

**CYBERSPACE VULNERABILITY  
AND  
INADEQUACY IN  
CYBER GOVERNANCE :  
FIT CASE FOR CYBER NEXUS**

**VIJAY TIWARI**

*(Visiting Faculty – Department of CS & IT)*  
Centre For Advance Studies, Lucknow, (UP), INDIA

# **CYBERSPACE VULNERABILITY AND INADEQUACY IN CYBER GOVERNANCE : FIT CASE FOR CYBER NEXUS**

Copyright © : Vijay Tiwari  
Publishing Right © : VSRD Academic Publishing  
*A Division of Visual Soft India Private Limited*

**ISBN-13: 978-93-86258-78-6**  
**FIRST EDITION, OCTOBER 2017, INDIA**

*Printed & Published by:*  
**VSRD Academic Publishing**  
*A Division of Visual Soft India Private Limited*

**Disclaimer:** The author(s) are solely responsible for the contents of the papers compiled in this book. The publishers or its staff do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the Editors or Publishers to avoid discrepancies in future.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the Publishers & Author.

*Printed & Bound in India*

**VSRD ACADEMIC PUBLISHING**  
*A Division of Visual Soft (India) Pvt. Ltd.*

## **REGISTERED OFFICE**

154, Tezabmill Campus, Anwarganj, KANPUR – 208 003 (UP) (INDIA)  
Mob.: +91 9956127040 || Web.: [www.vsrdpublishing.com](http://www.vsrdpublishing.com) || Email: [vsrdpublishing@gmail.com](mailto:vsrdpublishing@gmail.com)

## **MARKETING OFFICE (NORTH INDIA)**

Basement-2, Villa-10, Blk-V, Charmwood Village, FARIDABAD-9 (HY)(INDIA)  
Mob.: +91 9899936803 || Web.: [www.vsrdpublishing.com](http://www.vsrdpublishing.com) || Email: [vsrdpublishing@gmail.com](mailto:vsrdpublishing@gmail.com)

## **MARKETING OFFICE (SOUTH INDIA)**

340, FF, Adarsh Nagar, Oshiwara, Andheri(W), MUMBAI-53 (MH)(INDIA)  
Mob.: +91 9956127040 || Web.: [www.vsrdpublishing.com](http://www.vsrdpublishing.com) || Email: [vsrdpublishing@gmail.com](mailto:vsrdpublishing@gmail.com)

## **P R E F A C E**

Cyber vulnerabilities are much talked about however these are less evident till they really strike someone as a first person or very closely related network. Analysis of such incidents show willful delay in notification and every attempt to hide the facts. The victim network will mostly not reveal the attack till is beyond their control to do so. There are ample advisories and guidelines from the agencies that handle such cases. Also lot of literature is available on what are the latest trends in this field. Adequate number of updates, patches and antivirus, anti malware packages are available to prevent exposure. In addition, cyber guideline and responsibilities of the service provider have been outlined to fix accountability.

Government is pushing for Digital India and introducing IT in every possible field so as to ensure transparent and accountable functioning of various departments. IT has the potential to remove corruption from the system if implemented properly.

Information Technology Act 2000 has been a stepping stone in the regulation of IT Assets, functioning of network elements by defining various gray areas and setting the legal parameters.

In spite of the tool and guidelines, cyber attacks take place and cause major data loss. These necessitate

investigation of the cyber attack vectors. I have discussed the potential of compromised employee, pirated third party software, non adherence of the cyber security procedure etc while outlining the cyber attack vectors.

Systematic connivance of Cyber attack vectors and exploitation of hidden cyber vulnerability leads to a much coordinated Cyber Nexus among state or non-state actors. It is a fit case for cooperation and very potent alternative to conventional conflicts. In fact cyber has already been established as a separate dimension of warfare.

*✍ Vijay Tiwari*

## **ACKNOWLEDGEMENT**

Technical book such as this book requires a team of supporters and this one is no exception. First, I am grateful for the outstanding assistance from members of my team. They provided me with responsive, courteous and expert comments throughout this book. I am equally grateful to the members of the Advisory Board, most of whom reviewed several manuscripts and contributed immensely towards quality of this book. I am also appreciative to the external reviewers for their quality and timely reviews.

I am also thankful to Prof Manish Gaur, Director, Centre for Advance Studies for providing enough motivation to venture out in this field.

Last but not the least, I would acknowledge and appreciate the efforts of my family members to provide stress free atmosphere at home throughout this work.



# CONTENTS

## CHAPTER ONE

### **CYBERSPACE AND VULNERABILITY ..... 1**

- 1.1. INTRODUCTION .....3
- 1.2. CYBERSPACE .....4
- 1.3. NETWORK FEATURES AND VULNERABILITIES.....5
- 1.4. POSSIBILITY OF ITS EXPLOITATION: THE NEED IS REAL.....8
- 1.5. CYBER SECURITY LAWS IN INDIA.....9

## CHAPTER TWO

### **CYBER GOVERNANCE FRAMEWORK..... 11**

- 2.1. INADEQUACY IN CYBER GOVERNANCE FRAMEWORK.....14
  - 2.1.1. HEALTH CARE SECTOR..... 14
  - 2.1.2. FINANCIAL TRANSACTIONS ..... 16
  - 2.1.3. SERVICE MANAGEMENT ..... 16
- 2.2. CYBER RISKS .....17
- 2.3. DIGITAL INDIA AND DESIRED IMPROVEMENTS IN CYBER GOVERNANCE .....17
- 2.4. RESOURCE COOPERATION: NEED, CHALLENGES AND WAY AHEAD .....18
- 2.5. COOPERATION TYPES .....19
  - 2.5.1. SHARING OF SPECTRUM RESOURCE ..... 19
  - 2.5.2. SHARING OF INFRASTRUCTURE ..... 20
- 2.6. WAY AHEAD AND SECONDARY SPECTRUM MARKET .....20

## CHAPTER THREE

### **POSSIBILITY OF CYBER NEXUS..... 21**

- 3.1. ENORMITY OF CYBER RISK .....24
  - 3.1.1. VULNERABILITY ..... 26

<b>3.2.</b>	<b>OBSOLESCENT PACKAGES .....</b>	<b>26</b>
<b>3.3.</b>	<b>FACTORS THAT ENCOURAGE CYBER NEXUS .....</b>	<b>27</b>
	3.3.1. NETWORK BOUNDARIES DEFY GEOGRAPHICAL BOUNDARIES.....	27
	3.3.2. LONG AND SUSTAINED PROCEDURE.....	27
	3.3.3. TECHNOLOGICAL ADVANCEMENT .....	27
	3.3.4. PROXY OR SHADOW CYBER OPERATIONS.....	27
	3.3.5. PLURALITY OF NETWORKING PRODUCTS .....	28
	3.3.6. BROAD BASED RESULTS AND FINDINGS .....	28
<b>3.4.</b>	<b>UNIQUENESS OF CYBER THREAT .....</b>	<b>28</b>
	3.4.1. WHY DOES CYBERSPACE PRESENT A POTENT THREAT .....	29
	3.4.2. OPERATING SYSTEM VULNERABILITIES.....	29
	3.4.3. UTILITY SOFTWARE VULNERABILITIES .....	29
	3.4.4. MULTIDIMENSIONAL ISSUE .....	30
	3.4.5. NUMEROUS AND EXTENSIVE VARIETY OF TARGETS.....	30
	3.4.6. EXTENSIVE PAYLOADS/TOOLS FOR THE CYBER ATTACK .....	30
	3.4.7. UNCLEAR RESPONSIBILITY TO ADDRESS CYBER THREATS .....	30
<b>3.5.</b>	<b>VULNERABILITY DISCLOSURE .....</b>	<b>31</b>
	3.5.1. NON- DISCLOSURE .....	31
	3.5.2. FULL DISCLOSURE .....	31
	3.5.3. RESPONSIBLE DISCLOSURE .....	31
<b>3.6.</b>	<b>CYBER OPERATIONS AND HIERARCHY SECURITY THREATS.....</b>	<b>31</b>
<b>3.7.</b>	<b>COUNTERMEASURES TO CYBER NEXUS .....</b>	<b>32</b>
	3.7.1. OWN NETWORK SAFETY .....	32
	3.7.2. STATE SPONSORED CYBER COOPERATION .....	33
	3.7.3. GUIDED APPROACH TOWARDS CAPABILITY DEVELOPMENT ..	33
<b>3.8.</b>	<b>NEED FOR CYBER DOCTRINE .....</b>	<b>33</b>
<b>3.9.</b>	<b>COORDINATED CYBER THREAT INTELLIGENCE INFORMATION .....</b>	<b>34</b>
<b>3.10.</b>	<b>CONCLUSION .....</b>	<b>34</b>

**CHAPTER FOUR  
CYBER ATTACK VECTORS ..... 35**

<b>4.1.</b>	<b>COMPROMISED EMPLOYEE .....</b>	<b>40</b>
-------------	-----------------------------------	-----------



<b>4.2.</b>	<b>PROBABILISTIC EPIDEMIC OUTBREAK MODEL.....</b>	<b>41</b>
<b>4.3.</b>	<b>INFECTION THROUGH EMAIL .....</b>	<b>43</b>
<b>4.4.</b>	<b>THIRD PARTY SYSTEMS AND PACKAGES .....</b>	<b>44</b>
<b>4.5.</b>	<b>INFECTION THROUGH REMOVABLE MEDIA .....</b>	<b>45</b>
<b>4.6.</b>	<b>ATTACK ON MOBILE DEVICE .....</b>	<b>46</b>
<b>4.7.</b>	<b>TARGETED ATTACK ON USER NETWORK .....</b>	<b>46</b>
<b>4.8.</b>	<b>CONCLUSION .....</b>	<b>47</b>

## **CHAPTER FIVE**

### **INSURANCE AGAINST CYBER ATTACKS..... 49**

<b>5.1.</b>	<b>INFORMATION TECHNOLOGY ACT, 2000 (IT ACT 2000).....</b>	<b>51</b>
5.1.1.	“ARTICLE 29. ACCESS TO COMPUTERS AND DATA.....	51
5.1.2.	BASIC DEFINITIONS AS PER IT ACT 2000 .....	52
5.1.3.	POWER TO ADJUDICATE .....	53
5.1.4.	ARTICLE 48. ESTABLISHMENT OF CYBER APPELLATE TRIBUNAL .....	53
5.1.5.	ARTICLE 61. CIVIL COURT NOT TO HAVE JURISDICTION .....	53
5.1.6.	ARTICLE 62. APPEAL TO HIGH COURT .....	54
<b>5.2.</b>	<b>DISCLOSURE OF CYBER BREACH.....</b>	<b>55</b>
<b>5.3.</b>	<b>INTERNATIONAL AGREEMENTS .....</b>	<b>56</b>
5.3.1.	ANALYSIS .....	57
5.3.2.	THE LAW RESTRICTING CYBER WAR .....	57
5.3.3.	ACHIEVING CYBER SECURITY LAWFULLY.....	59
5.3.4.	CYBER LAW ENFORCEMENT COOPERATION .....	59
<b>5.4.</b>	<b>SECURITY INCIDENTS .....</b>	<b>59</b>
5.4.1.	ESTONIA AND NATO.....	59
5.4.2.	GEORGIA–RUSSIA.....	61
5.4.3.	STUXNET .....	62

### **REFERENCES ..... 63**

