Chapter-1
Introduction

1.1 Background

The Government of India has initiated a lot of e-Governance initiatives under Digital India programat national level such as, Aadhaar, digital locker, Direct Benefit Transfer (DBT), MyGov, PayGov etc.All the state Governments are also reaching to common people with e-Governance applications.These schemes require the use of communication and information technologies. The information structure for these is built by enterprises for the end customers and is used by common men for fetching the relevant information electronically. Cyberspace and infrastructure are vulnerable to a wide range of risk. These include risks emanating from both physical and cyber threats and hazards. The evolving nature of cyber attacks poses a major threat to government initiatives of e-Governance. Sophisticated cyber actors and nation-states exploit vulnerabilities of the information systems to steal information and money and have the capabilities to disrupt, destroy, sabotage and threaten the delivery of essential services. The requirement for cyber security emanates from warfare, espionage, national defense and for protection of intellectual property. Simultaneously confidentiality of information of employees and customers is required to be protected. While digitisation helps in improving information sharing and collaboration amongst all stakeholders, right protection throughcyber securityis mission critical to avoid any misuse of data.

1.2 Statement of the Problem

1.2.1 As part of Digital India Program, Government services are being made available to citizens electronically by storage of data online and building connectivity

infrastructure for fetching the information. Online records likeAadhaar, citizens biometrics, digital locker, financials, revenue records etc. requires Citizen's data to be stored/transacted online.All data which is stored or accessible online is susceptible to unauthorised access with malicious intent by individual/organised criminals, overseas adversaries, and terrorists. By gaining access to this data financial frauds can be committed, individuals can be targetted. Large scale cyber attack can also pose a challenge to National security and may also lead to destabilization of the economy of the country.The area of Information Technology (IT) is characterized by rapid developments and dynamic growth. With every IT product and service introduced into the market, newer vulnerabilities are discovered, leaving scope for malicious actions. Over a period, the nature and pattern of incidents have become more sophisticated and complex. In tune with the dynamic nature of Information Technology and limited time window available for an effective response, continuous efforts are required to be made to detect and prevent cyber attacks and ensuring safekeeping of data. With the proliferation of Information Technology, Internet users and related services and the advent of Internet of Things (IoT) there is a rise in number of cyber security incidents in the country as elsewhere in the world.

1.2.2 In order to address the issues of cyber security in a holistic manner, MeitY, Government of India had released the "National Cyber Security Policy-2013 (NCSP-2013)" in July 2013. The objective of the policy is to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country. The cyber security policy aims to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes,

technology and cooperation. It intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data".

1.2.3 As cyber crimes are a cause of global concern, many other countries like USA, Singapore, Australia etc. have also come out with their Cyber Security policies/strategies.

1.2.4 Vide this study; it is proposed to understand the present cyber security preparedness scenario in the country with respect to implementation of e-Governance/Digital India framework and issues involved. The status and magnitude of global vulnerability as well as vulnerability of Indian Government and citizen data to cyber attacks will also be enlisted. It is also attempted to catalogue a comparative study of Cyber security policy of India with those of some of the developed democratic countries such as USA, France, Singapore, Australia etc. Attempt will be made to analyse the provisions of National Cyber security policy (2013) in detail and the progress made on various implementation aspects till date. The dissertation will be concluded by attempting tounderstand the positives and shortcomings of the policy and to make a few recommendations to propose a way forward.

1.3 Objectives of the Study

Objectives of the study are as below:

(i) To understand the present e-services scenario in the country with respect to implementation of e-Governance/Digital India framework and issues involved.

(ii) To study the status of global vulnerability against Cyber Crimes.

(iii) To study the vulnerability of Government and Citizen data to Cyber Attacks in Indian context.

(iv) To analyse the provisions of National Cyber security policy (NCSP-2013).

(v) To catalogue a comparative study of Cyber security policy of Indiawith those of some of the advanced democratic countries such as USA, France, Singapore, Australia etc.

(vi) To propose a way forward for addressing shortcomings of the policy.

1.4 Research Questions

(i) Whether India's Cyber Security Policy is effective in tackling vulnerability to Cyber Attacks on Government IT Infrastructure, especially in wake of recent Digital India endeavours?

(ii) What could be the technological, legal and policy interventions that could help to fill the shortcomings to stay at par with global best practices?

1.5 Research design and methodology

The research design for this study is a mix of exploratory and descriptive. The data used for the study is a mix of both qualitative and quantitative data.

1.5.1 Primary Data

Primary data on policy aspects and the implementation has been collected through a pre designed semi structured questionnaire and interviews from selected stakeholders such as the concerned government department/ministry officials associated with formulation andimplementation of the policy.The contact was made through personal meetings with stakeholders, telephonically, email etc. In all five officials have shared their responses.

In addition to above for understanding the perception of the end users about cyber security and on the vulnerability of their information stored electronically, a structured questionnaire based survey was conducted. Selected users of e-Governance

services were distributed this questionnaire by way of email, Whatsapp messenger and hardcopies etc. In all one hundred and sixty threeusers have shared their opinion.

1.5.2 Secondary Data

Secondary data was collected from government policy documents, reports, parliament question replies, published articles/reports in academic journals and periodicals/books, policy documents from other countries governments published online. Though all these publications were considered, the best source for the secondary data was answers to parliament questions replied in Lok Sabha and Rajya Sabha.

1.6 Chapterisation Scheme

Chapter-One	:	Introduction
Chapter-Two	:	Current status of eGovernance services in India
Chapter-Three	:	Introduction to Cyber Security
Chapter-Four	:	Vulnerability to Cyber Crimes: Global and Indian Perspective
Chapter- Five	:	Literature Review
Chapter- Six	:	Cyber Security Policy of India: Analysis and comparison with other countries policies
Chapter-Seven	:	Research Findings and Analysis
Chapter- Eight	:	Conclusion and recommendations

1.7 Limitations/Delimitations

1.7.1 The secondary data collected from published reports and articles may bear the biases of the author or organization publishing them. However, the information taken from parliamentary questions replies is the stated factual position of government of

India. With regard to the primary data regarding the policy and implementation of the NCSP 2013, the opinion of serving officers from the concerned ministries may also have organizational affinity and bias.

1.7.2 Regarding the primary datacollected in survey, the samehad been taken from selected from e-governance users. Their responses are mainlyperception based as most of them were not aware of the nuances of cyber security as well as about critical aspects of NCSP-2013. Many of the users who took part in the survey weregovernment/private sector employees at senior positions who were otherwise well educated, affluent and have access to email and internet. Their survey may not actually reflect the perception of society at large and may be skewed to that extent.