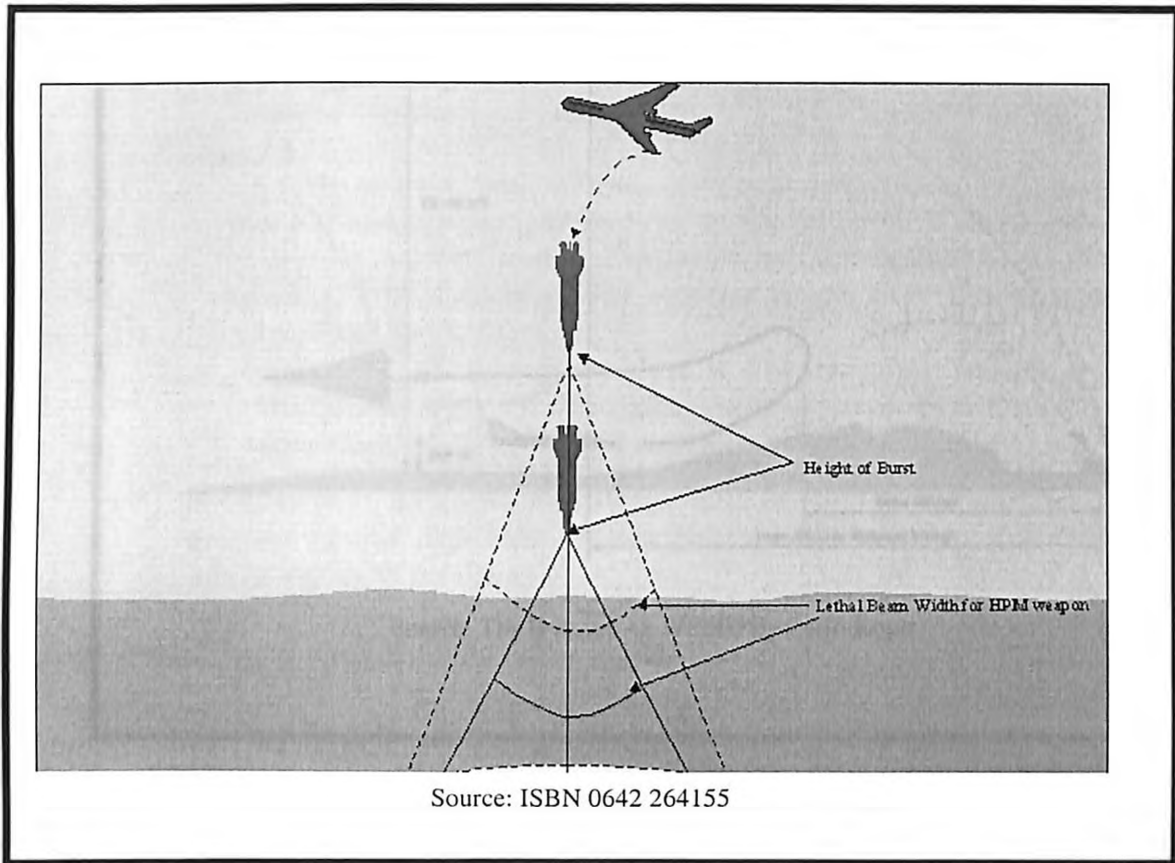


Figure 9.1: Height of Detonation vis-à-vis Lethality

The GPS satellite navigation guidance kits for conventional bombs and glidebombs can provide the optimal means for cheaply delivering such weapons. While GPS guided weapons without differential GPS enhancements may lack the pinpoint accuracy of laser or television guided munitions, they are still quite accurate and importantly, cheap, autonomous all weather weapons. The mode of delivery vis-à-vis CEP is given in figure 9.2. The delivery profile of a GPS guided EM weapon is shown in figure 9.3.

<u>Mode of Delivery</u>	<u>CEP</u>
Free-fall	100 - 1000ft
GPS aided	40 ft
Stand of missiles	40ft
Cruise missiles	10 - 40ft

Source: ISBN 0642 264155

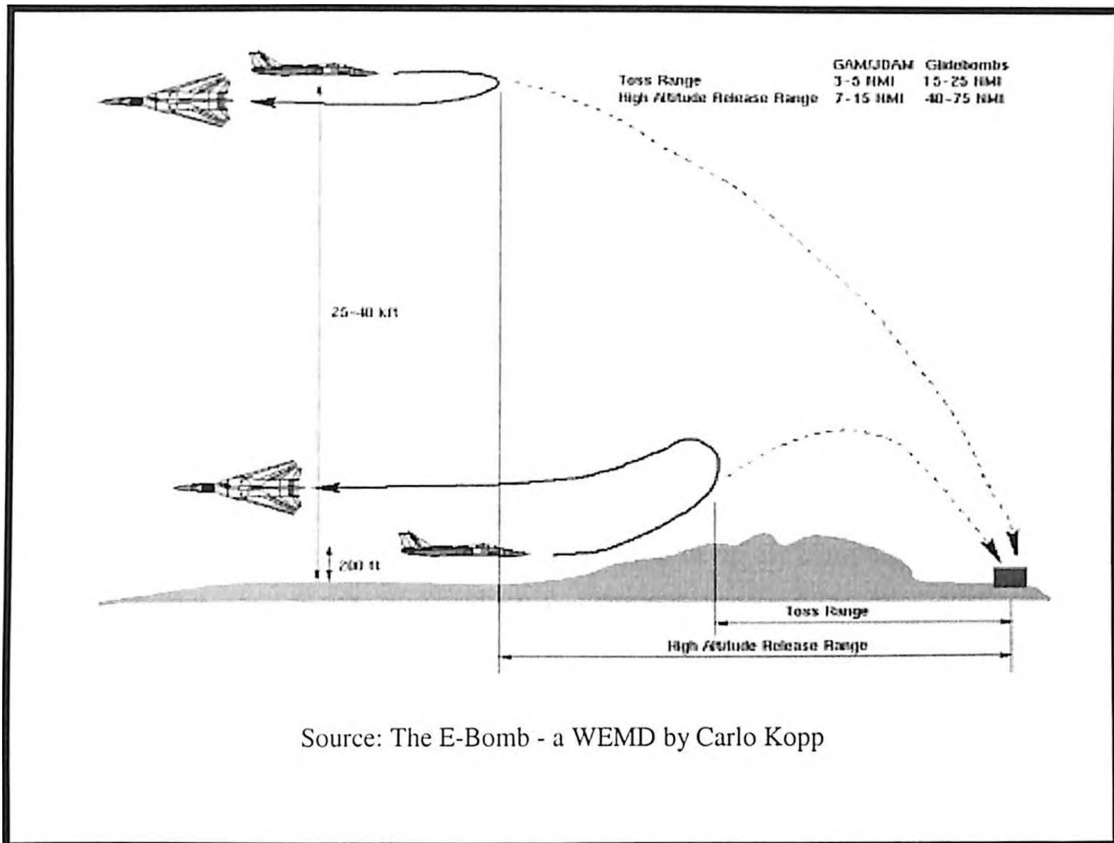


Figure 9.3 : Delivery Profile of GPS Guided EM Weapon

9.3.3 Glide Bombs

The use of glidebombs as delivery means for HPM warheads has following advantages.

- The glide bomb can be released from outside the effective radius of target air defences, therefore minimizing the risk to the launch aircraft.
- The large standoff range means that the launch aircraft can remain well clear of the bomb's effects.
- The bomb's auto-pilot can be programmed to shape the terminal trajectory of the weapon, such that a target may be engaged from the most suitable altitude and aspect.

9.3.4 Flexibility and Advantages of Aircraft Launch Platforms

Launching EM weapons from aircraft offers following advantages.

- The weapon can be delivered by any tactical aircraft with a navigation-attack system capable of delivering GPS guided munitions. If the EM weapon ballistic properties are identical to the standard weapon, no software changes to the aircraft may be required.
- EM bombs in comparison with Anti Radiation Missiles (ARM) are simple. These will be both cheaper to manufacture, and easier to support in the field, thus allowing

for larger weapon stocks. This makes saturation attacks a much more viable proposition.

- Following assessment by analysts about the US Air Force has been made.
 - The ability of a B-2A aircraft to deliver up to sixteen GAM/JDAM fitted EM weapon warheads with a 20 ft class CEP allows a small number of such aircraft to deliver a decisive blow against key strategic, air defence and theatre targets.
 - A strike and electronic combat capable derivative of the F-22 aircraft would also be a viable delivery platform for an EM weapon. With its superb radius, low signature and supersonic cruise capability, these aircraft could attack air defence sites, C³I sites, airbases and strategic targets with EM weapon, achieving a significant shock effect.
 - The whole F-22 aircraft is built to be EM weapon capable, as this would allow the USAF to apply the maximum concentration of force against arbitrary air and surface targets during the opening phase of an air campaign.
- In India's case, the Jaguar and Mirage-2000 can provide the capability to deliver EM weapons against high value targets with virtual impunity. In future the LCA can also be equipped for this role.

9.4 Lethality Assessment Issues

The technology base for weapon construction has been widely published in the open literature. However lethality related issues have been published much less frequently. The calculation of electromagnetic field strengths achievable at a given radius for a given device design is a comparatively simple and straightforward task. However determining a kill probability for a given class of targets under such conditions is complex and difficult. Therefore only the broad aspects of lethality assessment are described [41].

9.4.1 How EM Weapons Cause Damage

As described in the previous chapter, the FCGs induce high frequency, high voltage spikes on fixed wiring systems and the HPMs cause high voltage standing waves on fixed wiring systems. The standing waves couple through openings (doors, windows etc.), and produce spatial standing wave inside the equipment cavity, which in turn causes damage / destruction to the microelectronics.

- Low frequency EM weapons couple well into wiring infrastructure, as most telephone lines, networking cables and power lines follow streets, building risers and corridors. In most instances any particular cable run will comprise of multiple linear segments joined at approximately right angles. Whatever be the relative orientation of the weapons field, more than one linear segment of the cable run is likely to be oriented in such a way that a good coupling efficiency can be achieved. The diversity of target types and the unknown geometrical layout and electrical characteristics of the wiring and cabling infrastructure surrounding a target makes the exact prediction of lethality impossible.

- The microwave weapons couple more readily than low frequency weapons, and can bypass protection devices designed to stop low frequency coupling, Microwave weapons cause more lethal than low frequency weapons.
- With the current level of research it is difficult to produce workable models for predicting equipment vulnerability. However it provides a basis for shielding strategies and hardening of equipment.
- A general approach for dealing with wiring and cabling related back door coupling is to determine a known lethal voltage level, and then use this to find the required field strength to generate this voltage. Once the field strength is known, the lethal radius for a given weapon configuration can be calculated.

9.4.2 Factors Affecting Lethality

Following factors have a direct bearing on the lethality.

- The target types are very diverse in their electromagnetic hardness or ability to resist damage.
- Equipment, which has been intentionally shielded and hardened against electromagnetic attack, will withstand orders of magnitude greater field strengths than standard commercially rated equipment.
- Various manufacturer's implementations of like types of equipment may vary significantly in hardness due the choice of specific electrical designs, cabling schemes and chassis/shielding designs etc.
- Coupling efficiency, which is a measure of how much power is transferred from the field produced by the weapon into the target is a critical factor.
 - Front door coupling occurs through antenna. It affects transmitter / receiver semiconductor devices in RF range.
 - Back door coupling induces spikes of large transients. These are routed through water and sewage pipes, telephone lines, data cable ducts and affect exposed semiconductors, damaging power supplies and communication interfaces.

9.4.3 EM Voltage Levels Required to Cause Damage to Electronic Devices

It is important to know or establish safe operating envelopes of semiconductor devices. Typical figures are as follows [39].

- Manufacturer's guaranteed breakdown voltage ratings for silicon high frequency bipolar transistors, used in communications equipment, vary between 15 V and 55 V.
- Gallium Arsenide Field Effect Transistors are usually rated at about 10V.
- High density Dynamic Random Access Memories (DRAM), are usually rated to 7 V against earth.
- CMOS logic is rated between 7 V and 15 V, microprocessors running off 3.3 V or 5 V, power supplies are rated very closely to that voltage.
- Devices are equipped with additional protection circuits at each pin, to sink electrostatic discharges. Sustained or repeated application of a high voltage will often defeat these and damage the equipment in part or whole.

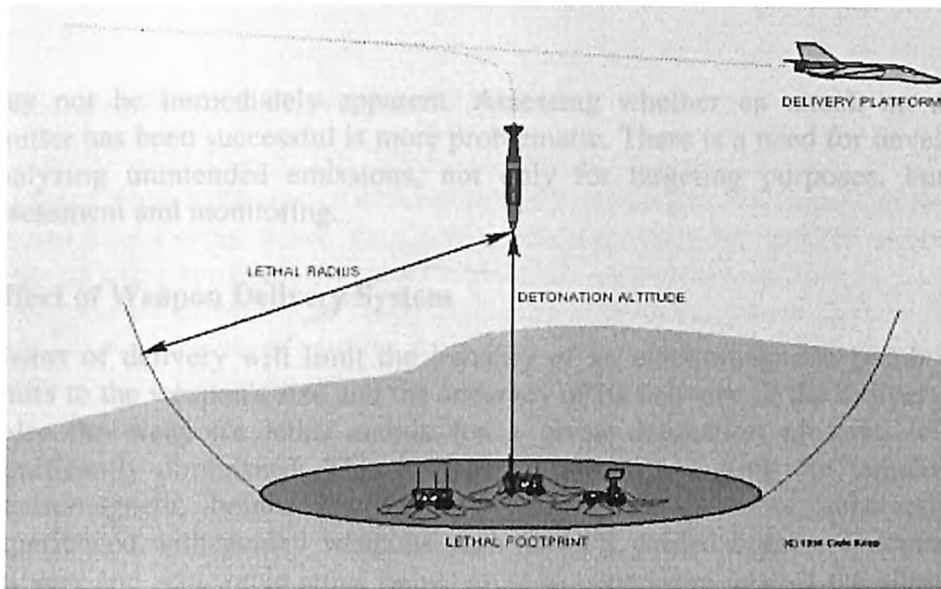
- Communications interfaces and power supplies must typically meet electrical safety requirements imposed by regulations. Such interfaces are usually protected by isolation transformers with ratings from hundreds of Volts to about 2 to 3 kV. Once the defence provided by a transformer, cable pulse arrestor or shielding is breached, voltages as low as 50 V can inflict substantial damage upon computer and communications equipment.

9.4.4 Constraint & Limitations of EM Weapons

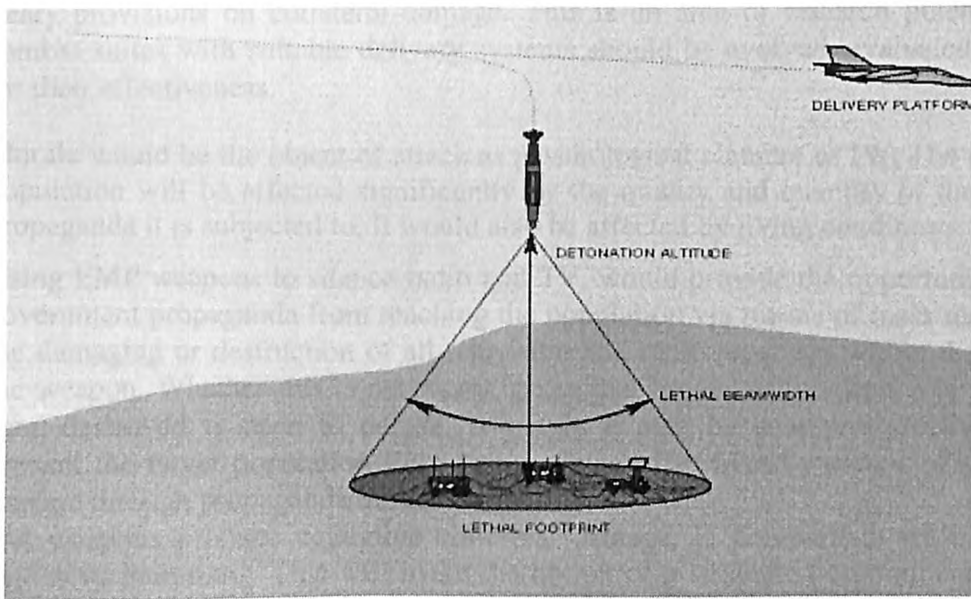
The constraint limitations of electromagnetic weapons are determined by weapon implementation and means of delivery. Weapon implementation will determine the electromagnetic field strength achievable at a given radius, and its spectral distribution. Means of delivery will constrain the accuracy with which the weapon can be positioned in relation to the intended target. Both constrain lethality.

9.4.5 Assessment of Lethal Coverage

An important factor in assessing the lethal coverage of an electromagnetic weapon is atmospheric propagation. While the relationship between electromagnetic field strength and distance from the weapon is one of an inverse square law in free space, the decay in lethal effect with increasing distance within the atmosphere will be greater due to quantum physical absorption effects. This is particularly so at higher frequencies, and significant absorption peaks due to water vapors and oxygen which exist at frequencies above 20 GHz. These will therefore constrain the effect of HPM weapons to shorter radii than are ideally achievable in the K and L frequency bands. Since there is very little control over this aspect, it would be necessary to examine range, lethality, payload, delivery options in terms of suitable tradeoffs. The precise assessment of atmosphere and its monitoring in own, as well as enemy territory would be another burden to be carried as part of deployment package. This would not only require more deeper research efforts but would also require satellite assets for space based surveillance of weather conditions and their on line relay to concerned deployment sites. The lethal foot print depicted by Carlo Kopp for low frequency E-bomb and HPM weapon is shown in figure 9.4 and figure 9.5



Source: The E-Bomb - a WEMD by Carlo Kopp
 Figure 9.4 : Lethal Footprint of Low Frequency E-bomb in Relation to Altitude



Source: The E-Bomb - a WEMD by Carlo Kopp

Figure 9.5: Lethal Footprint of HIPM E-Bomb in Relation to Altitude

9.4.6 Kill Assessment and Monitoring Difficulties

Radiating targets such as radar or communications equipment may continue to radiate after an attack even though their receivers and data processing systems have been damaged or destroyed. This means that equipment that has been successfully attacked may still appear to operate. Conversely an opponent may shut down an emitter if attack is imminent and the absence of emissions means that the success or failure of the attack

may not be immediately apparent. Assessing whether an attack on a non-radiating emitter has been successful is more problematic. There is a need for developing tools for analyzing unintended emissions, not only for targeting purposes, but also for kill assessment and monitoring.

9.4.7 Effect of Weapon Delivery System

Means of delivery will limit the lethality of an electromagnetic bomb by introducing limits to the weapon's size and the accuracy of its delivery. If the delivery error is of the order the weapon's lethal radius for a given detonation altitude, lethality will be significantly diminished. This is important when assessing the lethality of unguided electromagnetic bombs, as delivery errors will be more substantial than those experienced with guided weapons such as GPS guided bombs. Therefore accuracy of delivery and achievable lethal radius must be considered against the allowable collateral damage for the chosen target. Where collateral electrical damage is a consideration, accuracy of delivery and lethal radius are key parameters. An inaccurately delivered weapon of large lethal radius will be unusable against a target if the collateral electrical damage is beyond acceptable limits. This can be a major issue for nations constrained by treaty provisions on collateral damage. This is an area of research potential whereby combat suites with suitable delivery systems should be evolved, evaluated and verified for their effectiveness.

Morale would be the object of attack as psychological element of IW. The morale of the population will be affected significantly by the quality and quantity of the government propaganda it is subjected to. It would also be affected by living conditions.

Using EMP weapons to silence radio and TV, would provide the opportunity to prevent government propaganda from reaching the population via means of mass media, through the damaging or destruction of all television and radio receivers within the footprint of the weapon. Whether this is necessary, given that broadcast facilities may have already been destroyed is open to debate. Arguably it may be counterproductive, as it will prevent the target population from being subjected to friendly means of psychological warfare through propaganda broadcasts.

EM weapons produce negligible collateral damage, in comparison with conventional explosive munitions. This will make the option of a strategic bombing campaign more attractive in a foreseeable future to hood wink propaganda by international community and also where mass media coverage of the results of conventional strategic strike operations will adversely affect domestic civilian morale and public opinion.

The use of EM weapons against a target population requires careful consideration in the context of the overall IW campaign strategy. This is particularly critical because the civil and military aims of IW may not converge. If useful objectives can be achieved by isolating the population from government propaganda, then the population is a valid target for electromagnetic attack. In the foreseeable future when social impact of IW is clearer, the forces may be constrained by treaty obligations and may have to reconcile against the applicable regulations relating to denial of services to non-combatants. At this moment these issues are very nebulous.

9.4.8 Achievable Damage Ratings of EM Weapons

If a device of 10 GW, 5 GHz HPM is used to illuminate a footprint of 400 to 500 meters diameter, from a distance of several hundred meters, this will result in field strengths of several kilovolts per meter. This in turn would produce hundreds of volts to kilovolts on exposed wires or cables. Therefore lethal radii, of hundreds of meters is possible, subject to weapon performance and target set electrical hardness. These devices therefore can be used for amphibious operations to silence harbor defenses. The typical case of HPM usage in a sea-lane is shown in the figure 9.6 [41].

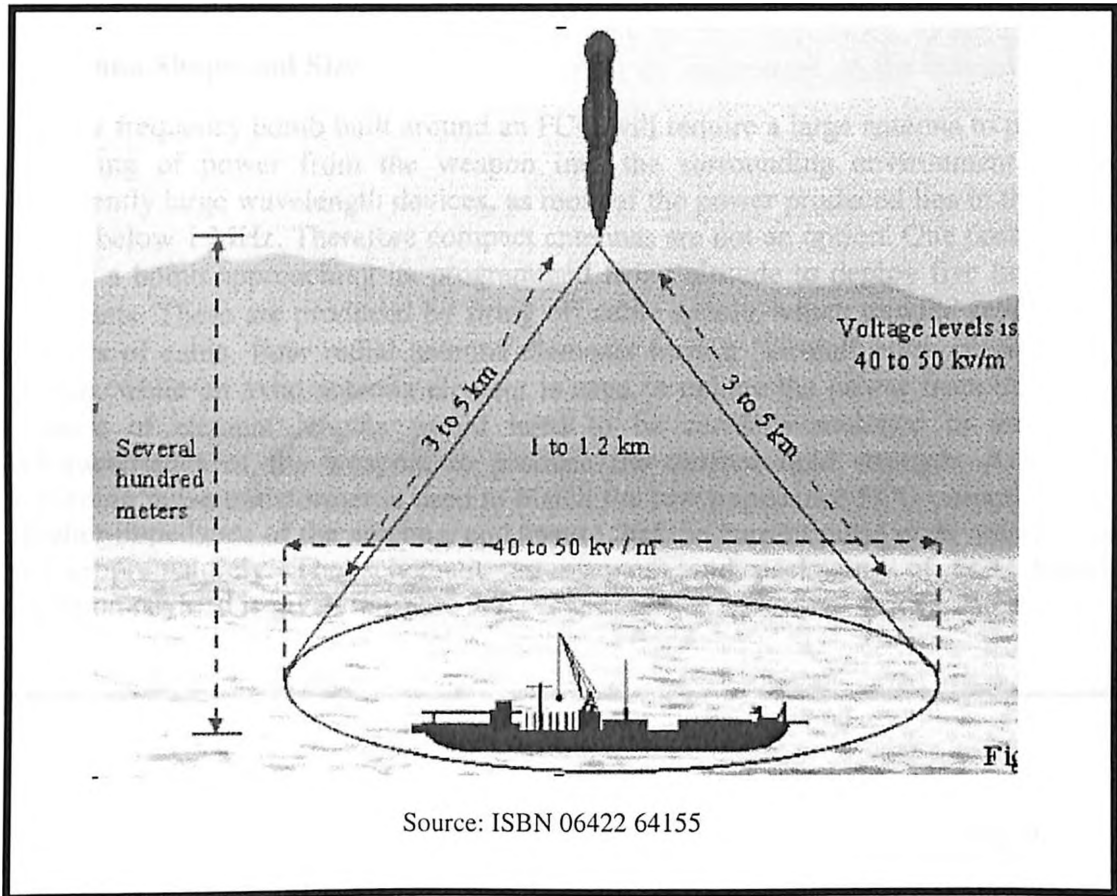


Figure:9.6: Damage Potential of HPM Weapon

9.5 Enhancing Lethality of EM weapons

9.5.1 Improved Coupling

Following steps can maximize lethality through power coupling.

- Maximize the peak power and duration of the radiation a given bomb size, by using the powerful flux compression generator.
- Maximize the efficiency of internal power transfer coupling using better techniques and system engineering.

9.5.2 Antenna Shape and Size

A low frequency bomb built around an FCG will require a large antenna to provide good coupling of power from the weapon into the surrounding environment. These are inherently large wavelength devices, as most of the power produced lies in the frequency band below 1 MHz. Therefore compact antennas are not an option. One possible scheme is for a bomb approaching its programmed firing altitude to deploy five linear antenna elements. These are produced by firing off cable spools, which unwind several hundred meters of cable. Four radial antenna elements form a "virtual" earth plane around the bomb, while an axial antenna element is used to radiate the power from the FCG. The choice of element lengths would need to be carefully matched to the frequency characteristics of the weapon, to produce the desired field strength. A high power coupling pulse transformer is used to match the low impedance FCG output to the much higher impedance of the antenna, and ensure that the current pulse does not vaporize the cable prematurely. The schematic arrangement and packaging of FCG based EM weapon payload is given in figure 9.7.

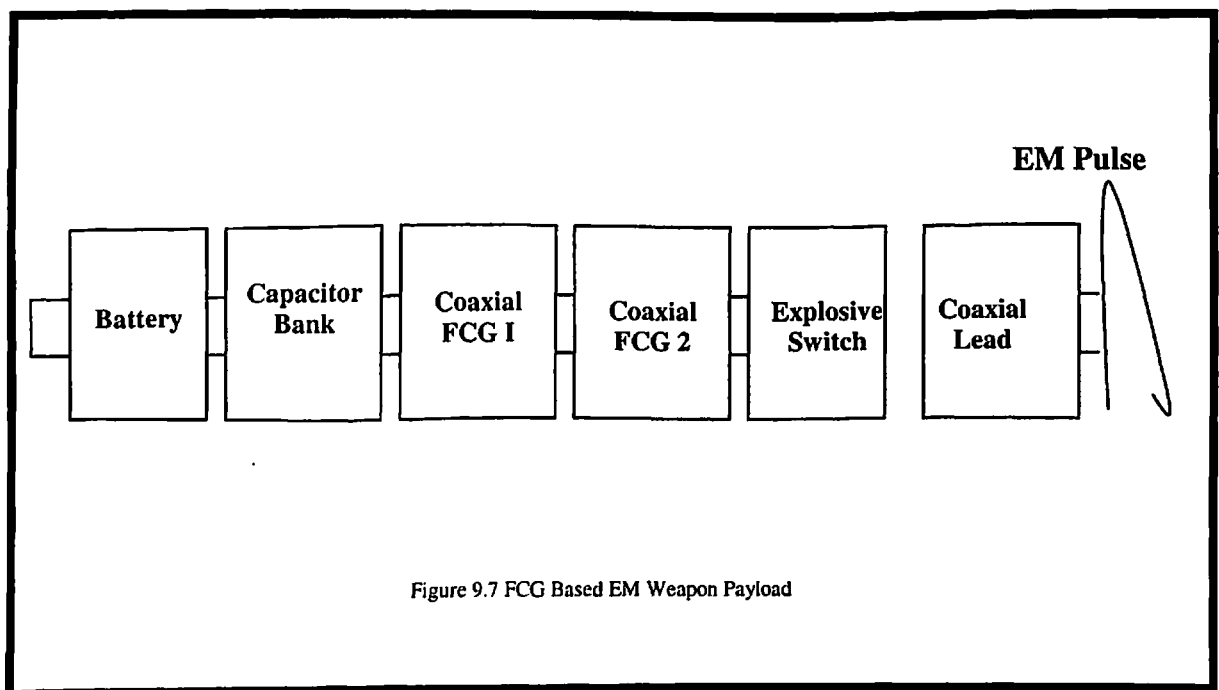


Figure 9.7 FCG Based EM Weapon Payload

9.5.3 Target Placement vis-à-vis Weapon

It can be possible to simply guide the bomb very close to the target, and rely upon the near field produced by the FCG winding, which is in effect a loop antenna of very small diameter relative to the wavelength. Whilst coupling efficiency is inherently poor, the use of a guided bomb would allow the warhead to be positioned accurately within meters of a target.

9.5.4 Design Aspect of Low Frequency EM and HPM Weapons

The low frequency bombs can damage or destroy magnetic media, as the near fields in the vicinity of a flux generator are an order of magnitude of the coercivity of most modern magnetic materials. These weapons can instantly wipe out tapes, discs, floppies or similar magnetic media in libraries, electronic record rooms, databases, web sites etc. Microwave bombs have a broader range of coupling modes and given the small wavelength in comparison with bomb dimensions. They can be readily focused against targets with a compact antenna assembly. Assuming that the antenna provides the required weapon footprint, following two mechanisms can be employed to further maximize lethality.

- **Frequency Sweeping:** The first option can be by sweeping the frequency or chirping the Vircator. This can improve coupling efficiency in comparison with a single frequency weapon, by enabling the radiation to couple into apertures and resonance over a range of frequencies. In this fashion, a larger number of coupling opportunities can be exploited.
- **Emission Polarization:** The second mechanism, which can be exploited to improve coupling, is the polarization of the weapon's emission. If we assume that the orientations of possible coupling apertures and resonance in the target set are random in relation to the weapon's antenna orientation, a linearly polarized emission will only exploit half of the opportunities available. A circularly polarized emission will exploit all coupling opportunities. This would enhance lethality considerably. However the practical constraint is that it may be difficult to produce an efficient and high power circularly polarized antenna design, which is compact and performs over a wide band. Some focused research therefore needs to be done on tapered helix or conical spiral type antennas capable of handling high power levels. A suitable interface to a Vircator with multiple extraction ports can be devised. A possible implementation is depicted in Fig. 9.8 [41]. In this arrangement, power is coupled from the tube by stubs, which directly feed a multi-filar conical helix antenna. An implementation of this scheme would need to address the specific requirements of bandwidth, beam width, efficiency of coupling from the tube, while delivering circularly polarized radiation.

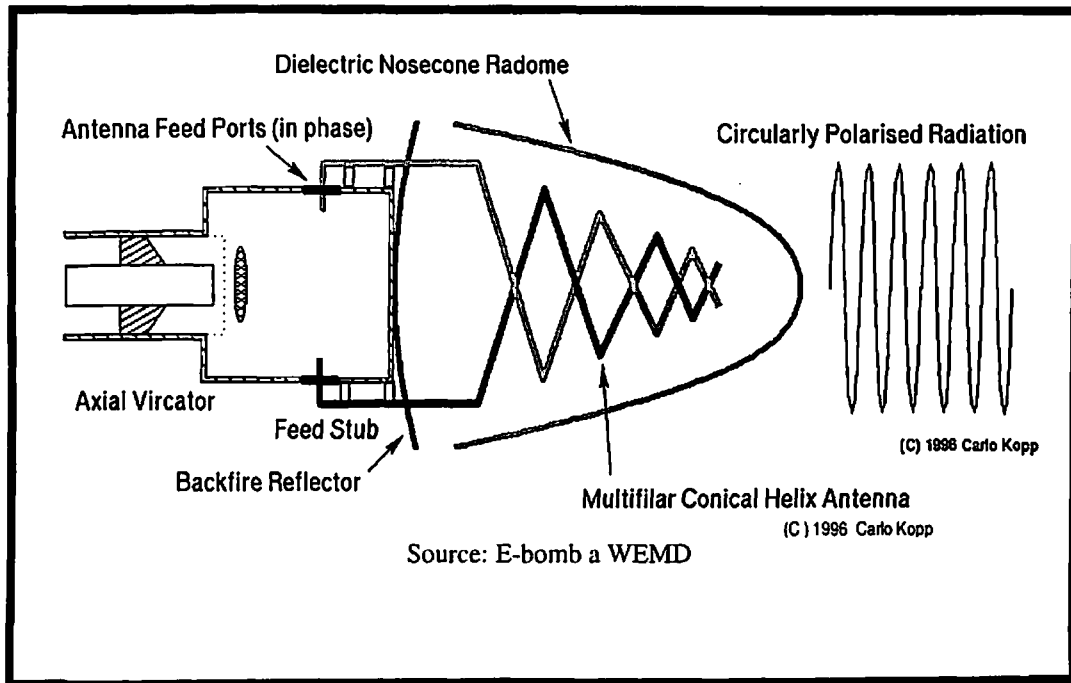


Figure 9.8: Packaging of HPM Vircator Based Device.

- The packaging of a HPM Vircator based device and low frequency E-Bomb is illustrated in figured 9.9 and 9.10.

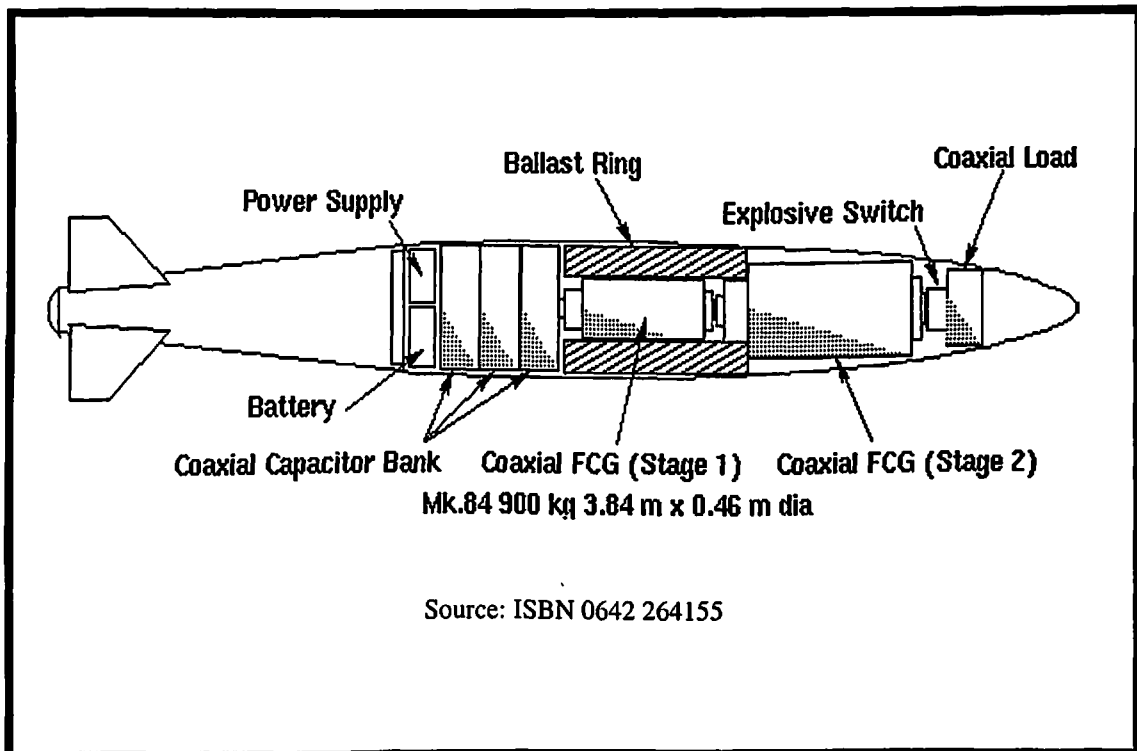


Figure 9.9: Low Frequency E-Bomb - General Arrangement for Packaging

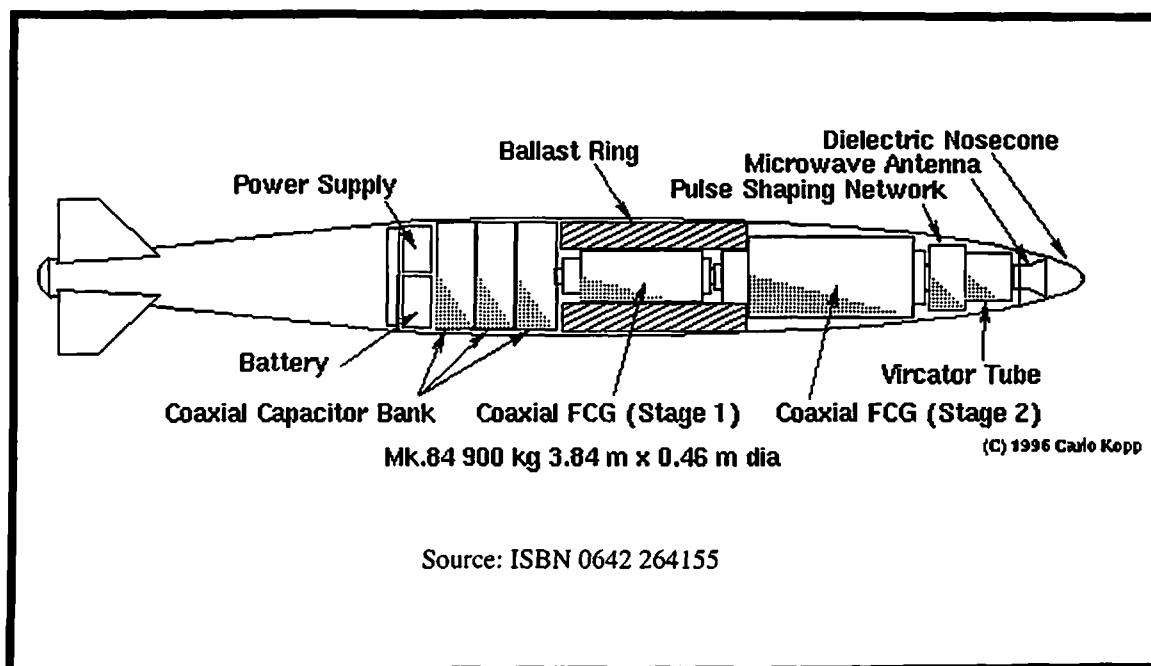


Figure 9.10: Packaging Using Vircator and 2Stage Flux Compression Generator

9.5.5 Detonation Altitude

Another aspect of electromagnetic bomb lethality is its detonation altitude. By varying the detonation altitude, a tradeoff may be achieved between the size of the lethal footprint and the intensity of the electromagnetic field in that footprint. This provides the option of sacrificing weapon coverage to achieve kills against targets of greater electromagnetic hardness, for a given bomb size as shown in figure 9.1.

9.6 Doctrines for Use of EM Weapons

The EM weapons would have to be developed in offensive and defensive role for a credible military posture. The deployment of these weapons will have to be in unison with conventional weapons. Therefore the existing operational doctrines will have to be modified and supplemented. The IW capability as applicable to use of EM weapons will have to be created in all three Services with requisite sensitivity to operational roles, interoperability, and command and control structure.

A basic tenet of IW is that complex organizational systems such as governments, industries and military forces cannot function without the flow of information through their structures. Information flow within these structures takes place in several directions, under typical conditions of function. A diverse military model for this functional role would see commands and directives flowing outward from a central decision making element, with information about the state of the system flowing in the opposite direction. The doctrines as applicable to conventional weapons systems in respect of following operational functions of the Armed Forces have been examined for use of EM weapons. These have been mapped for all the target categories described in modified Wardens Model.

- Electronic Combat Operations (ECO)

- Strategic Air Attack Operations (SAAO) with special focus on targeting leadership, infrastructure and military targets
- Air Defense Operation (ADO)
- Maritime Operations (MO)
- Operations in Land Battle (OLB)

A brief overview of each of these elements of the model is given in the succeeding paragraphs. The target spectrum vis-à-vis vulnerabilities are illustrated in figure 9.11.

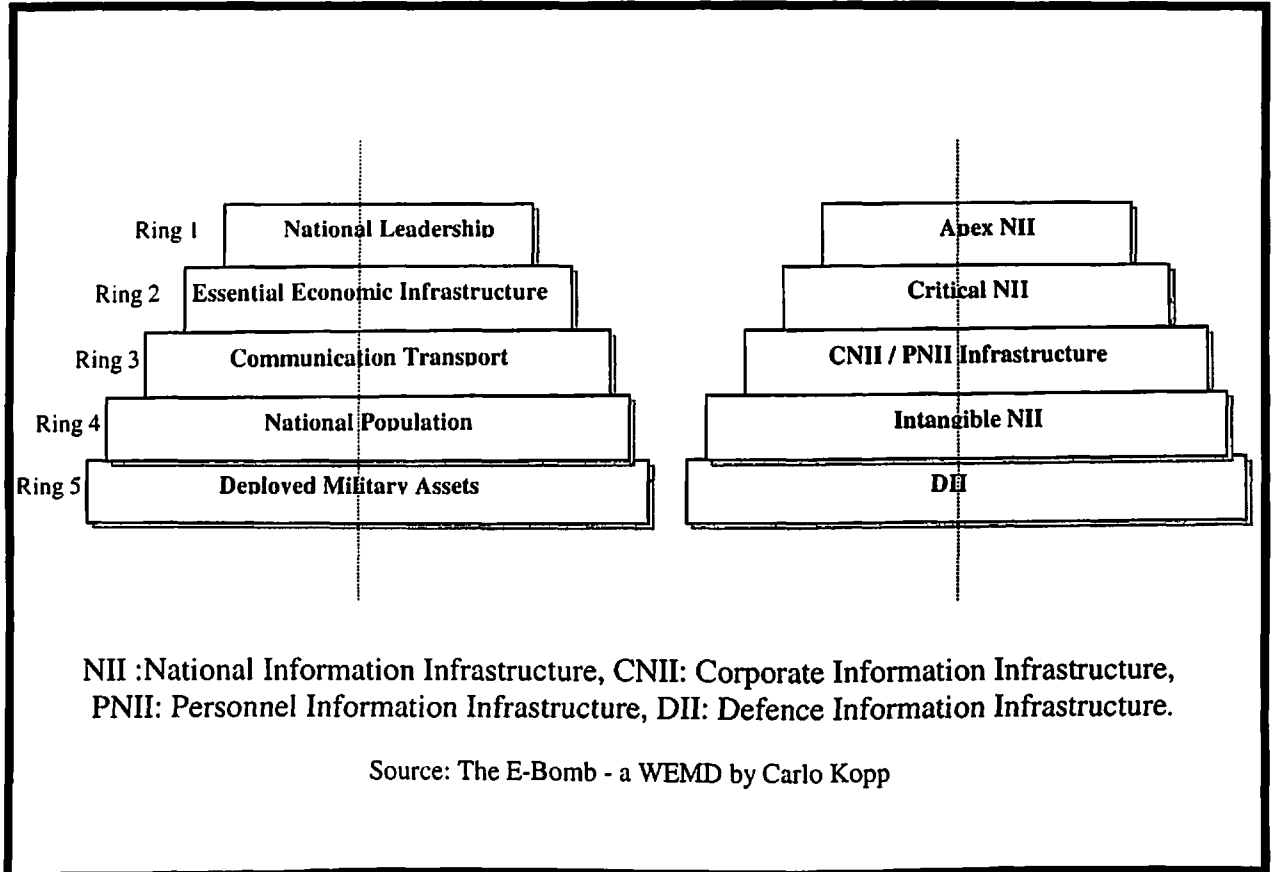


Figure 9.11: Mapping Warden's Model into NII

9.6.1 Proposed Combat Model for Use of EM Weapons

The Warden's 5 Ring model is proposed to be mapped for EM weapons as shown in figure 9.12.

Warden 5 Ring Combat Model	Proposed EM Weapon Combat Model
Ring 1 : National Leadership	Apex Nodes <ul style="list-style-type: none"> - National Security Council - Defence Headquarters - Ministry of Home, External Affairs, Defence and Finance. - Critical Governance Nodes.
Ring 2: Critical National Information Infrastructure	Information Infrastructure of the <ul style="list-style-type: none"> - Banking & finance. - Energy (oil, gas, coal & power). - Water & healthcare. - Transport (rail, road && air). - Telecom & Satellites.
Ring 3: Population	Information Infrastructure of <ul style="list-style-type: none"> - TV, media & cellular system. - Internet gateways.
Ring 4: Industry	IT, Software Technology parks & Manufacturing Plants etc.
Ring 5 : Armed Forces	C³I components, airports, missile bases etc.
<p>Source: E-Bomb - a WEMD, Carlo Kopp. Figure 9.12: Mapping warden Model for EMP Weapons.</p>	

9.6.2 Targeting Apex NII: Leadership (Innermost Ring)

9.6.2.1 Targeting Strategy

The innermost ring in the model comprises of political leadership, government bureaucracies and civilian and military elements of C⁴ISR systems. These are heavily dependent upon the use of computer and communications equipment and therefore prone to damage by EM weapons [68].

9.6.2.2 Vulnerability of Apex Nodes

The decentralization and networking of information technology systems produces a major vulnerability to electromagnetic attack. Whereas a small number of larger computers could be defended against electromagnetic attack by the use of electromagnetic hardened computer rooms, a large distributed network cannot. Unless optical fiber networking is used, the networking cables are themselves a medium via which electromagnetic effects can be efficiently propagated throughout the network, to destroy machines. Whilst the use of distributed computer networks reduces vulnerability to attack by conventional munitions, it increases vulnerability to attack by

electromagnetic weapons. As a defensive measure it would be necessary to design an in built immunity to EM weapons in terms of media and fiber. This is particularly opportune time since most part of NII in strict sense is still at planning and for India, stage and therefore considerable safety can be embedded.

9.6.2.3 Vulnerability of Support Infrastructure

Other targets, which fall into the innermost ring are the satellite links and control facilities. These are vital means of communication as well as the primary interface to military and commercial reconnaissance satellites. Television and radio broadcasting stations, one of the most powerful tools of any government, are equally vulnerable to electromagnetic attack due the very high concentration of electronic equipment in such sites. Telephone exchanges, particularly later generation digital switching systems, are also highly vulnerable to appropriate electromagnetic attack.

9.6.2.4 Damage Assessment

Selective targeting of government buildings with EM weapons will result in a substantial reduction in a government's ability to handle and process information. The damage inflicted upon information records will be permanent. This would be particularly dangerous if the appropriate backup strategies have not been used to protect stored data. Following exposure to EMP, most data stored on affected machines, which are affected, will perish with the host machine, or become extremely difficult to recover from damaged storage devices. This would virtually incapacitate the decision making and war support elements of the government agencies. This makes the defensive exercise far more stringent.

9.6.2.5 Cost of Protecting Govt. Assets Against EM Weapons

The cost of hardening existing computer networks would be prohibitive, Similarly the cost of replacement of existing equipment with hardened equipment would be prohibitive. The use of hardened equipment for critical tasks would provide some measure of resilience. However discipline required in the handling of information to implement such a scheme renders its utility outside of military organizations questionable. Therefore the use of electromagnetic weapons against government facilities offers an exceptionally high payoff.

9.6.2.6 Cost Benefit Ratio of Using EM Weapons

Use of EM weapons against leadership and components of C⁴I²SR as targets is highly profitable. A modest number of weapons appropriately used can introduce the desired state of strategic paralysis, without the substantial costs incurred by the use of conventional munitions to achieve the same effect.

9.6.3 Targeting Critical NII

Economy & Governance, (Second Inner-most Ring): The critical NII represented by second innermost ring pertains to information infrastructure of energy, banking, finance, transport, water, emergency services, power governance, telecommunications etc. These components are largest users of electronics and hence very vulnerable.

9.6.3.1 Vulnerability and Damage Potential

Attack on these of targets will halt almost all operations. The time required to either repair the destroyed equipment, or to reconfigure for manual operation will be large and make the recovery difficult. The multiple and multistage failures will have cascading effect with little potential for quicker recovery unless designed with that objective. Some production processes however require automated operation, either because hazardous conditions prevent human intervention, or the complexity of the control process required cannot be carried out by a human operator in real time as in the case of nuclear power plant and oil/gas production facilities. Destroying automated control facilities will therefore result in substantial loss of production, causing shortages of these vital materials. This can result in virtual paralysis of economy.

- The finance industry and stock markets are a special case in this context, as the destruction of their electronic infrastructure can yield, unlike manufacturing industries, much faster economic dislocation. This can in turn produce large systemic effects across the whole economy, including elements, which are not vulnerable to direct electromagnetic attack. This may be of particular relevance when dealing with an opponent which does not have a large and thus vulnerable manufacturing economy. For instance most of India's neighbors including India itself rely on agriculture, mining or trade for a large proportion of the gross domestic product. These countries including India are prime candidates for electromagnetic attack on their finance industry and stock markets. Since the latter are usually geographically concentrated and typically electromagnetically "soft" targets, they are highly vulnerable to EM-Weapon attacks. Therefore a large payoff in striking at critical NII, particularly in the opening phase of a strategic air attack campaign can be achieved. In terms of offense the centers of gravity within the target economy must be properly identified and prioritized for strikes to ensure that maximum effect is achieved as quickly as possible. On the other hand protection of own assets is equally critical and measures and strategies must be in place.
- The automated railways and road signaling systems are most vulnerable and can be used to produce traffic congestion by preventing the proper scheduling of rail traffic. The disabling of road traffic signaling may not yield much useful effect, except in metropolis. There the delays and dislocation can be expected, which can hamper military convoy movements or delay their response time. The Air Traffic Control system can be disabled to cause telling effect by causing closure like conditions. Similarly the port control facilities can be disabled to cause congestion and stoppage of craft movements.
- Most modern automobiles and trucks use electronic ignition systems, which are known to be vulnerable to EM weapons effects. However to find such concentrations so as to allow the desired effects may be difficult. In any case the cost-benefit ratio of causing traffic congestions would be too low.

9.6.4 Disruption of Industry: IT, Telecom, STPs, Manufacturing: (Fourth Innermost Ring)

Some military planners tend to base their events on historical opinion, which suggests that manufacturing industries are highly resilient to air attack as production machinery is

inherently mechanically robust and thus a very high blast overpressure is required to destroy it. This is not true any longer, because, the proliferation of electronic and computer controlled machinery has produced a major vulnerability, for which historical precedent does not exist. Therefore it will be necessary to reevaluate this orthodoxy in targeting strategy. Some of the manufacturing industries such as the electronics, computer and electrical industry, precision machine industry and aerospace industries rely heavily upon robotic and semiautomatic machinery. These industries are all key assets in supporting a conventional military capability. They are all highly vulnerable to electromagnetic attack. Whilst material processing industries may in some instances be capable of functioning with manual process control, the manufacturing industries are almost wholly dependent upon their automated machines to achieve higher production output and therefore vulnerable.

9.6.5 National Populace: Media, Internet, Telephones (Fourth Innermost Ring)

9.6.6 Armed Forces

Command Shelters, Weapon Depots, Airports, (Outer Ring): The C⁴I²SR nodes, fixed support bases as well as deployed forces can be attacked with EM weapons. Fixed support bases which carry out depot level maintenance on military equipment offer a substantial payoff, as the concentration of computers in both automatic test equipment and administrative and logistic support functions offers a good return per expended weapons pay load.

Any site where complex military equipment is concentrated, if attacked with EM weapons, would render the equipment unserviceable and hence reduce the fighting capability. Mobility of the targeted force would be retarded. The ability of EM weapons to achieve hard electrical kills will make them undefended and non-operational. Whether to expend conventional munitions on targets in this state would depend on the immediate military situation and the over all war objectives.

In summary the EM weapons offer a potentially high payoff, particularly when applied to leadership, and vital economic targets, all of which can be deprived of much of their function for substantial periods of time. The concentrated application of EM weapons in the opening phase of the campaign would introduce paralysis within the government, deprive it of much of information processing infrastructure, as well as paralysis in most vital industries. This can greatly reduce the capability of the target nation to conduct military operations of any substantial intensity.

9.6.6.1 Attack Strategy

ECO would involve the use of these weapons to attack radar, C3 elements of C⁴I²SR and air defense weapon systems. These can be attacked initially with EM weapons to achieve soft or hard electrical kills, followed up by attack with conventional munitions to preclude possible repair of disabled assets at a later time. As with conventional operations, the greatest payoff can be achieved by using EM weapons against systems of strategic importance first, followed by those of tactical importance.

9.6.6.2 Kill Potential of EMP –Weapons

EM weapons can cause both soft and hard electrical kill, subject to the lethality of the weapon and the hardness of its target. A hard electrical kill can be achieved in those

instances where a target would require the replacement of most, if not all of its internal electronics.

9.6.6.3 Force Multiplier Effect or Weapon of Electrical Mass Destruction (WEMD)

In comparison with an Anti Radiation Missile (ARM) the established and specialized tool in the conduct of ECOs, (which happens to be a missile which homes on the emissions from a threat radar), an EM weapon can achieve kills against multiple targets of diverse types within its lethal footprint and therefore can serve as a significant force multiplier.

9.6.6.4 Intensity of Operations vis-à-vis Asset Requirements

Conventional Electronic Combat Campaign (ECC), or Intensive Electronic Combat Operations (IECO), will initially concentrate on saturating the opponent's electronic defenses, denying information and inflicting maximum attrition upon electronic assets. The force multiplication offered by EM weapons can vastly reduce the number of air assets required to inflict same attrition. If proper electronic reconnaissance has been carried out before hand, it would also reduce the need for specialized assets such as ARM firing aircraft equipped with costly emitter locating systems. The concentrated application of EM weapons through saturation attacks in the opening phase of an electronic battle can allow much faster attainment of command of the electromagnetic spectrum, as it can inflict attrition upon electronic assets at a much faster rate than possible with conventional means.

9.6.6.5 Kill Capability

A single aircraft carrying an EM weapon can be capable of concurrently disabling a SAM site with its collocated acquisition radar and supporting radar directed AA weapons. It will therefore have the potency equivalent to several ARM firings plus support-jamming aircraft required to accomplish the same result by conventional weapons. This ability of EM Weapons and the ability of multi role tactical aircraft to perform this task can allow for a much greater concentration of force in the opening phase of the battle, for a given force size. This strategy can play decisive role in naval operations and the fleet can be rendered extremely vulnerable.

Therefore the saturation attacks using EM weapons in the ECO can provide for a much faster rate of attrition against hostile electronic assets, achievable with a significantly reduced number of specialized and multi role air assets. This will allow even a modestly sized force particularly in the context of naval aviation assets (if an air cover for this role from the air force is not available) to apply overwhelming pressure in the initial phase of an electronic combat battle, and achieve command of the EM spectrum in a significantly shorter time than by conventional means. The effectiveness of ECO using EM weapons is summarized below.

- Combination of hard and soft kill required for total effect
- Kill ability against large spectrum of electronics
- Coverage of tactical and strategic assets
- Equally amendable to use by Army, Navy and Air Force
- High damage vis-à-vis asset ratio
- Technology not yet perfected and model lacks proofs of effectiveness

9.6.7 Doctrine for EM Weapons in Electronic Combat Operations (ECO)

9.6.7.1 Ability

The ability of EM weapons to achieve kills against a wide range of target types makes them suitable for inflicting attrition upon an opponent's electronic assets, viz. air defense assets, Command-Control-Communications (C3) elements of C⁴I²SR and other assets of military intent [38].

9.6.8 Maritime Operations Doctrine for Use of EM Weapons

9.6.8.1 Electronics Intensive Equipment

As with modern military aircraft, naval surface combatants and submarines are fitted with a substantial volume of electronic equipment, performing similar functions in detecting and engaging targets and warning of attack. Therefore they are extremely vulnerable to electromagnetic attack, if not suitably hardened. Should they be hardened, volumetric, weight and cost penalties will have to be incurred which would be substantial [119].

9.6.8.2 Conventional Naval Attack Strategy

Conventional methods for attacking surface combatants involve the use of saturation attacks by anti-ship missiles or coordinated attacks using a combination of ARMs and anti-ship missiles. The latter instance is where disabling the target electronically by stripping its antennae precedes lethal attack with specialized anti-ship weapons.

9.6.8.3 Proposed EM weapons Strategy

An EM warhead detonated within lethal radius of a surface combatant will render its air defense system inoperable, and damage other electronic equipment such as electronic counter measures, electronic support measures, communications navigation, power and steering systems. This can leave the vessel undefended until these systems can be restored, which may or may not be possible on the high seas. Launching an EM glide bomb on to a surface combatant, and then attack it with laser or television guided weapons can be an alternate strategy for dealing with such high value targets.

9.6.8.4 Lethality of EM weapons Against Naval Targets

The EM weapon attack on an aircraft carrier can have devastating effect and cripple the task force groups irreparably. The disability or damage caused to surveillance radars and landing systems would render aircraft launch, direction, interception and recovery extremely difficult. Damage to electrical circuits would render lift operations and hence movement and stowage of aircraft difficult and time consuming. Following points in particular make the naval forces vulnerable.

- The aircraft carrier as a platform is dependent for its own defense upon other fleet units in the company. The loss of communications with the rest of fleet will make it even further vulnerable to such attacks.
- The most critical case in point can be the EM weapon attack on sea-lanes to cripple merchant shipping assets of a target nation. For example a concentrated air attack using EM weapons could disable communications and electrical systems of merchant ships making them absolutely blind even for want of navigational aids.

The EM weapons can also be launched from oil rigs or similar strategic locations, if the air assets are not deployable

9.6.8.5 Amphibious Operations

The amphibious operations using the conventional weapons involve saturation attacks on the enemy defenses so that beaching operations can be conducted with relative ease and with least loss of own assets. The saturation attack by EM weapons on the harbors or beach-heads can silence not only the command shelters but would also neutralize most of the infrastructure, power supplies and transport system which can lower the potential opposition during the street battle by ground troops. The absence of communications would make coordination efforts of target nation chaotic. On the other hand use of EM weapons for harbor defense as well as to prevent amphibious operations can be very effective against ship and other targets unless submarine launched weapons are being used to nullify the harbor defenses. EM weapons can also be very effectively used to force blockade in the harbors, busy sea-lanes and choke points.

9.6.9 Land Battle Doctrine for EM Weapons

The modern land warfare doctrine lays extensive emphasis on mobility. Therefore maneuver warfare methods are typical for contemporary land warfare. Coordination and control are essential to the successful conduct of maneuver operations, and this provides another opportunity to apply EM weapons. In land warfare operations the communications and command shelters are key elements in the force structure of a land army, and these concentrate communications and computer equipment. They can be attacked with EM weapons, to disrupt the command and control of land operations. For instance, during the war, if concentrations of armoured vehicles is found, these can be profitable targets for attack, as their communications and fire control systems can be substantially damaged or disabled.

A useful tactic would be to launch initial attack with EM weapons to create maximum confusion in mobility by disabling ignition systems of vehicles, followed by attack with conventional weapons to take advantage of the immediate situation. Land battle scenario is very dynamic in nature and therefore deployment of EM weapons need to be done with care and caution. For example in a close battle, discrimination between own and enemy assets deployed in the same area may become very difficult due to fast changing movement of troops on both the sides. The footprint, coverage and lethality in respect of EM weapons for close range and highly maneuvering target profile is a new area for research. Since there is no precedence of such operations and the above parameters in warfare doctrines still remain vague and untested, the effectiveness of EM weapons for land warfare opportunities need further investigation and research.

9.6.10 Defensive Counter-Air Operations

Using EM Weapons: As the compact EM warheads in future are built with useful lethality and performance, a number of other potential applications will become viable. One such application can be to equip an Air-Air Missile (AAM) with such a warhead. A weapon with data link for midcourse guidance can be used to break up inbound raids by causing soft or hard electrical kills in a formation of hostile aircraft. If this can be achieved, the defending fighters will have the advantage in following any engagement,

as the hostile aircraft may not be fully mission capable. Loss of air intercept or attack radar, electronic warfare equipment, its mission computers, digital engine controls, communications and electronic flight controls, where fitted, could render the victim aircraft defenseless against attack with conventional missiles. Numerous other low level tactical applications relating to sabotage operations or low intensity warfare using paramilitary forces can also be evolved around these class of EM weapons through further research.

9.6.11 Graduated Response Strategy for Use of EM Weapons

The induction of EM weapons into the inventory can considerably broaden the options for conducting strategic campaigns. Such weapons can indeed be potent force multipliers in conducting a conventional war, particularly when applied to Electronic Combat, OCA, strategic air attacks naval and land operations. The concentrated use of such weapons can provide a decisive advantage to any nation, which has EM weapon capability to effectively target and deliver them. The qualitative advantage in capability so gained can provide a significant gain even against a much stronger opponent not in the possession of this capability.

- These weapons also open up less controversial alternatives for the conduct of a strategic campaign. This is possible primarily due to their ability to inflict significant material damage without inflicting visible collateral damage and loss of life. As seen in the recent past, and in foreseeable future, many governments would be reluctant to commit to strategic campaigns. It is because the expectation of a lengthy and costly battle, with mass media coverage of its highly visible results, will quickly produce domestic political pressure to cease the conflict. For instance we cannot repeat events of 1971 war and its preparatory phase any more. The propaganda through TV media itself will bring considerable domestic and international pressure to stop this activity.
- In this strategy, an opponent who threatens escalation to a full-scale war can be preemptively attacked with EM weapons, to gain command of the electromagnetic spectrum and control of the air space. Selective attacks with EM weapons may then be applied against chosen strategic targets, to force concessions. If these fail to produce results, more targets can be disabled by EM weapons attack. Escalation would be sustained and graduated, to produce steadily increasing pressure to concede to the dispute. Air and sea blockades are complementary means via which pressure may be applied.
- It needs to be recognized that EM weapons can cause damage on a large scale very quickly. The rate at which damage can be inflicted can be very rapid, virtually at light speed. In this respect such a campaign will differ from the conventional campaign, where the rate at which damage is inflicted is limited by the usable sortie rate of strategic air attack capable assets.
- In case blockade and the total disabling of vital economic assets fail to yield results, these may be systematically attacked by conventional weapons, to further escalate the pressure. Finally, a full-scale conventional strategic air attack campaign can follow, to wholly destroy the hostile nation's war fighting capability.
- There is yet another situation where EM weapons will find useful application. This pertains to governments, which, actively implement a policy of state-sponsored

terrorism or info-terrorism, or alternately choose to conduct a sustained low-intensity land warfare campaign. Typical example in our case is the insurgency operations by Inter Services Intelligence (ISI) in Jammu and Kashmir. The strategy of graduated response, using electromagnetic bombs in the initial phases, can place the offending government under significant pressure to concede.

9.6.12 Strategies for Maximum Effect of EM-Weapons: - Integrated Warden's Model

- The long-term effects of a sustained and concentrated strategic bombing campaign using a combination of conventional and EM weapons will be important. The cost of computer and communications infrastructure is substantial, and its disability and destruction would be a major economic burden for any industrialized nation. In addition poor protection of stored data will add to further economic losses, as much data will be lost with the destroyed machines. Moreover it would paralyze the organizational functionality.
- Attack by EM weapons can decisively achieve many of the central objectives of neutralizing an enemy. The concentrated application of these weapons can inflict attrition on an opponent's information processing infrastructure in quick succession, and this would arguably add a further psychological dimension to the potency of the attack. Unlike the classical IW model of in which the opponent can arguably isolate his infrastructure from hostile penetration. Parallel or hyper war style saturation attack with electromagnetic weapons can be extremely difficult to defend against.
- The EM weapons can play extremely important and decisive role in Command and Control, Psychological, Economic and Electronic Warfare. In offensive role, the very knowledge about the availability of EM weapons in an opponent's inventory can cause a deterrent effect. Since the successful outcome of such IW campaigns cannot be assessed, the effectiveness of EM weapons for IW role would be debated amongst various agencies for some more time to come. As an extension to this part of the doctrine a neighboring state may indulge in use of EM Weapons for terrorist activities as a part of insurgency operations or psychological warfare as an extension of it's adventurous strategy. But cost of such adventure when used against a nation who possesses EM weapons can be extremely high and unbearable for the erring state.
- The approach to strategic air warfare should be devoted to disabling an opponent's fundamental information processing infrastructure. There is a need to evolve a systematic IW doctrine, which has been tested and refined.

9.7 Defense Against EM Weapons

A weapon development program would necessarily have elements of defensive and offensive warfare capabilities. In the previous section we have seen the lethality of EM Weapons against the NII. When such weapons are deployed by the enemy, we need to neutralize their effect. On the other hand when we deploy these weapons against enemy targets we need to be aware of what defence the enemy can have against our EM Weapons so that we use requisite tactics and strategies for maximum effect. Also if the defensive measures of the enemy are known to be proven and potent, there would be a need to refine our offensive weapons. This iterative process of building offensive-

defensive layers only can make the program comprehensive enough for credible effect. These issues are examined in succeeding paragraphs [42,62,63,64,75,127,128].

9.7.1 Destruction or Disabling of Delivery Platforms

In the previous section we have seen that the EM weapons can be delivered by aircraft, missiles, torpedoes or as directed energy through fixed or movable platforms. Therefore the most effective defence against electromagnetic weapons would be to prevent their delivery by destroying or disabling the launch platform or delivery vehicle, as is the case with nuclear weapons.

9.7.2 Hardening of Sites Prone to EM Weapons

The cent percent neutralization or physical destruction of delivery platforms will not be possible. Therefore systems which can be expected to suffer exposure to the EM weapons effects must be electromagnetically hardened. Some of these schemes and technologies are highlighted in the following paragraphs.

9.7.3 Use of Faraday's Cage

The most effective method would be to wholly contain the equipment in an electrically conductive enclosure, termed as a "Faradays Cage". This can prevent the electromagnetic field from gaining access to the protected equipment. However, most such equipment must communicate with and be fed with power from the outside. This can provide entry points via which electrical transients may enter the enclosure and affect damage. While optical fibers can address this requirement for transferring data in and out, electrical power feeds remain an ongoing vulnerability. Therefore this solution may not offer cent percent safety. A typical protection scheme is illustrated in figure. 9.13. Wherever an electrically conductive channel must enter the enclosure, electromagnetic arresting devices must be fitted. A range of such devices exist, however care must be taken in determining their parameters to ensure that they can deal with the rise time and strength of electrical transients produced by electromagnetic devices. The literature survey indicates that hardening measures attuned to the behavior of nuclear EMP bombs do not perform well when dealing with some conventional microwave electromagnetic device designs. This should form an area of research.

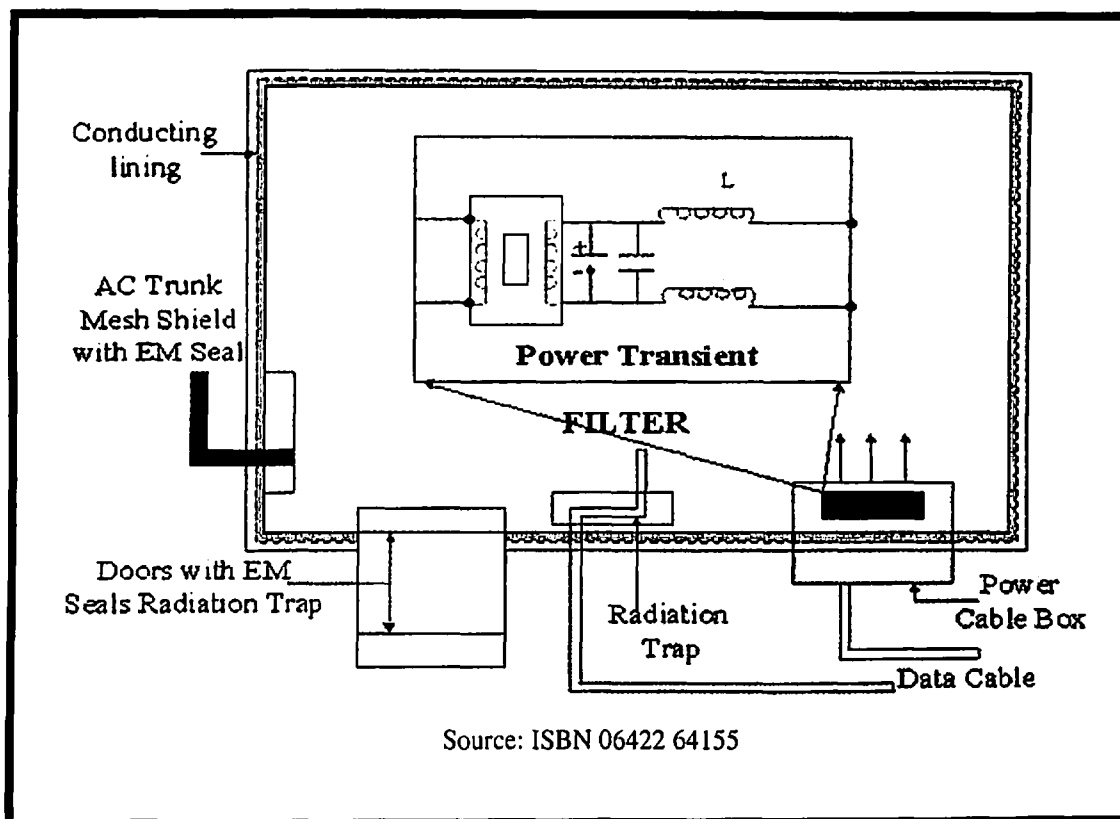


Figure 9.13: Typical Hardening Arrangement

9.7.4 Hardening at System Level

The hardening of systems must be carried out at a system level, as electromagnetic damage to any single element of a complex system could inhibit the function of the whole system. Hardening of newly built equipment and systems will add a substantial cost burden. Older equipment and systems may be impossible to harden properly and may require complete replacement. In simple terms, hardening by design is significantly easier than attempting to harden the existing equipment.

9.7.5 Quality of Hardening

A significant aspect of electrical damage to targets is the possibility of wounding semiconductor devices thereby causing equipment to suffer repetitive intermittent faults rather than complete failures. Such faults would tie down considerable maintenance resources while also diminishing the confidence of the operators in the equipment's reliability. Intermittent faults may not be possible to repair economically, thereby causing equipment in this state to be removed from service permanently, with considerable loss in maintenance hours during damage diagnosis. This factor must also be considered when assessing the hardness of equipment against electromagnetic attack, as partial or incomplete hardening may cause more difficulties than it would solve. On the other hand an incomplete, shielding may resonate when excited by radiation and thus contribute to damage inflicted upon the equipment contained within it. Therefore a well thought out hardening strategy would be needed.

9.7.6 Judicious Use of Emitters

Other than hardening against attack, facilities that are concealed should not radiate readily detectable emissions. Where radio frequency communications must be used, low probability of intercept techniques should be employed exclusively to preclude the use of site emissions for electromagnetic targeting purposes. Appropriate suppression of Undetected Emissions is also mandatory. This would require further research in developing systems using spread spectrum/equalizer techniques.

9.7.7 Protection of Networks

Communications networks for voice, data and video services should employ topologies with sufficient redundancy and failsafe mechanisms to allow operation with multiple nodes and links interoperative. This will deny a user of electromagnetic bombs the option of disabling large portions if not the whole of the network by taking down one or more key nodes or links with a single or small number of attacks. As most of NII's computerization and networking efforts are underway such serial and parallel redundancies should be evolved as a part of design so that the architecture, configurations, topologies are built accordingly.

9.7.8 Revival of Thermionic Technology

The thermionic technology (i.e. vacuum tube equipment) is substantially more resilient to the electromagnetic weapons effects than solid state (i.e. transistor) technology. Therefore a weapon optimized to destroy solid state computers and receivers may cause little or no damage to a thermionic technology device. Therefore a hard electrical kill may not be achieved against such targets unless a suitable weapon is used. Recognizing this aspect erstwhile Soviet Union had revived their valve technologies and critical systems such as reconnaissance aircraft and missile tracking sites are known to be fitted with this equipment. USA too is known to have been considering this option seriously. A serious evaluation of these options and the potential of BEL, HAL, ECIL and ITI to revive old technology and manufacturing lines will have to be examined.

9.8 EM Weapons for IW-Defense

Modern aircraft are densely packed with electronics, and unless properly hardened, are highly vulnerable targets for EM weapons. Therefore EM weapons can be very effectively used for Air Defense operations. Also cost of the onboard electronics represents a substantial fraction of the total cost of a modern military aircraft. Therefore stock levels of spares will in most instances be limited to what is deemed necessary to cover operational usage at some nominal sortie rate. The damage inflicted by the EM weapons to attacking aircraft could render them unusable for substantial periods of time. The above analogy is also applicable to air defense operations using area defense Surface to Air Missiles (SAMs). Large SAMs such as AKASH and TRISHUL can accommodate an EM warhead comparable in size to a bomb warhead. A SAM site subjected to jamming by inbound bombers could launch a first round under data link control with an EM warhead to disable the bombers, and then follow up with

conventional rounds against targets, which may not be able to defend themselves electronically. This has obvious implications for the electromagnetic hardness of combat aircraft systems.

9.9 Defense Against Air Attacks

Saturation attacks on the airfields with EM weapons can disable communications, air traffic control facilities, navigational aids and operational support equipment; if these items are not suitably electromagnetic hardened. Conventional blast hardening measures will not be effective, as electrical power and fixed communications cabling will carry electromagnetic induced transients into most buildings. Hardened aircraft shelters may provide some measure of protection due to electrically conductive reinforcement embedded in the concrete, However conventional rivetments will not be effective. Therefore operations against airfields and aircraft on the ground should include the use of EM weapons for counterattack against the incoming aircraft. The warheads fired in defence need to denote in the correct vicinity of high speed incoming aircraft for any meaningful effect. This is an area of research, design and development as they offer the potential to substantially reduce hostile sortie rates. This is analogous to neutralizing the enemy's potential even for first strike capability from certain locations.

9.10 Enforcement of Technology Control Regime Using EM Weapons

The high value targets such as R&D and production sites for Weapons of Mass Destruction (nuclear, biological, chemical) and many vital economic sites, such as petrochemical production facilities, are critically dependent upon electronic equipment. The proliferation of nuclear weapons into developing nations has been greatly assisted by the availability of test and measurement equipment commercially available from Western countries, as well as electronic process control equipment freely available in the world market. Selectively destroying such equipment can not only paralyze R&D effort, but also significantly impair revenue generating production effort. For example a nation sponsoring terrorism may use oil revenue to support such activity. Crippling its primary source of revenue without widespread environmental pollution by use of EM weapons may be an effective and politically acceptable punitive measure. This strategy has been effectively used by USA against Iraq even though using conventional weapons, therefore as a punitive action, EM weapons are attractive for dealing with belligerent governments. Substantial economic, military and political damage can be inflicted with a modest commitment of resources by their users, and without political controversies, collateral damage, or loss of life. There can also be an alternate strategy, whereby a graduated response may be workable. This however needs very clear and unambiguous perspective and understanding of own as well as enemy's assets [118].

9.11 Conclusions

In this chapter we have examined the packaging, induction and deployment of EM weapons in terms of technical, operational and targeting aspects. Following conclusions emerge.

- EM weapons offer applications across a broad spectrum of targets, spanning both the strategic and tactical range. Their use offers a very high payoff in attacking the fundamental information processing and communication facilities of a target nation.

The massed application of these weapons can produce substantial paralysis in any target system, thus providing a decisive advantage in the conduct of Electronic Combat, Offensive Counter Air and Strategic Air Attack, Land Battle engagements and Naval Operations.

- EM Weapons can cause hard electrical kills over larger areas than conventional explosive weapons of similar mass. Therefore they offer substantial economies in force size for a given level of inflicted damage, and are thus a potent force multiplier for appropriate target sets.
- Non-lethal nature of electromagnetic weapons makes their use far less politically damaging than that of conventional weapons, and therefore broadens the range of military options available.
- EM weapons can be a force multiplier. It will help to reduce force sizes for those who have budgetary constraints due to domestic economic compulsions, or nations who heavily depend on import of military equipment to meet their internal as well as external security needs. India happens to suffer from all these constraints and therefore can benefit immensely by successful realization of an EM weapon program.
- The mapping and perfecting the use of Warden's 5 Ring model for use of EM weapons can yield substantial pay off in strategic and tactical terms.
- As of now no historical experience exists upon which a doctrinal model for deployment of EM weapons can be evolved. The immaturity of technology limits the scope of this discussion, because it is difficult to precisely foresee EM weapon potential with existing force structures. Technological evolution will enable us to develop relationship between weapon size and lethality for producing further applications. The doctrines suggested for electronic air combat, maritime operation land battle will require research and refinements to make EM weapon is a very big challenge for the industry and is a subject of further research.

CHAPTER 10

RESEARCH & DEVELOPMENT NEEDS OF THE EM WEAPONS PROGRAM

10.1 Introduction

In chapter 3, 4 and 5 it emerged that unprecedented proliferation of microelectronics has made NII including military systems a "*target rich*" environment for the EMP & HPM energy weapons. In chapters 6, 7 and 8 we surveyed the ongoing developments in these weapons across the globe, assessed level of current maturity of the underlying technologies, program specific budgeted procurements, production and induction of RF and EM energy weapons. We concluded that Information Warfare capability built around EM energy weapons gives deterrence potential comparable to nuclear arsenal and would form a lynchpin for survival and sustenance of any nation including India in the emerging digital era. India has no option but to invest in building this capability.

This chapter presents a research, design and development (RD&D) perspective for the EM weapons, surveys global RD&D efforts encompassing basic sciences, microwave devices, major building blocks viz. pulsed power systems, high energy microwave sources, antennae systems, system engineering, simulation, virtual prototyping, testing, evaluation and protection techniques. It also highlights the research needs of EM weapons and presents outlines of a program for India in terms of technology development, demonstration and evaluation, assessment of effects and lethality, integration with current systems, hardening, protection strategies, assurance program and development of tactical and strategic doctrines.

10.2 Overview of Directed Energy Weapons (DEWs)

The coverage of complete range of laser and EM weapons termed as Directed Energy weapons is beyond the scope of this thesis. This brief preview is presented for completeness sake. The DEWs based on laser and microwave energy are synergistic, complementary and highly capable. Both have following common characteristics: [43]

- Travel at speed of light to the target.
- Capable of graduated effects ranging from deny, disrupt, degrade and complete destruction. They can also be used in defensive role.
- Cause collateral damage.

Their differing characters are presented in figure 10.1.

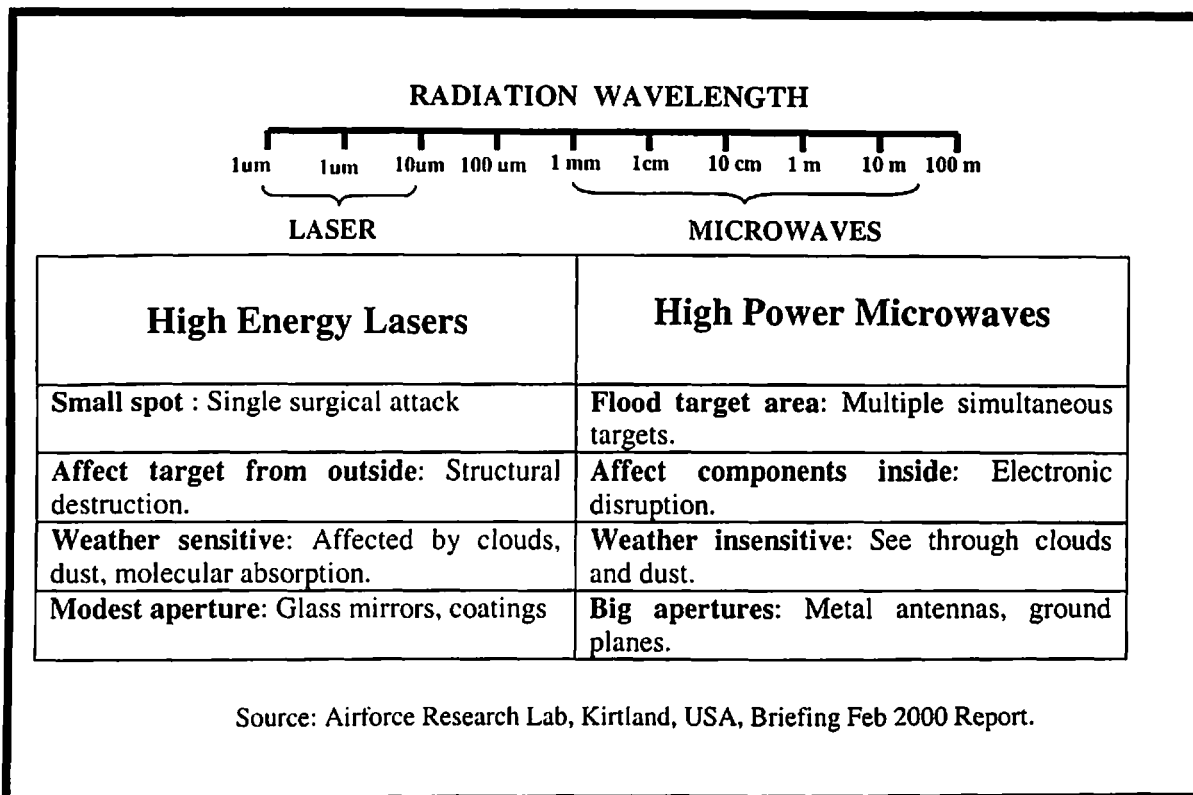


Figure 10.1: Differing Characteristics of Laser and HPM Weapons

10.3 Research Design and Development (RD&D) Perspective

In the preceding chapters we have seen that directed energy will dominate the IT intensive battle space of the early 21st century and probably beyond. Therefore investments in research, design and development can prepare the foundation to conceive and build future military capability in Directed Energy Weapon systems comprising of Laser and Microwave based building blocks. The focused RD&D efforts alone can provide the thought leadership to India in evolving the 21st century IW capability built around EM energy weapons. As Guilio Douhet wrote "*Victory smiles upon those who anticipate the changes in the character of war*". The emergence of DEW is an unprecedented change in the character of War, and, we as a nation need to recognize this and react appropriately. Against the above *background*, India's RD&D perspective should support user needs of DEW applications, address mission area deficiencies, exploit the relevance of directed energy technology to national security needs and create user awareness of the potential of directed energy for defence, industrial and healthcare applications. The idea is to avoid serious technological gaps & obsolescence and explore directed energy avenues that can offer high pays off in terms of capabilities and applications. We therefore need to cast our R & D vision with following user perspective in view.

- **Awareness**: Enhance battlefield awareness with directed energy tools capable of detection and identification.
- **Strike**: Strike deep in the enemy's territory at the speed of light, with little or no collateral damage or loss of life, crippling his ability to wage aggression.
- **Protect**: Protect high value military assets by invisible shields of directed energy.
- **Deterrence**: Provide deterrence with a wide range of graduated force for every military contingency.

The objective is to develop, integrate and transition science & technology for directed energy weapons to include high power microwaves, lasers, adaptive optics, imaging and its effects.

10.4 Survey of Global RD&D Initiatives in DEWs

The RD&D investments in DEWs around the globe are being made in several areas. A summary of ongoing research and developments in the USA is presented in the succeeding paragraphs. Reference to developments in other countries have been avoided due to lack of authentic information available in the open literature [20, 23, 24, 25, 26, 28,57,72,165,196,198,122-115, 120-123,136,165].

- Lasers
- Advanced Optics
- High Power RF

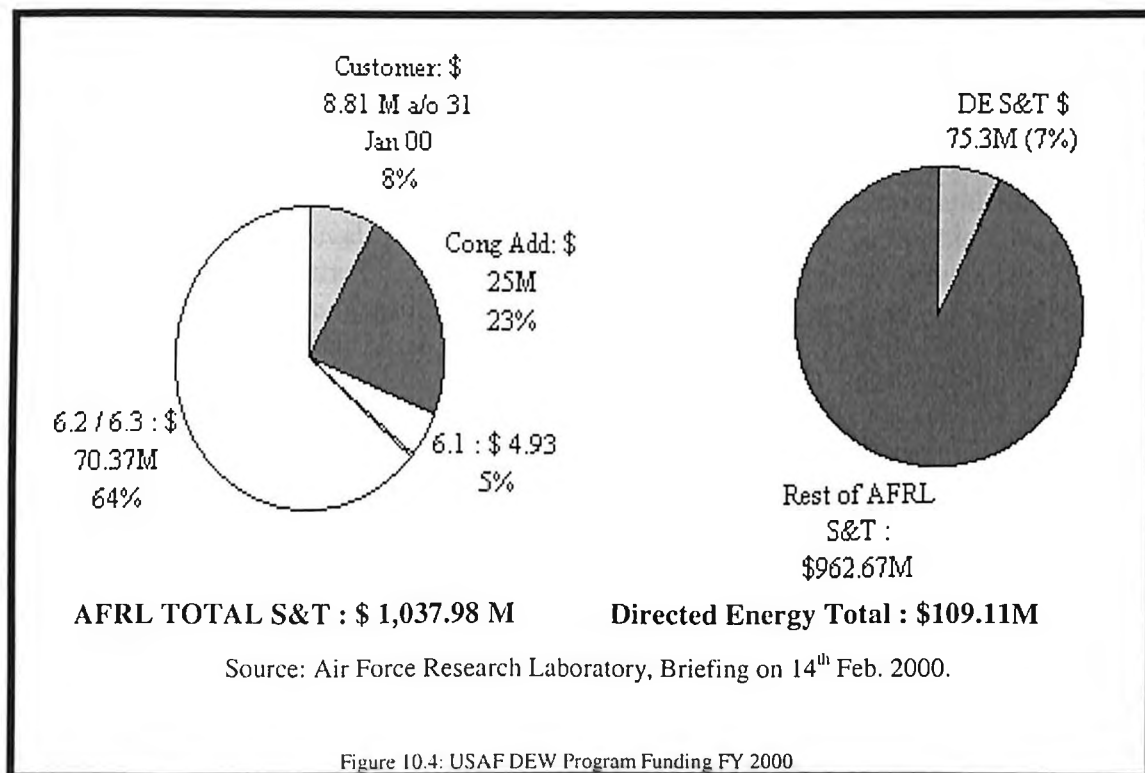
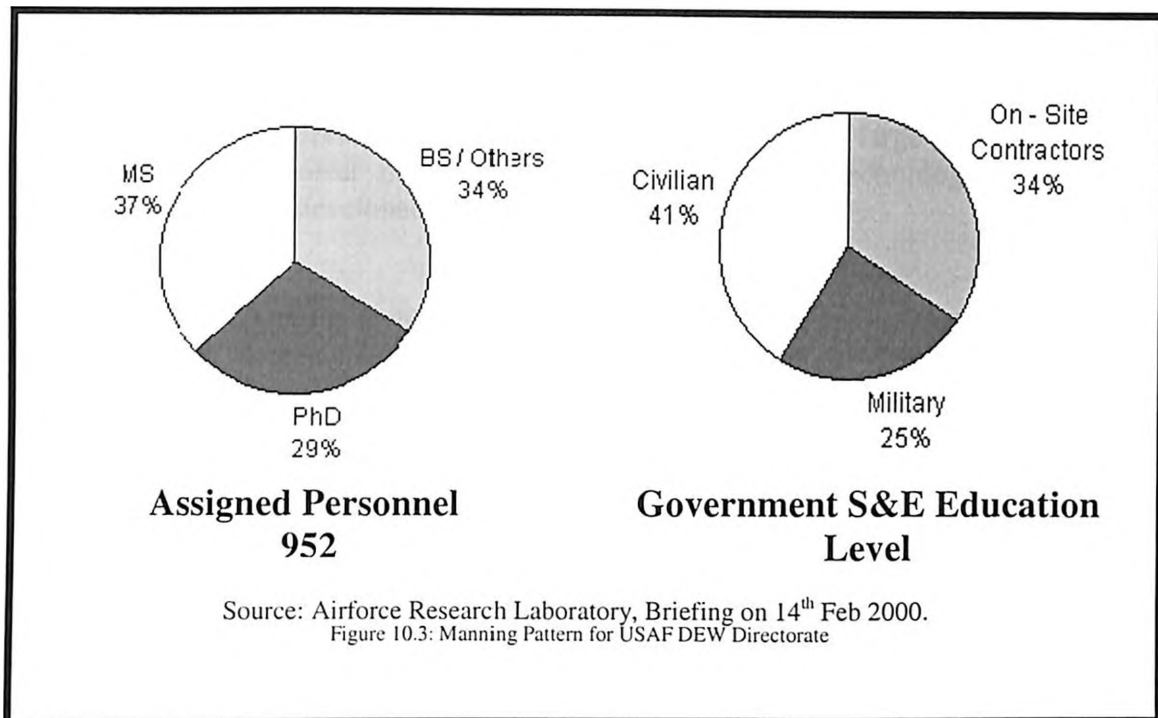
10.4.1 Umbrella DEWs Program of DoD, USA

An overview of the US, DoD's program for development of DEWs is shown in figure 10.2. It emerges that considerable investments are being made in the development of laser and RF energy weapon systems through Air force Research Laboratory (AFRL), Kirtland, USA.

Laser & Optics	RF Energy
<ul style="list-style-type: none"> • Ground Based Laser Technology Program • High Efficiency Electric laser program • Remote Securing large optics • Space Awareness Program • Air borne Laser Technology Program • High Power Laser Program • Scalable Multi-Wave length laser Program 	<ul style="list-style-type: none"> • HPM Source Program • HPM Pulsed Power Program • HPM Source Program • HPM Effects Program • HPM Application Program
<p>Source: Airforce Research Lab, Kirtland, USA, Briefing Feb 2000 Report.</p>	

Figure 10.2 : DE Technology Program of DoD, USA.

The personnel assigned to the Directorate of Directed Energy, DoD, USA, their education level and funding are presented in figures 10.3 and 10.4.



10.4.2 Developments at Calabazas Creek Research (CCR), Inc. USA

This agency is currently engaged in the development of a large number of products related to high power microwave and millimeter wave technologies. Some of the software products developed by it are as follows [177].

10.4.2.1 CASCADE

Cascade is a scattering matrix program for the design of microwave and millimeter wave circuits and components. Scattering matrix analysis has revolutionized the design of overloaded gyrotron circuits and is now used for designing wave guide components, including pillbox and coaxial windows, mode converters, tapers, and transitions. Scattering matrix software generates the scattering matrix by calculating the coupling coefficients between transitions, including the effects of dielectrics.

The software facilitates development of waveguide and circuit components consisting of circular, coaxial, or rectangular waveguide sections. A user-friendly, intuitive, graphical user interface facilitates user input and post processing with material properties for several standard ceramics built into the user interface. Output includes the complete mode composition throughout the problem domain. This allows the determination of the scattering matrix parameters, electric field profiles, resonant frequencies, electric field gradients, mode content, and ohmic loss. The software can be used to design smooth wall mode converters and tapers. Scattering parameters can be entered from other programs.

10.4.2.2 Beam Optics Analysis (BOA)

This software has been developed by CCR, in association with the Scientific Computational Research Center at Rensselaer Polytechnic Institute and North Carolina State University is developing a fully relativistic, 2D/3D, charged-particle beam analysis program with adaptive finite element meshing. The code is aimed to incorporate essentially all the advanced features and capabilities required for developing the following products [94]

- Multiple beam devices
- Sheet beam devices
- Inductive output tubes (IOTs)
- Field emission amplifier (FEA) arrays
- Gridded, high convergence, and highly thermal guns
- Flat panel displays
- High-frequency gyrotrons with extremely annular
- Bombardiers for fast-warm-up cathodes beams
- Field emission devices
- Asymmetrical cathodes
- Collectors, especially multi-stage, depressed collectors

Special emphasis is being given to the development of a user-friendly, intuitive, graphical user interface (GUI) to facilitate problem setup and iterative analysis. The GUI will be incorporated into AutoCAD and SolidWorks Advanced post-processing

capabilities will be included to facilitate component design and development. This program is funded by U.S. Department of Energy Grant No. DE-FG03-00ER82966.

10.4.2.3 Surface Integral Equation Analysis of Quasi-Optical Launchers Using the Multi Level Fast Multiple Algorithm (SURF 3D)

Existing design software is unable to accurately model the precise electromagnetic fields on quasioptical antennas, so approximations are used to obtain solutions. The accuracy is insufficient to obtain the precision necessary. Consequently, a series of correcting mirrors are used to correct the errors and improve the transmission. Even then, significant amount of RF power is lost through side lobes, mode conversion, and other antenna losses.

SURF 3D program solves the surface electromagnetic fields using advanced algorithms to reduce the computational resources. Direct solution would require days or weeks to complete. However implementation of advanced solution routines reduces the computation to several hours. Additional algorithms are being developed to reduce the computational time to several minutes. This will then allow syntheses of antenna structure to precisely tailor the RF wave coupling into down stream systems.

10.4.2.4 Hardware Development Projects of CCR

The Calabazas Creek Research, Inc. is also involved in several hardware development programs funded by the Department of Energy, Department of Defense, and the National Aeronautics and Space Administration. The hardware development activity is focused on extending the state of the art in high power microwave generation, transmission, and efficiency [91,94].

- 10 MW, W-Band Gyroklystron
- Multi-Stage Depressed Collectors
- Multiple Beam Guns
- High Power Microwave/Millimeter-Wave Windows and Waveguide Components
- Terahertz Backward Wave Oscillators
- Field Emission Array Electron Guns
- MEMS-Based RF Source Development
- Gridded Sheet Beam Electron Gun
- 13 kW CW klystron for the Jefferson Laboratory Upgrade
- Multiple Beam Klystron
- 100 MW Circulator
- Direct Gaussian Mode Coupler

10.4.3 Center for Pulsed power and Power Electronics, Texas Technical University, USA

Work at TTU pertains to the following [28]

- Basic Research in Pulsed Power.
- Development of Pulsed Power Systems.

10.4.3.1 Basic Research in Pulsed Power Technologies

The area of pulsed power research involves storing, shaping, transmitting, and measuring high voltage, high current pulses of electrical energy. This is important to many applications areas, such as laser drivers, high power microwave generators, particle accelerators, nuclear fusion, nuclear weapons effects and lightning simulations, industrial manufacturing technology, and electromagnetic mass drivers [PL PPRES].

High power switching, materials studies, explosive power generation, and high power microwaves are the high-priority research areas and the main emphasis. This is interdisciplinary program and involves faculty members from electrical engineering, mechanical engineering, physics, and chemistry. The specific areas of research being perused by Texas Technical University, USA are as follows.

- Breakdown in liquids and solids
- Electrical space propulsion devices
- Electron beam generation
- Erosion resistant materials for space propulsion
- High power microwave studies
- Industrial applications of pulsed power technology
- Insulators for H.V. applications in space
- Interaction of arc channels with electrodes and insulators
- Solid state power electronics
- Sub-nanosecond pulse phenomena
- Surface physics of insulators
- Various novel switch concepts
- Explosive generation of pulsed power
- Inductive energy storage

10.4.3.2 Development of Pulsed Power Systems at TTU, USA

The current research and support programs are shown in the figure 10.5 [10,28].

Agency	Projects
Air Force Office of Scientific Research	<ul style="list-style-type: none"> • <i>Microwave Studies of Dielectric Interfaces</i> • <i>High Energy Microwave Sources</i> • Nanosecond and Sub-Nanosecond Breakdown of Dielectric Media • High Power Microwave Breakdown of Dielectric Interfaces • Expendable Pulsed Power and High Power Microwave Devices • Explosively Driven Pulsed Power for Directed Energy Munitions • High Speed Diagnostic Instrumentation
NASA	<ul style="list-style-type: none"> • <i>Electric Space Propulsion</i> • <i>High Efficiency Power Supplies for Electric Propulsion Thrusters</i>
Army	<ul style="list-style-type: none"> • <i>Intelligent (Adaptive) Power Supply Design for Hall Effect Electric Space Propulsion Thrusters</i> • <i>Ultra fast Gas Breakdown</i>

Miscellaneous	<ul style="list-style-type: none"> • High Temperature Superconducting Opening Switch • Design Methodology for Super Efficient Power Supply Design Commercial Chemical Spill Cleanup Using Arc Jet Plasma Sources
<p>Source: Report of High Energy Microwave Device Consortium Figure 10.5: Developments in Pulsed Power Supplies</p>	

10.4.4 Research & Development Work at Voss Scientific, USA

Voss Scientific carries out state-of-the-art research in high-power microwave source development, diagnosis of the device and radiated environment, susceptibility effects testing, and system, subsystem and component hardening. Voss Scientific has made key contributions to high-power microwave source development and testing programs sponsored by the Air Force Research Laboratory (AFRL), and others [92].

Voss also supports the US AFRL in high-power microwave source and antenna designs for ongoing susceptibility testing. Some of high-power microwave research and developments are summarized below.

10.4.4.1 PC-Based Rapid Determination of Test Fidelity in Anechoic Chambers

Windows-based novel computational electromagnetics (EM) to analyze antennas and scattering from test assets and absorber to assess EM test fidelity in anechoic chambers.

10.4.4.2 Mobile Automated High-Power Microwave Diagnostic System

Advanced hardware and software DAAAC systems in a mobile enclosure.

10.4.4.3 Assessment of High-Power Microwave (HPM) Test Fidelity

This work presented and developed unique figures of merit to aid testers in the Maverick IR Missile Test and other HPM susceptibility experiments.

10.4.4.4 Mode Converters for Axially Extracted VCOs

Providing >70% efficiency at 25% bandwidth, these designs are used in narrowband high-power microwave effects testing.

10.4.4.5 Cross-Field Oscillator/Magnetically Insulated Oscillator (CFO/MILO) Source Development

The basic physics of an S-band CFO/MILO was investigated to demonstrate and document fundamental non-asymmetries in the RF processes of this device, even in nominally asymmetric configurations.

10.4.4.6 Millimeter Wavelength Virtual Cathode Oscillator Demonstration

A lumped-element, pulse-forming line (500 msec pulse length) and a 40 kilogauss magnetic field coil for a virtual cathode experiment were designed and built. The source was operated at frequencies up to 40 GHz.

10.4.4.7 Transient Wave Electromagnetic Sources

Voss Scientific has developed Transient Wave Electromagnetic Sources (TWEM) for use in electromagnetic susceptibility testing applications.

10.4.5 Development of Radio and Microwave Circuits and Antennas at Lee Center Caltech, USA

The DEW program will require circuits and antennas for a range of applications at frequencies ranging from 1MHz to 1THz. Radio and microwave circuits are the core of the wireless communications revolution and play a central role in radars, remote sensing, and satellite broadcasting. The research in quasi-optical power combining, micro-electro-mechanical systems (MEMS) for RF and microwave circuits, and Class-E amplifiers for communications transmitters can be utilised for this program. Professor David Rutledge, Director of Lee Center for Advanced Networking, USA has stated that the goal of the work in quasi-optical power combining is to make powerful solid-state oscillators and amplifiers. In recent years, there have been spectacular increases in the operating frequencies of solid-state devices. Gallium-arsenide transistors are now available that operate at frequencies as high as 200 GHz. At the same time, the output powers at these high frequencies are very low, and the outputs of hundreds or thousands of devices must be combined to make a high-power transmitter.

Caltech has also pioneered the development of radically different microwave circuits called active grids that directly produce and amplify microwave beams. Active grids are periodic metal patterns loaded with transistors and diodes. These circuits increase the output power of transmitters and improve the noise and saturation levels of receivers. The circuits are redundant, and this makes them less likely to fail. Also, active-grid circuits have fewer parts than conventional microwave circuits. Caltech has recently demonstrated a grid with 72 transistors that produces 0.6 W at 40 GHz [51].

Caltech has completed a Micro-Electro Mechanical Systems (MEMS) project, demonstrating a sliding buckshot that tunes a 600-GHz circuit and are now developing MEMS switches with the Rockwell Corporation for electromechanical steering of a 90-GHz radar beam, and are studying the use of MEMS capacitors and inductors in high-power transmitters.

Caltech also has projects in high-power Class-E amplifiers for communications transmitters, semiconductor plasma processing, and magnetic-resonance imaging. These amplifiers use power MOSFETs and have an efficiency of 90% and output powers of up to 500 watts.

10.4.6 Accelerator Research at Stanford, USA

The Accelerator Research Department A (ARDA) is a part of the Technical Division at the Stanford Linear Accelerator Center located in Stanford, CA. ARDA is a group activity of faculty, accelerator physicists, research associates, graduate students, and engineers. The primary expertise of the department is the design of particle accelerators, which includes calculation of the transport of particle beams and their interaction with the vacuum environment, the design of RF structures for acceleration and the design of RF power sources. The department has two primary missions, which are complementary

- To provide support to the Accelerator Department, performance improvements, design and development of accelerators on-site.
- Execution of special projects designed to advance the state of the art of accelerator physics
 - Development of the Final Focus Test Beam
 - Construction of the Next Linear Collider

The ARDA group structure and their areas of activities are presented in figure 10.6 [7,20,52,107,117,145,146,147,153,154,157,163,196,198].

Area of Research	Scope of Work
Accelerator Structure	<ul style="list-style-type: none"> • Design, engineer and test accelerator structures for colliders operating under extremely high gradient superior properties in higher modes suppression. • Theory, simulation, fabrication technology, characterization, and high power experiments.
Advanced Beam Concepts	<ul style="list-style-type: none"> • Develop concepts in beam physics for application in current and future accelerators. In the process, study theoretically and experimentally the basic science aspects of these concepts. • Research in astrophysics.
Advanced Electronics	<ul style="list-style-type: none"> • Develop electronic circuits, sign processing systems and laboratory measurement techniques. • Current concentration is on techniques for control of coherent in particle accelerators and storage rings. These include GHz bandwidth
Collective Effects	<ul style="list-style-type: none"> • Theoretical research on collective effects in beam dynamics concerning beam instabilities. • Analytical and numerical calculation of wakes and impedance. • Study of emittance dilution in linear accelerators. • Intrabeam Scattering. • Electron cloud effect. • Fast ion instability. • Coherent synchrotron radiation effects in beam dynamics. • Nonlinear effects for single bunch instabilities. • Laser acceleration in vacuum. • Accelerator physics for SASE FEL's.
High Power Microwave	<ul style="list-style-type: none"> • Research, design and development on the generation and control of RF power. • Design of passive RF components switches, and novel RF sources. • Development of high-power, overloaded RF pulse compression / distribution system for linear accelerator write computer codes to facilitate this work. • Study RF breakdown, and design of accelerator lines.

Lattice Dynamics	<ul style="list-style-type: none"> • Design of lattice including linear optics, tolerance analysis nonlinear particle dynamics. • Participate in the operations to improve accelerator performance using advanced methods of analysis. • Study the limitations of accelerator such as beam effects. • Develop and maintain object-oriented software designing, commissioning and operating.
Special Projects	<ul style="list-style-type: none"> • Design of crompton x-ray source. • Study of single-bunch longitudinal instabilities. • Design of RF / microwave components. • Beam measurement instrumentation. • Vacuum systems.
<p>Source: SLAC ARDA Group's, Home Page.</p>	

Figure 10.6: Project Groups and their Profiles at Stanford Linear Accelerator Center, USA.

10.4.7 Multi University Research Initiative (MURI), DoD, USA

The US Air Force Office of Scientific Research Laboratory (AFOSR) has formed a Multi University Research Initiative (MURI) to develop HPM Weapons technology. This Central Consortium is composed of faculty members and students from Texas Tech University (Coordinating University), the University of New Mexico, and the University of Michigan with collaboration from Microwave Sciences, Inc. The participants come from Electrical Engineering, Physics, Materials Science, Computational Systems, and Nuclear Engineering. The research at each university complements each other and covers Vircators, High Efficiency Backward Wave Oscillators, Fast Wave Gyro Devices, Plasma Filled Devices, Ferroelectric Cathodes, Ultra Wideband Technology, Microwave Vacuum and Window Breakdown, Multipactor Phenomena, "Smart" Tub Technology, Advanced Cathodes, Radial Accelerators, Transit Time Oscillators, and Free Electron Lasers.

The emphasis of the research is to increase the device efficiencies and to reduce their weight and volume. Efforts to increase the radio frequency vacuum strength of cavities and windows hold promise for higher energy density devices. Novel cathodes may lead to longer pulse devices resulting in higher energy sources. An important aspect of the program is to research various control strategies relevant to pulsed high power microwave sources. An assessment of expert systems and their usefulness to these sources is being made. There is active collaboration with industrial companies, especially Primex Physics International Co., Titan, and Sandia National Laboratories. The cooperation between the three universities and the Air Force Research Laboratory (Phillips Site) has been expanded and strengthened. The USAF is the lead agency in this field and the largest DoD effort is at the Air Force Research Laboratory at Kirtland AFB in Albuquerque, NM. Because of this, as well as geographical considerations and

historical ties, the Central MURI Consortium has particularly strong ties with Phillips Site [87].

Amongst the consortium members, the Texas Tech University (TTU) is emphasizing on the HPM window breakdown work and testing new window materials. Collaborative work is being carried out with the University of Michigan on multipactor theory and experiments. The University of New Mexico (UNM) has a program on compact sources of high-energy microwaves. The list of projects, their scope and the concerned agency is presented in figure 10.7.

Scope of Work	Work Center / University
Microwave Vacuum and Window Breakdown: Microwave experiment design and modeling of microwave systems.	Texas Technical University
Ultrawideband Microwave Generation	Texas Technical University
Alternate Geometry Vircators	Texas Technical University
Theoretical Modeling of Interactions in Plasma Filled Microwave Generators	Texas Technical University
Deflecting Extended Interaction Klystron:	Texas Technical University
Demonstration of a Gigawatt Level Smart Tube	University of New Mexico
Hybrid Hard Tube BWO	University of New Mexico
Plasma-Filled BWO	University of New Mexico
Ferroelectric Cathodes	University of New Mexico
Radial Acceleratron	University of New Mexico
Educational Reltron HPM Source	University of New Mexico
HPM Characterization of Photonic Crystals	University of New Mexico
Smith-Purcell Free Electron Laser	University of New Mexico
Microwave Pulse Shortening on High Power Gyrotrons	University of Michigan
Theoretical Work on Multipac	University of Michigan
Scaling in Detune of Resonant Structure by Intense E-beam	University of Michigan
Resonant Absorption of RF by Impurities in Dielectric	University of Michigan
Pulse Shortening in HPM Generators	University of Michigan
Transition to Better HPM Source Surface and Vacuum Conditions	Microwave Sciences
Low-Closure-Rate Cathode Materials at High Electric Fields.	Microwave Sciences
Vircator Studies	Microwave Sciences
Source: Project Report of High Energy Microwave Device Consortium.	

Figure 10.7: RD&D Collaboration by AFOSR under MURI program

10.5 Role of Simulation and Modeling: Foundation for Development of Next Generation EM Weapons

10.5.1 Background

Directed HPM radiation is emerging as a powerful means of projecting large amounts of useful form of energy at the speed of light to far-away targets. High power RF technology, despite being over 20 years old, is in its infancy for compact systems. The high power Microwave Division of the Air Force Research Laboratory USA is the world's leading center in HPM research and technology. The work at the HPM Division has been progressed on three fronts and involves three teams [203].

- **Source Development:** The source development team designs the sources that generate the RF pulse.
- **Beam Tracking:** The beam tracking team is tasked with proper propagation of the RF energy and then directing it toward the target.
- **Effects Study:** The effects team studies the interaction of the RF energy with the target.

Intensive modeling and simulation is crucial in all the above mentioned three phases of the project. Following are the examples of software programs being used for simulation.

- **Magneto-hydrodynamics (MHD):** These software programs are used in the analysis and modeling of the pulsed power.
- **Particle-In-Cell (PIC) Software Programs:** These are used in the modeling and simulation of the source.
- **Electromagnetic (EM) Equation Programs:** These are used in the modeling and simulation of extraction and propagation of the RF and in modeling certain aspects of the effects.

Laboratory uses number of parallel first - principle physics software programs, developed by previous AFOSR or CHSSI projects, to do modeling and simulation on the massively parallel computers at the DoD's high performance computing centers. The design and development of the entire HPM system, including the pulsed power, the source, the extraction and transport and the effects is modeled.

10.5.2 Virtual Prototyping of RF Weapons

The Directed Energy Applications for Tactical Airborne Combat (DE ATAC) study, commissioned by Maj. Gen. Richard Paul and headed by former AF Chief Gen. Ronald Fogelman identified and rank-ordered 20 concepts. The top five among them were HPM concepts. This determined the AF investment strategy in HPM. Consequently the AFRL laboratory efforts are focused on those technologies that can in the future support the Aircraft Self Protection, Munitions Electronic Attack and Airborne Electronic Attack. Under this project the AFOSR has pursued virtual prototyping and simulation of the following.

- **Target Effects:** This includes a missile target coupling, system effects and trajectory.
- **Weapon Performance:** The effects of weapons on antennas, systems, sources and power systems.
- **War Fighter Payoffs:** One to one engagements and Force-to-force engagements.

10.5.3 Virtual Prototyping Requirements

Use of virtual prototyping was made to develop and apply theory and advanced computation to enhance the development of HPM and related technology for the program. The approach has been to use best software available to analyze existing systems and to design future HPM components. New software has been developed to undertake the following

- Predict effect of RF weapons on a verity of targets.
- Reduce time and cost of RF weapons from concept-to-battlefield using virtual prototyping

10.5.4 The Computational Challenges of Virtual Prototyping.

- **Need:** End to end simulation
 - Coupling to target systems
 - Source components
 - System integration
- **Near- term Requirements**
 - Thousand-fold increase in computing speed and memory.
 - Advanced algorithm development
- **Status**
 - 3-D time - dependent physics simulation of source components now possible.
 - Need new models for weapon target interaction

10.5.5 Target of HPM Simulation and Virtual Prototyping

As compared to conventional microwave industry based on solid state electronics, the HPM have following peculiarities.

- Power exceeds 100 MW (> 100 GW possible).
- Frequency ranges cm-mm waves (100 MHz - 100GHz).
- Narrowband RF if produced by intense relativistic electron beams.

The Narrowband HPM systems have three components

- Prime pulsed power to generate high DC voltage.
- Microwave source to transform DC voltage to RF Generator by relative emission from electrons that under go oscillations. Coherent radiation achieved by a resonance condition between periodic motion of electrons and wave in cavities.
- Radiation structure (antenna) to direct RF in desired direction.

The long-term objective of virtual prototyping is to create end to end software design tool for microwave engineer of future. The short-term objective is to make contribution to improvement of existing microwave components.

10.5.6 Efforts of US Air Force, in Simulation Areas under EM Weapons Program.

The US AFSOR has put in following efforts in the areas of Simulation and Virtual Prototyping of the EM weapons [11,12,13,168].

- Understanding and reducing the numerical dispersion on the physics of relativistic charged particle beams.
- Electron-neutral, ion-neutral, electron-solid interaction.
- General 2D and 3D complex geometry computational grids.
- Implementing these concepts into parallel ICEPIC software and extending the range of parallel machines on which this code runs (e.g. linux superclusters).
- MHD algorithm development and application in/with MACH2 and MACH3.

The AFOSR - funded in house algorithm has achieved breakthrough for parallel PIC.

- **Parallel ICEPIC:**
 - Extensively validated against mature software.
 - Parallel features being exploited to tackle larger and more complex problems.
 - Design tool of choice for complex sources based on IREBs.
- **Physics algorithms**
 - Developed in response to HPM requirements.
 - Neutral with wider PIC community for other applications.
- **Basic research investment continues**
 - Big payoff in HPM applications arena.
 - Non -HPM applications on horizon.

10.5.7 Case Studies of Software Intensive Simulation & Prototyping

The Center for Plasma Theory and Computation under the direction and control of AFRL, Kirtland, USA develops and maintains a suite of scientific software to support this development of HPM Weapons. Typical narrowband HPM devices have three components.

- **A Pulsed Power Source:** It releases stored energy as a fast (- nsec to msec) applied voltage.
- **A Beam/Cavity Interaction Region:** Here the beam's kinetic energy is transformed to microwave radiation.
- **An Antenna:** It directs the radiation.

These components are distinct in their density of charged particles. Specifically, pulsed power devices often involve high-density plasmas, beam/cavity source and have a low density of charged particles, and antennae ideally have no charged particles. These regimes are simulated most effectively by magnetohydrodynamic, particle-in-cell and computational electromagnetic techniques, respectively.

From a weapons perspective the ultra wide band devices emit radiation over a broad range of frequency but with a low power density. These devices are appropriate when the threat is not well identified so that the optimal frequency is not known. Narrowband sources emit at a single frequency at a very high power. If this frequency is such that it can resonate with the target then it will be very effective in disabling it. Ambitious experimental efforts are in progress to support RF weapon development. Weapons based on HPM devices have the potential to satisfy the non-lethality requirements as well as the ability to disrupt enemy electronics, and have several advantages over competing concepts. Such weapons are fast, have unlimited "ammunition," and are not affected by adverse weather conditions.

The design of an HPM device that provides the required power and effectively radiates EM waves presents difficult and interesting challenges. Complex and expensive experimental efforts are more timely and cost-effective if they are guided by theoretical and computational modeling. The required modeling is based on Maxwell's equations, the Navier-Stokes compressible fluid equations, and the Lorentz Force law. Analytical solution of the resulting system of nonlinear partial differential equations is intractable. Furthermore, numerical solution requires fine-grained resolution in both time and space. Thus, modeling and simulation, which is critical to timely development, is computationally intensive. Such computations are made tractable by viewing the device as a system consisting of a pulsed power source, a microwave source, and an antenna. Each of these components has important, distinguishing characteristics and has been simulated at The AFRL that facilitates its simulation using the software MACH, ICEPIC, and PARANA, respectively [203]. Brief description of these packages is given as follows.

10.5.7.1 Pulsed Power

The pulsed power source converts stored energy into a high power electrical pulse. Stored energy can be as high as a kiloJoule, with power in the gigawatt range. A concept of particular interest for several designs is explosively driven magnetic flux compression. One device based on this concept is the helical magneto-cumulative generator (MCG), that is being designed and tested by AFRL/DE. In this device, a modest initial magnetic field is compressed by high explosive. Because of the conservation of magnetic flux (magnetic field integrated over a surface area), the magnetic field increases as its cross-sectional area decreases. Thus, the kinetic energy of the explosive material induces a fast-rising electrical pulse in an attached load. The efficiency of the process increases with reduced flux losses (e.g. magnetic diffusion, geometrical detachment, and electrical breakdown), which typically requires increased geometrical complexity. These high-density phenomena are modeled by magneto-hydrodynamic (MHD) calculations, which are performed by the software Multiblock Arbitrary Coordinate Hydromagnetics (MACH).

The MACH program exists as 2D serial software (MACH2) and as 3D parallel software (MACH3). Recent software enhancements allow accurate modeling of real explosives in an environment that includes a magnetic field, as well as material strength properties of

the solid materials. The arbitrary Lagrangian-Eulerian capability of the software is ideally suited for modeling the interaction between the explosive and the armature, which moves with respect to the stator. Two-dimensional simulations of the MCG compare well with experiment. Full 3-D simulations of the MCG are ongoing on the ASC IBM SP and the SGI O2K, the results of which have a number of uses. Simulations of the MCG as an independent unit can be used to reduce the device's size, improve its efficiency, and decrease the rise time of the generated pulse. The results may also be combined with simulations of the HPM source to determine the effects of the pulse shape on the source. This is an iterative process because MACH uses a lumped circuit model of the HPM source for its load. The model is not known to represent the HPM source effectively due to the non-linear nature of the source. An interface between these codes was proposed.

10.5.7.2 HPM Source

The electrical pulse created by the pulsed power source is applied to a diode to create a high energy (~400 kV), high current (10-60 KAmp) beam of electrons. Although the configuration for the diode region varies widely from source to source, the principle is the same. The beam of electrons created in the diode region then interacts with the structure of the cavity and energy is transferred from the kinetic energy of the beam to EM energy in the existing modes of the cavity (preferably in a single desired mode). Finally, the beam is collected in a beam dump and the microwaves are extracted from the cavity. For interactions in the beam-cavity region, the collisionality of the charged particles is low so that the use of a fluid-like MHD software program is not appropriate. This type of problem is better simulated with a particle-in-cell (PIC) software program where the spatial domain is divided into stationary cells upon which electric and magnetic fields are defined and charged macroparticles are allowed to move through the cells under the influence of the electric and magnetic fields.

A 3D PIC code, Improved Concurrent Electromagnetic Particle-in-Cell (ICEPIC), has been developed at the Center for Plasma Theory. ICEPIC is a fully relativistic, 3D, Cartesian, variable mesh PIC software capable of simulating a wide range of problems. Two narrowband HPM sources of interest, the relativistic klystron oscillator (RKO), and the magnetically insulated line oscillator (MILO) have been simulated using ICEPIC.

10.6 Research & Development Blue Print for India's EM Weapons Program

The emerging compulsion of security needs of the digital age would compel India to develop or procure EM weapons and deploy them as a principal component of its military posture within next 7 to 10 years. This initiative will be of unprecedented volume and complexity and would require involvement at the highest political and administrative level. A suggested framework for development of IW capability around EM energy weapons is presented in the succeeding paragraphs.

10.6.1 Basic Research

The program will require university level basic research in pulsed power sources, microwave sources and antenna technologies. The area of pulsed power research involves storing, shaping, transmitting and measuring high voltage, high current pulses

of electrical energy. The multidisciplinary efforts should be focused on accelerator structure, advanced beam concepts, collective effects, high power microwave etc. The research in microwave would also involve vircators, high efficiency backward wave oscillators, fast wave gyro devices, plasma filled devices, ferro-electric cathodes, ultra wideband technology, multipactor phenomena, smart tube technology, advanced cathodes, radial accelerator, transit time oscillator etc.

10.6.2 Technology Development

Following should constitute the basic building blocks from the technology development perspective.

- Compact, High Power HPM Sources
- Power exceeds 700 MW (> 700 GW possible).
- Pulse length (Cm-mm waves, 700 MHz-700GHz).
- Compact, High Power, High Gain, Ultra-Wide Band Antennas
- Compact, Efficient, High Power Pulse Power Drivers

10.6.3 Study and Assessment of HPM Effects and Lethality

This should include the following

- RF testing of a wide range of air, sea, land, and air borne assets.
- RF effects database development to provide reliable prediction of RF effects to permit extrapolation to other systems.
- Development of countermeasure techniques and incorporation of HPM into accepted weapon engagement models of all the three Services.
- Assessment of biological effects necessary to establish safety thresholds for personnel protection.
- Study of civil Defence issues.

10.6.4 Integration With Existing Programs

This should encompass integration of EMP and RF energy weapons into platforms such as fixed-wing and rotary wing aircraft, naval combatants, land vehicles, aircraft pods, unmanned aerial vehicles and munitions.

10.6.5 Low Impact Hardening of Systems Against Hostile and Self-Induced EMI

This should include following

- Transitioning EM hardening to users in response to existing EMI/EMC problems and projected threats.
- Identifying susceptibilities in air, land, sea and other militarily critical systems, medical electronics, industrial controls and other components of critical NII.
- Developing hardening countermeasures, which minimally impact system performance, cost or maintainability.

10.6.6 Development of Military Posture

Based on effects assessments and technology development efforts, following should be undertaken.

- Air Surveillance for Missile Defence (ASMD)
- Counter-proliferation.
- Counter-munition, and air space control

10.6.7 Technology Demonstration

- Platform Self Protection should pertain to existing air crafts, strategic and tactical nuclear assets, indigenous DRDO programs viz. Light Combat Aircraft (LCA), Advanced Light Helicopter (ALH) and the Main Battle Tanks (MBT), Air Craft Carriers, supply ships or equivalent platforms to meet the needs of there Services.
- Command and Control Warfare/Information Warfare demonstration can include networking components (Switches, Routers, Servers, Command Shatters)
- Suppression of Enemy Air Defenses Demonstration.

10.6.8 System Level Developments

Following should be attempted

- Develop capability to perform weapon system analysis in the context of a realistic battlefield environment to include dynamic terrain, weather, obscuration (man-made smokes, vehicular and high explosive dust, etc.), Command Control and Communications (C³) and Counter Measures (CM) and Counter Measures (CCM).
- Conduct weapon system munition configuration effectiveness/value-added analysis.
- Conduct weapon system-sensor mix effectiveness/value-added analysis.
- Conduct direct-fire / indirect-fire lethality, delivery accuracy effectiveness / value-added analysis.

10.6.9 Technology Development and Evaluation

There is a need to provide the Armed Forces with an engineering level-simulation to evaluate Service level systems and subsystems to include the individual end user for current as well as future needs of virtual prototypes.

- Perform weapon systems “*what if*” value-added analysis
- Perform countermeasure “*trade-off*”/ value-added analysis
- Perform sensor technology “*what-if*”/ value-added analysis
- Perform lethality “*what-if*”/ value-added analysis
- Perform survivability analysis

10.6.10 Tactics and Doctrine

There is a need to provide capability to support development and evaluation of tactics and operational concepts for the three Services at all echelons.

- Conduct weapon system force mix analysis
- Determine tactics, techniques and products for optimum employment of weapon systems/technologies.
- Determine which configuration is more effective. For example a unit of 4 LCAs where 2 can serve as reconnaissance vehicles, can be a typical mix in order to draw a practical operational doctrine or 3 ALHs and 2 Jaguars serving as the reconnaissance vehicles. The reconnaissance vehicles can establish and maintain contact with the

opposing force, identify the main axis of advance, provide situational awareness, and report the activity back to the appropriate command and control center.

10.6.11 Test and Evaluation

In support of the development and acquisition process, there is a need to provide capability to augment the testing for hardware/ prototypes and conceptual models to full fill the following requirements [172.173].

- Serve as Command, Control, and Communications (C3) driver to stress information handling systems and networks
- Evaluate sensor to shooter capability of "*system of systems*" as and when it is developed.
- Expand scope of operational tests beyond live participants
- Rehearse large scale tests
- Replay large scale tests
- Provide synthetic test environment and stimuli.
- Create proof of concept centers and test sites.

10.6.12 Force Modernization

- Conduct survivability/value-added analysis.
- Create Command, Control, Communications (C3) driver
- Augment operational synthetic battlefield
- Supplement analysis of alternatives

10.6.13 Protection and Assurance Program

- EMP Vulnerability Assessment
- Electromagnetic Hardening Technology
- Hardening of Battlefield Environment
- Electronic System Radiation Hardening
- Protection of Communications & Power Lines

10.6.14 Development of Risk Mitigation Technologies Against EM Weapons.

- Fiber Optics and Shielding Technologies
- Built in Protection at Design Stage
- Improved Packaging of Electronics
- EMP Hardening Schemes

10.6.15 Education & Training

The Directed Energy Microwaves Research and Education Program should prepare graduate students to contribute to the development of EM weapons program. The curriculum, leading to M.S. and Ph.D. degrees should prepare the students in pulsed power, charged particle beam accelerator, plasma physics, advanced electromagnetic, microwave engineering and several other areas important to Directed Energy

Microwaves. The curriculum should be strengthened by hands on laboratory courses that complement the theoretical and engineering fundamentals.

10.6.16 Research on Personnel Safety

As brought out above, Directed Energy Weapons are among the high-tech arms of the 21st century. They are known to hurt and kill with electromagnetic power. Microwave weapons can be aimed at computers, electronic devices and persons. They have strong physical and psychological effects and can be used for military and terrorist activities. These weapons are also part of crimes in Europe that almost nobody knows except the victims and the offenders. Until now they make the perfect crime possible [60]. In future these weapons are likely to become favorite with the terrorists.

The HPM-weapons used by high-^{tech} gangs supply continued or pulsed waves over long periods of time, especially in the night, from cars or vans or buildings around the target/person(s). They use magnetrons, microwave-generators, amplifiers, and integrated systems. In addition they apply through wall imaging methods. The criminals follow a double strategy: One way the victims are weakened, injured, tortured and intimidated. On the other side, the victims experience extreme, unbelievable things; almost no one can believe their reports. Most interpret the information from the victims as chimerical thinking. Some experts who work for the German Army or NATO know very well about these weapons, but secrecy keeps them from talking in public. Therefore HPM crimes have some very new characteristics. The International Union of Radio Science emphasized in a resolution of 1999 on Criminal Activities using Electromagnetic Tools: *"The fact that criminal activities using electromagnetic tools can be undertaken covertly and anonymously and that physical boundaries such as fences and walls can be penetrated by electromagnetic fields."*

In view of the above, significant efforts should be invested in researching the personnel safety aspects of these weapons.

10.7 Indications for Future RD&D in EM Weapons

In the Indian subcontinent the general awareness of the of EMP and RF energy weapons has dawned only recently after the declaration by US to invade Iraq. As reported in the media, we are expected to see the first use of high-power microwave weapons that produce a split-second spike of energy powerful enough to damage electronic components and scramble computer memories. Expendable, high-power microwave weapons mounted in cruise missiles and other aerial weapons could be first used in combat in Iraq. They are designed, at least initially, for use from cruise missiles and unmanned aircraft.

Adding a directed-energy weapon to an unmanned combat vehicle avoids risk to a pilot, there's a greater degree of accuracy. Everybody wants that capability. The combination of unmanned vehicles and HPM weapons also provides a way to attack the toughest targets and combined with the UCAVs there is a combination that uses stealth to debilitate

communications and electronics. In the longer term, perhaps in 3-5 years, there is a possibility of making reusable HPM weapons that can be installed on aircraft or unmanned combat aircraft. Because of HPM's limited range planners look at unmanned aircraft as the perfect platform to go into heavily defended areas to damage air defense radars, communications, command and control computers, and chemical/biological storage or production facilities [38,45].

The, HPM weapons now available are built like bombs, as expendable one-time-use weapons. Many of the payloads are designed for carriage by cruise missiles like the ALCM, Tomahawk, Jassm or Britain's Storm Shadow. However, there may be an alternative to one-way missions by these expensive cruise missiles. At the recent Farnborough air show, Lockheed Martin's advanced development program produced concepts for returnable cruise missiles, which would help defray the cost of expensive airframes and HPM payloads.

Two systems have been used to produce HPM energy. An older technology explodes high explosives wrapped around a coil with an electrical field to produce a blast of HPM. A version of this was tested by the U.S. Air Force using specially modified Air Launched Cruise Missiles but was supposedly abandoned for not being directional or long-range enough. A higher technology version uses a new generation of capacitors. These are discharged, and the pulse of energy focused in a relatively tight arc in front of the missile.

Range of HPM is expected to increase as apertures and electronically steered antennas are improved. This class of weapon is expected to be effective against command and control centers and weapons production sites buried deep underground as a defense against allied air attacks. Current research emphasis has now shifted to "*reusable payloads, not on one-way, cruise missile-type missions*". TRW is engaged in a number of projects at AFRL, Kirtland, USA".

10.8 Conclusion

- We recognize that the military has long exploited EM spectrum beginning with wireless communications in late 1880s and then radar in 1930s. These were followed by quick evolution of early warning, detection and weapon fire control systems in late 1980s. However electromagnetic waves in the form of directed energy appeared only in the fiction literature and movies till recent times. But "*directed energy*" now is a proven and visible scientific fact. However one area of the directed energy spectrum viz. the high power microwave technology has received significantly lesser attention.
- In India the paucity of knowledge of the high power microwaves technologies within defence establishments, institutions and industry pegs the national expertise in this area at lower than critical mass to commence a full fledged military program in EM energy weapons. The relevance and necessity for possessing this capability will require the defence planners to accord the program the requisite recognition, priority, funding and preference in support at political, military and scientific level.
- The development of core competencies at university level and a focus on basic research is inescapable to undertake knowledge and technology transfer amongst the

- industry and military establishments, even if the country seeks larger scale import of technology or systems.
- The proposed Research, Design and Development outlines are aimed to cover concept to delivery and deployment activities, since very few of these competencies exist in scientific, engineering or manufacturing areas in the country in any organized form.
 - The country possesses significant know-how and know-why in software and computing technologies, which can become the bed rock for simulation and prototyping of EM weapons. This in turn can help in compressing the development efforts, expenses, time frame, risks as well as uncertainties in environmental testing.
 - The collaborative efforts of US, DoD under the MURI program, involvement of industry across many verticals, program control by the AFSOR, DoD, USA have been presented in this chapter to signify the enormity and complexity of this program. A similar effort on the part of Armed Forces, Scientific, Technology and Engineering Institutions, Defence Research and Development Organization (DRDO), Defence Public Undertakings, Indian Space Research Organization (ISRO), Department of Atomic Energy (DAE), Ministries of Communications Information Technology, Science & Technology and industry in general, along with strategic overseas tie-ups in certain critical areas can only bring such a program to fruition.
 - A program of this magnitude would require funding and long-term commitments on the lines of major initiatives of ISRO, DAE, DRDO etc.

REFERENCES

1. "A New Threat to Aircraft Survivability: Radio Frequency Directed Energy Weapons (RF DEW)", John T. Tatum, U.S. Army Research Laboratory; Aircraft Survivability Newsletter, Fall 1995
2. "A Process for Information Security Technology Policy", Report of XIWT on the Industry - Government Corporation for Effective Public Policy, (Dec. 1997) www.xiwt.org/documents/security Rpt.html.
3. "A Study of the Federal Agency Needs for Information Technology Security" Report of the Study Conducted by NIST, USA, reprinted by Dennis M Gilbert, Data Pro, USA, May 1994.
4. "Air Force High Power Microwave Technology Program," Dr. William L. Baker, Air Force Phillips Laboratory; Aircraft Survivability Newsletter, Fall 1995
5. "Air Force 2025: Executive Summary", Vision Report of US Air Force, 2025 Support Office, Air University Press, Maxwell Air Force Base, Alabama, Aug 1996, <http://www.AV.af.mil/au/2035/contact.html> and www.au.af.mil.
6. "An Assessment of Non lethal Weapons Science & Technology" Report of the Naval Studies Board, National Academy of Sciences, USA, Nov. 2002.
7. A NEW PROPOSAL FOR BABAR TRIGGER UPGRADE FOR 10**34 HIGH LUMINOSITY RUNNING: LEVEL 2 DOCAZ TRIGGER
By Ted Liu *BABAR-Note-538, 29-APR-2000 Postscript Version from server.*
<http://www.slac.stanford.edu/bbnotes.html>
8. Admiral Robert J Natter, " The Future of Fleet Information Warfare: Combat Readiness Through Innovation" US Navy, 2002. <http://wwwchips.navy.mil>
9. AE Peveler "Security Implications of High Power Microwave Technology", IEE Symp. 1997
10. AE Pevler, " Security Implications of High Power Microwave Technology" IEE International Symposium on Technology and Society, Texas Engineering Solutions, Dallas, Texas, USA, (1997).
11. AF 00--211 " An MHD APU for Airborne Platforms, Abstract", John T Lineberry, Lytec LLC, Tullahoma, TN, USA, (2000).
12. AF 99 - 023, " High Average Power Modulator for Multi-Gigawatt HPM Sources", Allen Ramrus, Applied Pulse Technologies Inc., San Diego, CA, USA (1999).
13. AF 99- 184, " A Continuous Rod Electro Magnetically Pulsed Warhead", Tom Schilling, TPL Inc, Albuquerque, NM, USA, (1999).

14. Air Cmde. C N Gosh, "Battle Field of the 21st Century: Application of EMP Weapons", IDSA, Min. of Defence, New Delhi, (March 2001).
15. Akshay Joshi "Information Age and India" Published by Knowledge world and IDSA, New Delhi, Apr. 2001
16. An Architectural Framework for the National Information Infrastructure" Report of the Cross Industry Working Team, USA, (Sep 1994, Updated in Dec. 1999) www.xiwt.org/documents/Archframe.html.
17. AP 237 STC (97)7 (English), "Information Warfare and the Millennium Bomb", Draft General Report, Lord Lyell (UK), International Secretariat, (Sep. 1997) <http://www.iwar.org.uk/iwar/resources/nato/ap237/ste.pdf>.
18. ASPC Paper No. 47, "Military Information Operations in a Conventional Warfare Environment", Air Power Studies Center, Air Force war college, Australia, 1995.
19. 'Australian Communications Electronic Security Instructions 33 (ACSI33)", Email: assist@dsd.gov.au
20. AUTOMATIC COMPARISON OF OPR HISTOGRAMS
By Frederic Brochu *BABAR-Note-545, 06-NOV-200* *Postscript Version from server.*
<http://www.slac.stanford.edu/bbnotes.html>.
21. BM Leiner and EA Drozdora, " Critical Infrastructure: "The Path Ahead", Proceedings of the XIWT Symposium on Cross Industry Activities for Information Infrastructure Robustness, Virginia, USA, (Nov. 1998).
22. BMDO 00-001, " Magneto Hydro Dynamic Power Generation in Space from a Receptively Detonated Device, Abstract", Jean - Luc Cambeir, MSE Technology Applications, Inc, Butte MT, USA, (2000).
23. BMDO 98 - 001, "Electromagnetic Flak for Cruise and Sea Skimming Missile Defence", Dr. Jon R Mayes, Applied Physical Electronics, LC While Water, KS, USA, (1998).
24. BMDO 98-001, "Directed Energy Concepts and Components" Robert D. Sears, Vanguard Research Inc, Fairfax, VA, USA, (1998)
25. BMDO 99 -001, "Novel Ferro Magnetic Materials for Electromagnetic. A munitions Devices", Matt Aldissi, Fractal Systems Inc. Tampa, FL, USA, (1999).
26. BMDO 99-001, "High Power Microwave Pulse Sources of Coherent Micro Radiation for Distance Disabling of Electronic Devices", Czeslaw Golkowski, Super Pulse, Ithaca, NY, USA, (2001).
27. "Canadian Security Intelligence Science (CSIS) Information Operations", National Coordination, Economic and Information Security, Ottawa, Ontario, Canada, July 2001.

28. "Center for Pulsed Power and Power Electronic Research", Project Details, Dept. of Electrical Engineering & Physics, Texas Tech University, Texas, USA, Contact Judy.Patterson@coe.ttu.edu.
29. "Communications and Information Infrastructure Assurance Program (CIIAP)" PPT Slides Presentation by Don Wynegar to Communication and Information Sector Working Group, (May 2000).
30. "Computer Science and Telecommunication Board Projects on Critical Infrastructure Protection and Law", CSTB Washington, USA, <http://www7nationalacademies.org/cstb>.
31. "Computer Science and Telecommunication Board Projects Under Development", CSTB, USA <http://www.cstb@nas.edu>.
32. "Concept Definition, Architecture and Configuration of National C4ISR", Report by Prem Chand, WESEE, MOD, New Delhi, 1996.
33. Col. Richard Skimmer, Principal Director, "Prepared Testimony on EMP Threat Environment and Growing Dependence on COTS to US House of Representatives, Committee on Small Business", Office of Assistant Secretary of Defence, C4ISR, DoD, USA. Smbi@mail.house.gov.
34. "Congressional and Presidential Transition Efforts: Using Information Technology" Report by the United States General Accounting Office, Oct 2001, <http://www.gao.gov>.
35. "Critical Foundations Protecting America's Infrastructures" the Report of the US President's Commission on Critical Infrastructure Protection, PO Box 46258, Washington DC, USA, October 97.
36. "Critical Infrastructures and Internet", Slides of CISAC working group meeting on Infrastructure Vulnerability, Stanford University, Jun. 2002, http://www.stanford.edu/n_alderd/talks/CISAC.
37. "Critical Issues of Cyber Security _ Education and Awareness", Indication of MCIT, GOI, Future Direction. (Mar. 2003), <http://wwwmit.gov.in/security.asp>.
38. Captain William I Mc. Carthy AV, "Directed Energy and Fleet Defence : Implications for Naval Defence", OP No. 10, Air War college Maxwell Airbase, USA, May 2000.
39. Carlo Kopp "The Electromagnetic Bomb, A Weapon of Electrical Mass Destruction", Dept. of Computer Science Montosh University, Clayton, Australia, 1996, <http://www.csmanash.edu.au/ncarlo>.
40. Carlo Kopp and Ronald Pose "The Impact of Electromagnetic Radiations on Computer System Architecture", MUC, Clayton, Australia, 1996.

41. Carlo Kopp, "An Introduction to the Technical and Operational Aspects of the Electromagnetic Bomb", Paper No. 50 (ISBN 0642 264155), Air Power Study Center, Nov. 1996.
42. Carlo Kopp, "Electromagnetic Pulse (EMP) Systems" 1996, <http://www.abovetopsecret.com/papers/ebomb.html>
43. Charles N. Brownstein, "Next Generation Internet R&D Programs of the Federal Government", White Paper of Cross Industry Working Team, USA, (Apr. 1997).
44. Clayborne D. Taylor, Ph.D., "High Power Microwave Systems and Effects". Published by Taylor & Francis limited, Apr. 1994.
45. "Defence Technology Area Plan, Chapter 10, Weapons, Table X-10 HPM Sub Area Goals and Time Frame", DoD, USA, 1998. [http://www.fas.org/spp/military/docops/defence/97_dtap/weapons/ch to 100309 html](http://www.fas.org/spp/military/docops/defence/97_dtap/weapons/ch%20to%20100309.html).
46. "Defending America, Redefining the Conceptual Borders of Home and Defence (Draft Report), on Critical Infrastructure Protection and Information Warfare, Anthony H. Cardsman, Center for Strategic and International Studies, Washington, USA, Sep. 2000.
47. "Denial of Service Attacks" <http://www.cnn.com/2000/us/02/10/hacking.investigation.02>
48. "Directed High Power RF Energy: Foundation of Next Generation Air Force Weapons", DoD, HPC FY 2002 Challenge Projects by M. Joseph Arman, AFRL, DoD, Kirtland, USA, 2002.
49. D Sridar, "EMP Nightmare for Industrialized Nations" Strategic Affairs, NO. 0022/ issue: Nov. 16, (2001), Marketing@stratmag.com.
50. Dan L. Fenstermacher and Frank Van Hipple, " An Atmospheric limit on Nuclear - Powered Microwave Weapons" Science and Global Security, 1991, Vol. 2 PP 301-324.
51. David B Rutledge, "Research in Radio and Microwave Circuits and Antennas", Director Lee Center for Advanced Networking. University of California, USA, (Jan 2003). Rutledge@Catech.edu.
52. DOCUMENTATION FOR ONLINE PROMPT RECONSTRUCTION-QUALITY ASSURANCE
By Frederic Brochu *BABAR-Note-541, 28-AUG-2000 Postscript Version from server.*
<http://www.slac.stanford.edu/bbnotes.html>
53. DoE/ITG/Vol. 1.1 "India IT Vision 2010: Action Plan", Draft Action Plan for Achieving National goals enunciated by Hon. Prime Minister in his address to the nation on 22nd March 1998, Information Technology Group, Department of Electronics, Govt. of India, New Delhi, May 1998.

54. Dorothy E. Denning "Introduction to Information Warfare" PTT Slides, Georgetown University, USA, (2001), <http://www.csgeorgetown.edu/ndenning>
55. Douglas Wallel, "Onward Cyber Soldiers", Time Magazine, Aug 21, 1995, P.33.
56. Dr Rainhard Munzert, "Targeting the Human with Directed Energy Weapons", InfoWar Con, Vienna, 2002.
57. Dr. Charles N. Brownstein, "Future Priorities for NSF Networking activities: Workshop Report of Corporation for National Research Initiatives, Reston, VA, USA, (May 1999).
58. Dr. Kent Eschenberg and Mr. Mike Mc. Craney, "Virtual Prototyping Radio Frequency Weapon Project Visualization: A case study", Nicholas Research Corporation, CEWESMSRC, Viksburg, Mississippi, USA, (1997).
59. Dr. Nicholas Chantler, "The Direst Threat of Electronic High Technology Weapons:., Faculty of law Justice Studies Dept., Queens Land University of Technology, Brisbane, Australia, InfoWar Con 1997.
60. Dr. Reinhard Munzert, "Targeting the Human with Directed Energy Weapons", Info War Conference (Sep. 2002).
61. Dr. Rodney Smith and Bob Both, "Army Science and Technology Master Plan: Electronic Warfare / Directed Energy Weapons, Table E-13. International Research Capabilities", EW & DEW Directorate, DoD, Army Material Command, DoD, USA, (1998). <http://www.fas.org/man/dod-101/armydocs/astmp/cs>.
62. DSWA 98 - 008, "Flexible EMP Sheilding Material", Kelly Renter, Sensortex Inc, Unionville, PA, USA, (1998).
63. DTRA 00--017 "Statistical HPM / EMP Effects Assessment Abstract" Ted Lehman, Scientific Application and Research Associates, Huntington Beach, CA, USA, (2000).
64. DTRA 99-003, "Electromagnetic Hardening Technology Development", Robert F. Grey, Mission Research Corp, Santa Barbara, CA, USA (1999).
65. "Effects from High Power Microwave Illumination," C.D. Taylor and N.H. Younan, Microwave Journal June 1992.
66. E Schamiloglu et al, "Basic Research on Pulsed Power for Narrow Band High Power Microwave Sources", University of Nevada, Reno, USA, 1995.
67. Edl Schamiloglu, Professor & Principal Investigator. "The Importance of Ceramics in Pulsed Power Applications", PPT Slides for CDS Oct 2002 meeting, Dept. of Electrical & Computer Engineering, University of Mexico, USA, Oct. 2002, edl@ece.unm.edu.

68. Eileen M Walling, "High Power Microwaves: Strategic and Operational Implications for Warfare" OP11, Center for Strategy and Technology, AWC, AUM Maxwell Air Force Base, Alabama, USA, Feb. 2000.
69. Electronics Warfare/ Directed Energy Weapons": Army Science and Technology Master Plan (ASTMP), Chapter IV", DoD, USA, (1997).
70. EP1110-3-2, "Engineering and Design of Electromagnetic Pulse and Tempest Protection for Facilities "CEMP-ET Dec 1990,www.fas.org/nuke/intro/nuke/emp/toc.paf
71. E. Enderson Eriksson, "View Point: Information Warfare Hype or Reality?", The Non Proliferation Review / Spring-Summer 1999, <http://cns.miis.edu/pubs/npr/vol6/63/erikss63.pdf>.
72. "Electromagnetic Directed Energy Applications" Department of Defence Programs at Los Alamos Natural Laboratory, USA, 2000, Contact cece@lanl.gov
73. "Electronic Cash, Tokens and Payments in the National Information Infrastructure", Report of Cross - Industry Working Team, USA, (Dec 1999), www.XIWT-org/documents/ Eleccash.html.
74. "Electronic Commerce in NII", Report of Cross - Industry Working Team, USA, (Dec. 1999), www.xiwt.org/documents/Ecommerce.html.
75. "EMP Survivability of Military Equipment - A review", RK Chopra, Defence Laboratory, Jodhpur, 1998.
76. "End to End Dependability of the Engineering Information Infrastructure", Report of the Joint Cross Industry working Team / Bell Core Workshop, USA, (1998), www.xiwt.org/documents/march1998.wksh.html.
77. "Executive Summary of Quadrennial Defence Review" DoD, USA, 1998, <http://www.com .org/gdr/pgarrity.htm>.
78. FM Tesche, "Electromagnetic Topology : Analysis of RF Effects on Electrical Systems", PPT Slides Prepared under AFOSR MURI Grant, Clemson University, USA, June 2001.
79. "FY 1997 Defence Technology Area Plan: for weapon: Ch. 3.9 DEW_HPM", DoD, USA, 1997, <http://www.fas.org/ssp/military/docops/defnce/dtap/weapons>.
80. "Food, Air, Water and Terrorism: Perspectives on an evolving landscape" PPT Slides Presentation by Robert J. Clerman, MTS systems, USA, 1999.
81. Georg Schofbanker, Linz, "Why Arms Control Matters: Perspectives for Cyber Arms Controls", PPT slides presented at Austrian Information Center for Security Policy and Arms Control, ISODARCO, Aug. 2002.

82. Gord Cook, Barmaby Godley, " Systems Design Engineering 1999-2000 4th year Project Workshops Automobile Killer", University of Waterloo, USA, Nov. 1999.
83. "Global Information Infrastructure Commission, GIIC Overview, 99". <http://www.giic.org/events/ec990615 India.html>.
84. "Global Information System Development" Policy Paper on Telecommunication Services, 1996. <http://www.giic.org/pubs/polpapers.html>.
85. "GoAP eGovernance IT Architecture" Report of Government of Andra Pradesh prepared by Price Water House Coopers, State Secretariat, Hydrabad, Jun. 2001, www.ap-if.com/cde.pdf
86. "Guidelines for Developing an Information Strategy", A report Prepared by Coopers and Lybrand and the JISC's Information Strategies Stemming Group, JISC, Northvon House, Bristol, UK, Feb 2001, Email JISC@JISC.ac.UK.
87. "High Energy Microwave", Project Report of High Energy Microwave Device Consortium, Under Multi University Research Initiatives (MURI), Texas University, USA, Krisk@coe.ttu.edu, (1999).
88. "High Power Radio Frequency Weapons: A potential Counter to US Stealth and Cruise Missile Technology", Report by Col. John Brunderman, USAF, Center for Strategy and Technology, AWC, Maxwell Airbase, Alabama, Dec. 1999.
89. "High-Power Microwaves: An Overview with a Focus on Cerenkov Devices," J.A. Swengle, Ph.D., Lawrence Livermore National Laboratory; AMEREM '96 International Conference on "The World of Electromagnetics."
90. "Homeland Security Initiative", PPT Slides on Training Aspects prepared by Naval PostGraduate School, Monterey, California, USA, Aug. 2002. Pstockton@nsp.navy.mil.
91. "HPM Hardware Products Developed under Grants DE_FG03_01ER83209, by Calabazas Creek Research, Inc. USA, (2002), RLives@calcreek.com.
92. "HPM Sources, Diagnostic and Effect Testing" Voss Scientific, USA, (Dec. 2000), www.vosssci.com/hpm.html,
93. "HPM Terrorism," Major General Vladimir M. Loborev, Russian Federation Ministry of Defense Central Institute of Physics and Technology; AMEREM '96 International Conference on "The World of Electromagnetics."
94. Hardware Design and Software Development Services, "Calabazas Creek Research Inc., USA, (2002), RLives@calcreek.com.
95. "Information Assurance and Critical Infrastructure Protection- A Federal Perspective", Position Paper by Government Electronics and Information Technology Association, USA, 2001, <http://www.geia.org/pdf/ IA Position Paper. Pdf>.

96. "Information Superiority and Future of DoD: Opportunities, Risks, Challenges" PPT Slides by Dr. David S. Alberts, 2001, <http://www.dodccrporg/is/infosup.html>.
97. "Information Superiority and Network Centric Warfare "Defence Science Agency Information Systems, brief by Dr. David S. Alberts, (1999).
98. "Information Survivability of Interoperable Military Systems in High Threat Environment", "PPT Slides of Seminar sessions D1 & D2, Dr. Anita D Amico, Northrop Grumman, Lt Col. Perry Luzwick, DISA, D33 and Dr. Jerry Kovacich, Northrop Grumman, e-mail anita_beadon@atobc.northgrum.com
99. "Information Technology, National Information Infrastructure: Agenda for Action Version 1.01", the Action Points by the Concerned Project Agencies of the US, NII Initiatives. Metalab.unc.edu/nii/NII_Agenda-far-action-hml.
100. "Information Technology for the Masses, Part I, Recommendations", Report of the working Group, MIT, GOI, New Delhi, Jul. 2000.
101. "Information Warfare and International Security" NATO Report AS 285 stc (99) 8E to Parliamentary Assembly Committee on Science and Technology, Oct 1999. <http://www.iwar.org.uk/iwar/resources/nato/as285stc-e.html>.
102. "Information warfare-Defence, Appendix A, Threat Assessment", Report of National Science Board, USA, (1996), www.cryptome.org/iwd-a.html.
103. "Information Technology Action Plan", Report of the National Task Force on Information Technology and Software Development, NIC GOI, New Delhi, (Jul. 1988).
104. "Information Technology Action Plan II: Development, Management, Manufacture, and Export of Information Technology Hardware", Report of National Task Force on Information Technology & Software Development, NIC, GOI, New Delhi, (Oct. 1998).
105. "Information Technology Action Plan III : Long-term National IT Policy", Report of National Task Force on Information Technology & Software Development, NIC, GOI, New Delhi, (Apr. 1999)
106. "Invitation workshop on End-to-End Wireless Integration" Report of workshop sponsored by cross- industry working Team and Sun Microsystems,(Aug. 1998).www.xiwt.org/documents/etew_Report.html,
107. IFR FORWARD ENDCAP UPGRADE
By Concetta Cartaro , Francesco Fabozzi , Luca Lista *BABAR-Note-540, 25-MAY-2000* *Postscript Version from server* . <http://www.slac.stanford.edu/bbnotes.html>
108. ISBN0 - 16-055880-8, " Economic Espionage, Technology Transfers and National Security" the Statement of Lt. General Robert L. Schweitzer, to the Joint Economic Committee of the 105th Congress, USA, (June 1997).

109. "Joint Vision 2020", The Report of DoD, USA.<http://www.dtic.mil/jv2020/jvpub2.html>
110. Jasjit Singh "Asian Security in the 21st Century" Published by knowledge world and IDSA, New Delhi, Oct. 1999.
111. Judy Wall, "Time Line: Electromagnetic Weapons" Editor, Resonance News Letter, USA, 2002.
112. Kadiramangalam, M.N., M.I. Hoffert and G. Miller. "Onboard Energy Conversion and Thermal Analysis of the MTL System." In: Microwave and Particle Beam Sources and Directed Energy Concepts; Proceedings of the Meeting, Los Angeles, CA, January 16-20, 1989. Bellingham, WA: Society of Photo-Optical Instrumentation Engineers, 1989, p. 313-341.
113. King R.J. et al. "Phenomenology of Microwave Coupling Part I." Livermore, CA: Lawrence Livermore National Laboratory, November 1984. 91p.
114. Kopp, Carlo. "The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction." Clayton, Australia: Monash University, October 1996. 31 p.
115. Krall, J. and Y.Y. Lau. "Modulation of an Intense Beam by an External Microwave Source - Theory and Simulation." Interim report. Washington, DC: Naval Research Laboratory, 7 October 1987. 17p.
116. Laurence D. Merkle, Robert E Peterkin Jr. et. at, " Virtual Prototyping of RF weapons: A DOD Challenge Project", Airforce Research Laboratory, Kirtland, AFB, USA, Jan 1998.
117. Lavine, T.L. et al. "High-Power Radio-Frequency Binary Pulse-Compression Experiment at SLAC." Stanford Linear Accelerator Center, CA. May 1991. 13p. In: 1991 Institute of Electrical and Electronics Engineers (IEEE) Particle Accelerator Conference (PAC), San Francisco, CA, 6-9 May 1991.
118. Lawrence T Greenberg, Seymour E-Goodman and Kevin I Soo Hoo, "Information Warfare and International Law", National Defence University Press, (1998).
119. Lt Cdr. Irene M. Smith, "Information Warfare the New Battle Space", "Surface Warfare Magazine Vol. 24, No. 2, (Mar/Apr. 1999).
120. Legro, J.R., N.C. Abi-Samra and F.M. Tesche. "Study to Assess the Effects of Magneto Hydrodynamic Electromagnetic Pulse on Electric Power Systems." Phase 1, Final Report. Volume 3. Pittsburgh, PA: Westinghouse Electric Corp., Advanced Systems Technology Division, May 1985. 135p.
121. Lemke, R.W. "Linear Stability of Relativistic Space-Charge Flow in a Magnetically Insulated Transmission Line Oscillator." Final report. 2 January 1986-31 May 1988. Kirtland AFB, NM: Air Force Weapons Laboratory, April 1989. 103p.

122. Lemke, Raymond W. "Linear Stability of Relativistic Space-Charge Flow in a Magnetically Insulated Transmission Line Oscillator." In: Microwave and Particle Beam Sources and Directed Energy Concepts; Proceedings of the Meeting, Los Angeles, CA, January 16-20, 1989. Bellingham, WA: Society of Photo-Optical Instrumentation Engineers, 1989, p. 112-124.
123. Liska, D. and L. Dauelsberg. "Design of High-Power Radio-Frequency Drive Loops for Operation into 425-MHz Linear Accelerators." Los Alamos National Laboratory, NM. April 1988. 20p.
124. Lt. Gen. Abc. C Lin, "A look at the Military Applications of Information Warfare by Peoples Republic of China (PRC)", Communication Electronics Information Bureau, Min of National Defence, Taiwan, (2000).
125. Maj. Carmine Cicalese, "Information Systems Security Office (ISSO) Services" CINC INFOSEC Support, DoD, USA, Jun 2002.
126. Maj. Gen. Wang Pufeng, "The Challenge of Information Warfare, China Military Science, Spring 1995.
127. Major Scott W. Merkle, " Non-Nuclear EMP : Automatically the Military May Prove a Real Threat", Military Intelligence Bulletin, Air Force Base, Montgomery, Alabama, USA, (May 2002).
128. Marion A Rose "Nuclear Hardening of Weapon Systems (Part I)", Defence Electronics, Sep 1979.
129. Martin & Labicki, "What is Information Warfare?", Strategic Forum No.28, Institute for National Strategic Studies, National Defence University, USA, May 1995.
130. Martin Libicki, " What is Information Warfare" ACIS Paper 3, National Defence University, USA, (Aug. 1995).
131. Matt overholt and Prof. Brenner, " Cyber Terrorist Weapon, Methods and Techniques" <http://crypton.org/rfw-jec.html>.
132. Minimum Provisions for Investigation of Computer Based Offenses" Report Series No. 129.1, Australian Center for Policing Research, 1998. <http://www.acprogov.au>.
133. "Managing Access to Digital Information: An Approach Based on Digital Objects and Stated Operations", Report of Cross- Industry Working Team, (May 1997), updated in Dec. 1999, www.xiwt.org/documents/manageAccess.html.
134. "Measures and Protection Against Information Warfare - A proposal for Division of Responsibilities etc.. "Report No. 2 (Unclassified) from Cabinet working Group on Defence Information Warfare (FO -D/1A0), Sweden, Sep. 1998. <http://www.fhs.milselinstitute/kvi/cios/pdf/report2>.

135. "Measures and Protection against Information Warfare" Report No. 1 of the Cabinet Working Group on Defensive Information Warfare, Sweden, (Aug. 1997).
<http://www.fhs.milselinstitute/kvi/cios/pdf/report2>.
136. "Memorandum for High Performance Computing Advisory Panel for Selection of FY 2003 DoD, HPC Challenges Projects", Office of Director, Defence Research & Engineering, Pentagon, Washington, USA, Jun 2002.
137. "Message From Beijing, Part 3", News Brief by Dr. Alexander Nemets, Editor News Max.com, Mar. 2002.
138. "Military Critical Technology - Section 10, Information Technology", Defence Threat Reduction Agency, DoD, USA, (May 2000).
139. " National Security for a New Century", The White House Report, USA, Dec. 1999.
<http://www.clinton2.nara.gov/WH/EOP/NSC/html/documentsnsr.pdf>.
140. "National Plan for Information System Protection: Executive Summary ", The Report of the US President, (Jan 2000), <http://www.cryptom.org/cybersoc-plan.zip>.
141. "Nomadicity in the NII", Report of Cross- Industry Working Team, (Nov 1995, Updated in Dec. 1999).www.xiwt.org/documents/Scenariois.html.
142. "Non Lethal Warfare Management Structure and The Joint Non - Lethal Core Capabilities". User Conference on Non - Lethal Weapons, Directorate of Non-Lethal Technologies, DoD, USA (1999).
143. "Non Lethal Weapons for Military Operations other than War", Seminar on Military operations, Air Force Academy, USA, (1997).
144. "Nuclear Weapon EMP Effects", Federation of American Scientists. , Special Weapons Premier, Weapon of Mass Destruction, John Pike, (Oct. 1998).
<http://www.fas.org/nuke/intro/nuke/emp.html>,
145. ONLINE FRAME CLASH CALIBRATION SOFTWARE FOR THE LEVEL 1 CALORIMETER TRIGGER
By Paul McGrath *BABAR-Note-544, 02-NOV-2000 Postscript Version from server.*
<http://www.slac.stanford.edu/bbnotes.html>
146. ONLINE SOFTWARE FOR THE LEVEL 1 ELECTROMAGNETIC CALORIMETER TRIGGER SYSTEM
By David Wallom *BABAR-Note-546, 21-NOV-2000 Postscript Version from server,*
<http://www.slac.stanford.edu/bbnotes.html>
147. Prof. David B Rutledge, "Research in Audio and Microwave Circuits and Antennas",
<http://www.its.caltech.edu>.

148. Project Groups and Areas of Activities at Stanford Linear Accelerator, ARDA, CA, USA, <http://www.slac.stanford.edu>.
149. "Perspectives on US Homeland Security Activities" PPT slides. Presented to US-EU workshop on Critical Infrastructure Protection. by Dr. Sam Varnado, Director Infrastructure & Information Systems, Sandia National Laboratory, USA, Sep. 2002.
150. "Program Complexities of India's Information Infrastructure Security and Information Warfare Initiatives for the Year 2000 and beyond", Reports by Admiral Arun Saxena and Commodore Prem Chand, spread over 10 volumes, described below, WESEE, Ministry of Defence, New, (Jan. 2000).
- Volume - I: "Information Warfare Perspective and preparing the Nation to meet this Challenge".
- Volume - II: "Non - Lethal and Less Lethal Technologies and their role in Information Warfare".
- Volume - III: "Information Warfare Threat Assessment for a Defensive and Offensive Security Posture".
- Volume - IV: "Development Initiatives for Protection of National Information Infrastructure".
- Volume - IX: "Need Assessment for Interoperable and War Quality Databases - A Case Study for Naval Command & Control Applications".
- Volume - V: "Necessity and Relevance of Constitutional Sovereign and Military Issues for Living in A Cyber Society".
- Volume - VI: "Development of EMP Weapons - A Blue Print for National Initiatives".
- Volume - VIII: "Script for Industry and Institutional Partnership in India's Information Warfare Initiatives".
- Volume - X: "Management Challenges for National Information Infrastructure Security and Information Warfare Initiatives".
- Volume -VII: "EMP and Tempest Protection Program for National Information Infrastructure - A Route for Survival in the Information Warfare Environment".
151. "Proliferation and Significance of Radio Frequency Weapons Technology", Statement of Dr. Irs W. Merrit, Chief, Concepts Identification and Application Analysis Division, Army Space & Missile Defence Command, USA, (Feb. 1998).
152. "Protecting the Homeland", Report of the Defence Science Board Task Force on Defensive Information operations, 2000 Summer Study Vol-II. Office of Under Secretary, Defence Washington, DC, USA, Mar.2001.

153. "Public Safety, Security and Critical Infrastructure Protection", Research Agenda, Science and Technology Policy Institute, Rand Corporation, USA, <http://www.randcc.com>.
154. "Publications of Accelerator Research Department - A (ARDA) : at Stanford Linear Accelerator Center "Oct 2002, <http://www.slac.stanford.edu/grp/ara/structuresmeetings>, CrystalTilghman Crystal@Slac.stanford.edu-MS-26_2575.
155. "Radio Frequency Weapons and the Infrastructure", paper submitted by Lt. Gen. (Retd.) Robert L. Schweitzer to the Joint Economic Committee of the US Congress on 17th June 1997.
156. "Research Needs in Critical Infrastructure Protection", Slides Presented by Terry Kelly, Senior National Security Officer, White House office of S&TP, USA, March 2001.
157. "REVIEW OF SOFTWARE FOR THE LEVEL 1 CALORIMETER TRIGGER"
By Paul Dauncey *BABAR-Note-547, 06-DEC-200* ,
<http://www.slac.stanford.edu/bbnotes.html>
158. "RF Terrorism – A Menace of the 90's," A.E. Pevler; limited distribution white paper; January, 1992, <http://www.hektik.org/hightech/herf.html>.
159. "RF Weapons in the Hands of Terrorists – Threats and Countermeasures," A.E. Pevler; 5th National Conference on High Power Microwave Technology; June 1990 .
160. "Risk Management Process and Risk Assessment: The Challenges of CIP Interdependencies" PPT Slides, presented to Critical Infrastructure Protection Task Force at University of Tulsa, Canada, Sep. 2000.
161. "Roadmap for National Security: Imperative for Change. " The phase III Report of the US Commission on National Security / 21st Century", Feb 2001, http://www.nssg.gov/phase_IIIF.R.pdf.
162. "Role and Mission of Live Testing of EMP Weapons", Statement of Mr. James F. O Bryan, Deputy Director Operational Test and Education, DoD, USA to JEC, US Congress of 25th Feb. 1998.
163. RADIATIVE BHABHA CALIBRATION FOR THE BABAR ELECTROMAGNETIC CALORIMETER
By Johannes Bauer *BABAR-Note-537, 17-APR-200* *Postscript Version from server*.
<http://www.slac.stanford.edu/bbnotes.html>
164. Rajinder S Siwach, "National Security and Process of Globalization", Indian Defence Review, Jan-Mar 99, p.89.
165. RC 21102 (94394) "Building a High - Performance, Programmable Secure Co-processor", IBM Research Report by Scan Smith and Steve Weingart, IBM Research Division, New York, USA, Feb, 1998.

166. RL 30735, "CRS Report for Congress on Cyberspace", by Steven A Hildreth, Congressional Research Service, The Library of Congress, USA, Jun 2001.
167. Robert E. Peterkin Jr. And John W. Luginland, HPM Division AFRL, "Parallel Computing for 3D Plasma Simulation" PPT slides presented during controller / Guarantee Meeting, Stanford University, USA, Jul. 2001.
168. Robert J. Barker, PC, Edl Schami loglu, "High Power Microwave Sources and Technologies" ISBN 0780360060, IEEE, Publication , Jan 1991.
169. Robert M Frieden and William J drake, "Telecommunications in Information Age: The Global Information Infrastructure" Pennsylvania, State University, USA, 1997.
170. Ron Fisher and Jim Peerenboom "Lessons Learned from Industry Vulnerability Assessments and September 11th" PPT Slides presented at US DoE, Energy Assurance Conference, Arlington, Virginia, USA, Dec. 2001.
171. Ronald Knecht and Ronald A Gore, "The Information Warfare Challenges of a National Information Infrastructure" DISA, DoD, USA, 2001. Infowar.com & Interpact.Inc.welowarrior@Infowar.com
172. Scott D. Nelson and Robert A Anderson, "EM Field and Instrumentation Diagnostic in Support of the LFT & E HPM Methodology Testing", Lawrence Livermore National Laboratory, USA, (1998).
173. SLAC-PUB-6691, "Final Focus Testing Facility (FFTb), SLAC, Stanford, USA. WWW.stac.stanford.edu, (Feb 1999).
174. Stan Stahl, Ph.D. "Information Warfare : Defending Against Attack on Critical Corporate Data, Information and Systems : An Executive Guide", Solution Dynamics Los Angeles, CA, USA, Aug 2001, <http://www.solutionD.com>
175. Steven M. Rinaldi, "Sharing the knowledge: Government - Private Sector Partnership to Enhance Information Security" INSS Paper 33, USAF Academy, Colorado, May 2000, <http://www.usafa.af.mil.inss> .
176. "Security in the Information Age, New Challenges, New Strategies", Report of Joint Economic Committee of US Congress, Washington, USA, May 02.
177. "Software Products and Tools Developed under Grant DE-FG03-01ER 83209, by Calabazas Creek Research Inc. (CCR), USA, (2002), RLives@calcreek.com.
178. "Submissions to the United States Airforce AF 2025 Study in 1995 - 96", A sets of 5 documents on EMP weapons, by Carlo Kopp [carlo@cs.manash-edu.au]
179. "Table of Contents, 11th IEEE International Pulsed Power Conference, Baltimore, Maryland, 1997" Edited by G. Coopersteen and Vitkovitsky, IEEE Cat No. 97 Ch36127.

180. "Technology Environment Scan" Report Series No. 133.1, Australian Center for Policing Research, 2000. <http://www.acpro.gov.au>
181. "Tempest Monitoring Devices" , [http:// www.fas.org/irp/eprint/tempest.html](http://www.fas.org/irp/eprint/tempest.html), [http : www.esbimo.com/njoclm/tempest.html](http://www.esbimo.com/njoclm/tempest.html)
182. "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 "White House, USA, May 1998.
183. "The Design and Fabrication of Damage Inflicting RF Weapons by Backyard Methods", Statement of Mr. David Schriner before the Joint Economic Committee, of US Congress, (Feb. 1998).
184. "The Direct Threat of Electromagnetic High - Technology Weapons", Dr. Nicholas Chantler, Info War con, Vienna, 1997.
185. "The National Strategy to Secure Cyber Space", White House Report, Washington DC, USA, Feb 2003.
186. "The Official US Air Force Doctrine Document 2-5-4: Information Operations, DoD, USA, Aug 1998. [http://wwwcadre.maxwell.af.mil/warfaresudies/iwac/afold 2-5-1](http://wwwcadre.maxwell.af.mil/warfaresudies/iwac/afold2-5-1)
187. "The PRC's Research on Information Warfare, Its Influences over the RoC and the RoC's Counter measures", Report by Tseng Jangreny, Director, NDU Preparatory Office, Armed Forces University, Taiwan, (2000).
188. "The Radio Frequency Weapons Threat and Proliferation of Radio Frequency Weapons", Statement of Dr. R. Alan Kehas, Army Research Lab, Before the Joint Economic Committee of US Congress, (Feb. 1998).
189. "The Role and Mission of Live Fire Testing of EMP Weapons" Statement by Mr. James F. O Bryan, DD, OT & ELFT, DOD, USA, before the Joint Economic Committee of US Congress, (Feb 1998).
190. "The UK National Information Infrastructure "Report of Parliamentary Office of Science and Technology, Post Report Summary, (May1995).
191. "The Worldwide Threat in 2000", Statement of George Tenet, Director CIA, before the Senate Committee on Armed Services, USA, (Feb. 2000).
192. "TIA - Critical Infrastructure Protection (CIP) / Cyber Terrorism", [http:// www. TIA.com](http://www.TIA.com).
193. "Transient Electromagnetic Device (TED)" Shriner, (1998) [http:// www. House.gov/jec/hearing/radio/Schriner.html](http://www.House.gov/jec/hearing/radio/Schriner.html).

194. Tennenbaun, Jonathan, "Some ABC of the Electromagnetic Anti Personnel Weapons", Executive Intelligence Review Special Report, 99, Feb 1998, 31T Pency/vania AVE, SE Second Floor Washington, USA. <http://www.angelfire.com/or/mctrl.index.html>.
195. Testimony of Dr. Charles N. Brownstein, Executive Director, XIWT, Corporation for National Research Initiatives to US House of Representative Committee on Science, Subcommittee on Technology, USA, (June1996). www.xiwt.org/document/testimony.html
196. THE BABAR DRIFT CHAMBER DE/DX CALIBRATION PROCEDURE
By Federico Colecchia , Paolo Faccin *BABAR-Note-539, 04-MAY-2000 Postscript Version from server* . <http://www.slac.stanford.edu/bbnotes.html>
197. Timothy L Thomas, "Like Adding Wings to the Tiger: Chinese Information Warfare Theory and Practice", Foreign Military Studies office, Fort Leavenworth, KS, USA, 2000, http://www.certum_stuffgard.de/archive/ism.
198. TOOLS FOR IMPLEMENTATION OF THE EMC DIGITAL FILTER FEATURE EXTRACTION
By Matthew Weaver *BABAR-Note-543, 25-OCT-2000 Postscript Version from server* . <http://www.slac.stanford.edu/bbnotes.html>
199. Toshi Yoshihara, "Chinese Information Warfare: A Phantom Menace or Engineering Threat" ISBN 1-58487-074-5 (Nov. 2001).
200. US JP 3-54, "Joint Doctrine for Operations Security", DoD, USA, Jan 1997.
201. US JP3 -13, " Joint Doctrine for Information operation"
202. "US Army Field Manual 100-6 on Information Operations" US Army Command and General Staff College, (Aug 1996).
203. "Virtual Prototyping of RF Weapons", User Group Conference, Air Force Research Lab, Kirtland, USA, Presentation by Robert E Peterkim Jr et al. Jun 2000.
204. "Virus, Logic Bombs, Trojan Horses ect" ,[http : /www.outrack.com/hc/sc_5.asp](http://www.outrack.com/hc/sc_5.asp), [http : /www.Hackersclub.com/km/libraray/hack/virus.txt](http://www.Hackersclub.com/km/libraray/hack/virus.txt), <http://www.eecs.UIC.edu/ukbrown/compvip1.html>, <http://ukcc.uky.edu/Security/virusmemo>.
205. VV Onoochin, "Analysis of the Equivalent Circuits of Explosive Magnetic Generator of Frequency", Sirius, Moscow,(1998) E-mail a 33am@dol.rer.
206. "White Paper on Information Infrastructure Assurance", Security, Policy Board, 2001, <http://www.fas.org/sgp/spb/whitepap.html>. DoD, USA, Oct 1998.
207. WESEE-4001.0-IT-99 "Institutionalizing a National Framework for Policy Research in Information Operations: for setting up a Center for Information Technology Policy and

Minatory Issues, and a Center for National Information Infrastructure Security", Report by Prem Chand, WESEE, Ministry of defence, New Delhi, Nov 1999.

208. William Yurcik, " Information Warfare Survivability: Is the Best Defense good offence?" Dept. of Applied Computer Science, Illinois State University, (2000) wjyurci@ilstu.edu.

PUBLICATIONS

- 1) *"Managed Network and Security Services"*, Strategy Paper to create MNSS Business in India submitted to British Telecom, UK, June 2002
- 2) *"Impact of IT and e-Commerce on International Relations and Security"*, National Defence College, New Delhi. Jul. 2001
- 3) *"Protection of Critical Infrastructures: Need for a National Initiative"*. Published in National Security Council Report on Infrastructure protection (classified), June 2001
- 4) *"Indian Army Road Map for e-Security Awareness, Education Training and Certification"*, Approach paper for ADG (System), Army Headquarters, Feb 2001
- 5) *"Custodial Architecture for Security and Protection of Time Sensitive, Long life, High Value Electronic Records"*, Concept Paper for Futuristic Technology Development, Pending Application for IPR and Patent, Dec 2000.
- 6) *"Strategy for Security and Protection of the National Information Infrastructure"* conference on Asian Security in the 21st Century, Proceedings Published by knowledge world & IDSA, Edited by Jasjit Singh, Oct 2000
- 7) *"Network Centric Warfare Paradigms: Concepts and Architecture"*, (classified) WESEE, Ministry of Defence, New Delhi, May 2000
- 8) *"Program Complexities of India's Information Infrastructure Security and Information Warfare Initiatives for the Year 2000 and beyond"*, co-authored with Admiral Arun Saxena, spread over 10 volumes, described below, WESEE – 373.0- IW-2000-10/10., Ministry of Defence, New Delhi, Jan. 2000
 - Volume – I: *"Information Warfare Perspective and preparing the Nation to meet this Challenge"*
 - Volume – II: *"Non-Lethal and Less Lethal Technologies and their role in Information Warfare"*.
 - Volume – III: *"Information Warfare Threat Assessment for a Defensive and Offensive Security Posture"*.
 - Volume – IV: *"Development Initiatives for Protection of National Information Infrastructure"*.
 - Volume – V: *"Necessity and Relevance of Constitutional Sovereign and Military Issues for Living in a Cyber Society"*.
 - Volume – VI: *"Development of EMP Weapons – A Blue Print for National Initiatives"*.
 - Volume – VII: *"Script for Industry and Institutional Partnership in India's Information Warfare Initiatives"*.
 - Volume – VIII: *"EMP and Tempest Protection Program for National Information Warfare Initiatives"*.

Volume – IX: “*Management Challenges for National Information Infrastructure Security and Information Warfare Initiatives*”.

Volume – X: “*Management Challenges for National Information Infrastructure Security and Information Warfare Initiatives*”.

- 9) “*Conceptual and Architectural Framework for Development of Networking Components for Security and Self Reliance – Mission Mode Initiative at National Level*”, co-authored with IP-Cell Technology Ltd., Bangalore, WESEE-3741.0-IW-99, Ministry of Defence, New Delhi, Aug 1999

INVITED TALKS

1. *"Information Assurance Program: A lynchpin for the Navy in the Emerging Digital Age"* Navy Foundation, New Delhi, March 03.
2. *"Information Assurance Needs of the Indian Army"* Technology Seminar, MCTE, MHOW, Jan. 2003.
3. *"Information Assurance Program: An Imperative for Enterprise Information Infrastructure"*, ISACA Conference, Mumbai, Aug. 2002.
4. *"Business Continuity Planning: Imperative for IT Services Organization"*, PMO-NASSCOM Conference, New Delhi, Jun. 2002.
5. *"E-security- A New Wave opportunity for India in Global ITC Business"*, International Conference, NASSCOM- 2002, Feb. 02.
6. *"Information Technology Vision Policy and Road Map for Madhya Pradesh"*, Chief Minister, Bhopal, Dec. 2001.
7. *"E-security Practice, System Integration and Support for IT and Telecom Infrastructure"* IT&T Ltd. Noida, Sep. 2001.
8. *"Strategy and Road Map for Security of Navy Information Infrastructure"* Navy-CII Seminar, New Delhi, Oct. 2001.
9. *"Impact of IT and e-Commerce on International Relation and Security"*, National Defence College, New Delhi, Jul. 2001.
10. *"Pangs of Building the Defence Information Infrastructure"*, Navy-CII Seminar, Mumbai , Jun. 2001
11. *"National Cyberspace Security Concerns"*, United Services Institute, New Delhi, Dec. 2002
12. *"National Security Concerns in All Dimensions"*, National Security Secretariat, New Delhi, Jul. 2002

GLOSSARY

- C3** Command and Control: command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of a mission.
- C3W** Command-and-control warfare. The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions, command systems, rather than commanders, are the chief target, as in Persian Gulf war.
- Cracking** Illegally gaining entry to a computer or computer network in order to do harm.
- CSWS** Cylindrical Shock Wave Source
- CVCM** Counter Virus Counter Measures
- Cyberspace** The global network of interconnected computers and communication systems.
- DD** Dumpster Diving – Accessing an opponent’s information by examining the contents of garbage pails and recycling bins.
- DDA** Data Driven Attack – A form of attack that is encoded in innocuous seeming data which is executed by a user or other software to implement an attack. In the case of firewalls, a data driven attack is a concern since it may get through the firewall in data form and launch an attack against a system behind the firewall.
- DII** Defense Information Infrastructure. The worldwide shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structures serving a nation’s military’s information needs.
- DISA** Defense Information Security Administration, Military organization charged with responsibility to provide information systems support to fighting units.
- Army, Director of Information Systems for Command, Control, Communications, and Computers

DNS Spoofing	Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.
EMP	Electromagnetic Pulse. A pulse of electromagnetic energy capable of disrupting computers, computer networks, and many forms of telecommunication equipment.
EMP/T Bomb	A device to destroy electronic networks that is similar to a HERF Gun but many times more powerful.
Firewall	A system or combination of systems that enforces a boundary between two or more networks, i.e. an electronic gate that limits access between networks in accordance with local security policy.
GIE	Global Information Environment. A military term for cyberspace.
Hacker	A persons who either breaks into systems for which they have no authorization or intentionally overstep their bounds on systems for which they do have legitimate access, i.e. unauthorized individuals who attempt to penetrate information systems; to browse, steal, or harm in some other way.
HERF	High Energy Radio Frequency. A HERF gun is a device that can disrupt the normal operation of digital equipment such as computers and navigational equipment by directing HERF emissions at them.
INFOSEC	Information Security: Protection of classified information that is stored on computers or transmitted by radio, telephone, teletype, or any other means.
Intelligence-Based-Warfare	Warfighting characterized by rapid and effective acquisition and application of intelligence data. (cf. Libicki, 3995).
ISR	Intelligence/ Surveillance / reconnaissance (i.e., the set of the functions comprising the sensor / perception' interface of a military system).
IW	Information Warfare, is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries (Dr. Ivan Goldberg's definition)
IW-D	Information Warfare-defence- i.e., that subset of IW, which address protection of own-force systems and networks against intrusion and attacks.

Logic Bomb	Unauthorized computer code, sometimes delivered by email, which, when executed, checks for particular conditions or particular states of the system which, when satisfied triggers the perpetration of an unauthorized, usually destructive act.
NSA	National Security Agency. This agency is charged with the tasks of exploiting foreign electromagnetic signals and protecting the electronic information critical to national security.
PSYOPS	Planned psychological activities in peace and war directed to enemy, friendly, and neutral audiences in order to influence attitudes and behavior affecting the achievement of political and military objectives. They include strategic, psychological activities, consolidation of psychological operations and battlefield psychological activities.
RMA	Revolution in Military Affairs. The realization by the military that information, and information technologies must be considered as a weapon in achieving national objectives via military activity.
SPOOFING	Assuming the identity of another as in sending email under someone else's name.
TEMPEST	Military code-name for activities related to van ECK Monitoring, and technology to defend against such monitoring
TROJAN HORSE	A seemingly harmless computer virus that turns out to be extremely destructive
Van Eck Monitoring	Monitoring the activity of a computer or other electronic equipment by detecting low levels of electromagnetic emissions from the device. Named after Dr. Wim van Eck who published on this topic in 1985.
VIRUS	A Self replicating program that is hidden in another piece of computer code, such as an email.
WORM	A self-replicating destructive program that stands alone and spreads itself through computer networks.