

**ANALYSIS OF ISSUES OF INFORMATION SECURITY
METRIC IN INDIAN CONTEXT**

By

MANMOHAN CHATURVEDI

Submitted

In fulfillment of the requirements of the degree of

Doctor of Philosophy

To the



**BHARTI SCHOOL OF TELECOMMUNICATION
TECHNOLOGY AND MANAGEMENT
INDIAN INSTITUTE OF TECHNOLOGY DELHI
July 2012**

CERTIFICATE

This is to certify that the thesis entitled '**Analysis of Issues of Information Security Metric in Indian Context**' being submitted by Manmohan Chaturvedi to the Indian Institute of Technology Delhi for the award of the degree of **Doctor of Philosophy (PhD)**, is a record of *bona fide* research work carried out by him. He has worked under our guidance and supervision and fulfilled the requirements for the submission of the thesis, which has attained the standard required for a PhD degree of the Institute. The results presented in this thesis have not been submitted elsewhere for the award of any degree or diploma.

(Prof. MP Gupta)
Research Supervisor
Department of Management Studies,
Indian Institute of Technology Delhi

(Dr Jaijit Bhattacharya)
Research Supervisor
Department of Management Studies
Indian Institute of Technology Delhi

ACKNOWLEDGEMENT

I express my sincere thanks and appreciation to my supervisors Prof (Dr) MP Gupta and Dr Jaijit Bhattacharya for their patient and professional guidance towards shaping this PhD thesis from disjointed thoughts and material to a harmonious flow of ideas.

I would like to express my deep gratitude to all members of Department of Management Studies for providing an environment conducive to such intellectual pursuit.

I acknowledge the support provided by Mr. Dominic K., a freelance journalist, in reaching out to suitable Delphi members from industry.

Without active and positive involvement of Delphi members, this research would have been a non-starter. The anonymity of the Delphi members is a requirement of this methodology and, therefore, researcher is unable to acknowledge their personal details. I thank all of them for their invaluable contribution in shaping the findings of this research.

Finally, I would like to acknowledge the silent and total support of my wife Smita during this long and arduous journey.

(Manmohan Chaturvedi)

Abstract

The thesis attempts to suggest certain approaches which may lead to a more formal assessment of India's Information Security posture.

Information warfare with its various dimensions is a reality of present day Information society. Defensive strategy to counter the inevitable side effects of a digital economy is essential at national and international level. Concerted efforts at International level have resulted in ITU taking pro-active action on behalf of UNO to suggest comprehensive National Cyber Security framework. This framework throws certain challenges to the national governments to put in place measures stipulated there in. It is difficult to incrementally beef up Cyber Security measures without a metric on the current status and feedback to guide the policy makers towards threat mitigation strategy.

Literature survey confirms the spread of Information Warfare to civil domain from traditional military domain. A target-adversary matrix evolved from these considerations highlights the need for defensive Information Warfare initiative at national level to protect ICT assets in both military and civil (public and private sector) domains. The nature and complexity of the problem demands that key experts connected with India's Cyber Security apply themselves to address this challenge.

To begin with, the researcher has explored the existing approaches to Information Security in India and tried to evolve a suitable template for national level framework through literature survey. Using this basic framework, the researcher has acted as a facilitator to an expert Delphi group, selected from key stakeholders in Indian context, for identification and prioritization of the dimensions and indicators of National Information

Security construct using Delphi ranking methodology. In the next phase, relative weights of these indicators are ascertained using Analytical Hierarchy Process (AHP) methodology.

Alternate view of the inter-relationship amongst identified indicators is attempted using Interpretive Structural Model (ISM) and *Matrice d'Impacts Croises Multiplication Appliquee a un Classment* (MICMAC) and this view is synthesized with AHP results to generate useful insights of practical implication in designing a Cyber Security structure at the national level.

The validation of the research is achieved in two stages. In the first stage; we map the identified indicators with existing components of the Cybersecurity policies of various nations. This provides us the content validity.

In the second stage; we attempt external validation of NISI construct both in terms of Dimensions/Indicators and their relative weights through a survey of a selected expert group during a seminar and through Internet.

The construct of National Information Security Index (NISI) in Indian context is the outcome of this research. Finally, the possible use of NISI to measure India's readiness at national level to secure evolving NGN based telecommunication infrastructure is explored.

Contents

	Page Number
Abstract	i
Contents	iii
List of Figures	ix
List of Tables	xi
List of Appendices	xiv
List of Abbreviations Used	xv
 Chapter 1	 Introduction to the Study
	1
1.1	Background 1
1.2	Evolution of Information Warfare 2
1.3	Domains of Information Warfare 3
1.4	Cyber Security Initiatives at International level 4
1.5	Initiatives on Cyber Security in India 7
1.6	Motivation for the Research 11
1.7	Outline of Research 12
1.8	Organization of the report 13
 Chapter 2	 Literature Review
	16
2.1	Introduction 16
2.2	Information's role in warfare 16
2.3	Defining Information Warfare and its context 18
2.3.1	Forms of Information warfare 19
2.4	Expanse of Information Warfare Battle Space 20
2.5	Cyber-Warfare and Cyber Incidents trends 22
2.6	Trends in Cybersecurity Issues 24
2.7	Cyber Security Considerations 34
2.8	Conventional Military Warfare versus Information Warfare 41

2.9	Threats to ICT Infrastructure	42
2.9.1	Information Warfare Targets	43
2.10	A National Approach to Cyber Security	45
2.11	Indian Context: Evolving ICT infrastructure and related Challenges	46
2.12	Evolution of Next Generation Networks	50
2.12.1	Regulatory issues on deployment of NGN	51
2.12.2	Security aspects of NGN	52
2.13	Understanding Security Metrics	54
2.13.1	The Value of Security Metrics	55
2.13.2	Challenge of Cyber Security Metrics	56
2.14	Role of Practitioners and Researchers	57
2.15	Research Gaps	60
2.16	Concluding Remarks	63
Chapter 3	Design of the Study	64
3.1	Introduction	64
3.2	Problem Statement	64
3.3	Research Questions	64
3.4	Research Objectives	65
3.5	Related Issues	65
3.6	Scope	66
3.7	Research Methodology	67
3.7.1	Delphi Methodology	67
3.7.2	Analytic Hierarchy Process (AHP) Approach	69
3.7.3	Combining Delphi and AHP	73
3.7.4	Selecting the panel of experts	73
3.7.5	Delphi member's empanelment from various stakeholders in Indian Context	74
3.7.6	Questionnaires for Delphi process rounds	75

	3.7.7	Questionnaire for Analytic Hierarchy Process (AHP) Approach	76
	3.7.8	Synthesis & Validation of the research findings	77
3.8		Concluding Remarks	78
Chapter 4		Study of select national level initiatives to evolve a measurement model	80
4.1		Introduction	80
4.2		Indian Government Initiatives	80
4.3		Indian Industry Response	85
4.4		Threat Scenario at National level	87
	4.4.1	National level agencies connected with Information Security	88
	4.4.2	Recommended National Structure for Cyber Security	92
4.5		Need for a comprehensive view of national cyber security initiatives	94
4.6		ITU's perspective on National Approach to Cyber Security	95
4.7		USA's perspective of Information Security domain	95
4.8		South Korea's perspective on National Information Security	96
4.9		Industry and academic perspective on Information Security	96
4.10		Leading, coincident and lagging Indicators	96
4.11		The construct of National Information Security Index	100
4.12		Combined mapping of perspectives on Information Security Issues	103
4.13		A Model of National Information Security	112

Index

4.14	Concluding Remarks	114
Chapter 5	Design of National Information Security Index (NISI) in Indian Context	115
5.1	Introduction	115
5.2	Identification of Delphi members from various stakeholders in Indian Context	115
5.2.1	Identification of Dimensions and Indicators of NISI using Delphi methodology	117
5.3	Development of a Hierarchical Decision Model for AHP	118
5.3.1	Ascertaining Relative Weights of various dimensions	121
5.3.2	Instructions for Judgment Matrix	122
5.3.3	Illustration	123
5.4	Results	126
5.5	Discussion and Managerial Insight	130
5.6	Concluding Remarks	133
Chapter 6	Synthesis and Validation of Research Findings	134
6.1	Introduction	134
6.2	Analysis of interplay of dependency among indicators	134
6.2.1	Dependency Structure of Indicators of NISI	136
6.3	Analysis of hierarchical relationships of Indicators	137
6.4	Driving power and dependency of Indicators	138
6.5	Analysis of Indirect linkages amongst	141

	Indicators	
6.6	Synthesis of the insights about dependency and relative weights of Indicators	145
6.6.1	Important indicator identified by MICMAC analysis	146
6.6.2	Revisiting proposed National Structure for Cyber Security	147
6.7	Content and external validity of research	150
6.7.1	Related Studies	150
6.8	Methodology of Validation	153
6.9	Discussion of the results received from validation exercise	156
6.10	Concluding Remarks	176
Chapter 7	Applicability of NISI to evolving NGN Infrastructure	177
7.1	Introduction	177
7.2	Evolving NGN Infrastructure	177
7.3	Convergence and NGN	180
7.4	NGN and network security	182
7.5	Analysis of Threats to NGN by the NSTAC task force	187
7.5.1	Widespread Susceptibility	188
7.5.2	Threat Actor Convergence	188
7.5.3	Network Convergence Threat Impacts	189
7.6	Options at National level	189
7.7	How NISI concept can be used for secure NGN rollout?	190
7.7.1	Setting of Targets and their Measurement	191
7.7.2	Targets on Strategy Dimension	191

7.7.3	Illustrative yearly achievements - Strategy Dimension	192
7.7.4	Overall Performance Evaluation of Strategy dimension	192
7.7.5	Illustrative Computation of NISI	193
7.8	Concluding Remarks	195
Chapter 8	Conclusion	196
8.1	Introduction	196
8.2	Summary of the study	196
8.3	Revisiting Research Questions	198
8.4	Revisiting Research Objectives	199
8.5	Major Research Findings	202
8.6	Implications to Practice	203
8.7	Implications for researchers	205
8.8	Major Research Contribution	205
8.9	Limitations of Research	207
8.10	Future Scope of Research	207
8.12	Concluding Remarks	208
References		209
Appendices		246
Brief Curriculum Vitae		311