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

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

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 || Email: 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 || Email: 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 || Email: vsrdpublishing@gmail.com

PREFACE

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