Public-Private Partnerships in Indian Industrial IoT

A Set of Policy Recommendations to Improve Cyber Security

Chandrasekhar Muppiri (s1912046)

19 January 2019

Thesis Supervisors:

Prof.dr.ir. Jan van den Berg, TU Delft University

Sergei Boeke LL.M., Leiden University

This thesis was written in fulfillment of the requirements of the Executive Master in Cybersecurity from the Cyber Security Academy in The Hague, Netherlands.

Abstract

The Indian IoT ecosystem is projected to increase its connected devices to over 2.7 billion by 2020, of which the industrial IoT adoption is predicted to be playing a key role in this digital transformation. The research aimed to design governance policies to stimulate public private partnership (PPP) networks, in an effort to deal with (existing and upcoming) cyber risks in the Indian industrial IoT. The meta-governance process steps as presented by Dunn-Cavelty (2009) were applied for identifying the role of the government to coordinate and stimulate self-regulating PPP networks to achieve enhanced cyber security. While applying Hevner's design approach, the relevance of Indian IIoT business need was incorporated by first studying the present policy framework. A case study analysis using Consultative Objective Risk Analysis System (CORAS) was performed to identify risk treatment and attention points in the Indian PPP governance. These were corroborated with the interview inputs from public, private, and international experts active within the critical infrastructures and PPPs.

The findings conclude with the under-represented PPP policy recommendations for a continuous, responsive governance to the rapid technology advancements in the cyber domain. The recommendations are aimed to bridge the gap between policy and implementation. **"**Shortage of skilled manpower", "duty to care of all stakeholders", "unified cyber incident management with sectorial and state CERTs", and "fostering IoT startups", among others, are recommendations that need to be addressed. The policy recommendations on PPP governance are derived to accelerate and enhance cyber security in the Indian industrial IoT ecosystem.

Key Words: Industrial Internet of Things (IIoT), Public Private Partnership, Meta-Governance, Indian draft IoT policy, CORAS Risk Modeling.

Preface

This thesis is written in the partial fulfillment of Master of Science in Cyber Security at Leiden University conducted by the Cyber Security Academy, The Hague, The Netherlands.

Present research originated from thoughts on trust and information sharing requirement in public private partnerships(PPPs) in the Indian industrial Internet of Things (IoT). This triggered me to reflect on the Indian governance policies that can stimulate the PPPs to implement the public tasks. The adoption of a ubiquitous technology for any nation in a large scale requires promotion of PPP models to achieve larger IoT deployments. Similarly, more PPPs are expected to be part of the growing Indian industrial IoT. To my knowledge, such attempts were not taken up in research on the Indian industrial IoT ecosystem. The cyber threat landscape is projected to grow exponentially with deployment of internet of things (IoT) in the Indian industrial usage. These threats possibly lead to concerns for national security and safety of Indian citizens. This thesis attempts to recommend policy instruments required to enhance the cyber security of growing Indian industrial IoT ecosystem through the coordination and stimulation of PPPs by the Government of India.

I would like to thank my employer, the Ministry of Telecommunications, Government of India, for offering me a chance to complete this masters programme. I am confident that I can contribute to the cyber space governance framework. I would like to express my thanks to my colleagues and friends for their support in writing this thesis. I would like to specially thank my family: Madhavi, Nirmal Reddy, and Mamata Sekhar for their support, patience, time, and valuable comments during the entire period of completing this masters. Equally to my two supervisors, Prof.dr.ir. Jan van den Berg, who has supported me throughout my thesis and ignited my thought process with his criticism “Think”. I am grateful for his guidance and constructive reviews on my thesis. Mr Sergei Boeke LL.M., has motivated me and stood by me during my thesis. I am thankful for his advice in academic writing skills and with his feedback on my thesis. Finally, I would like to thank all the expert interview respondents for sharing their experiences and opinions which have contributed as invaluable resource for my thesis.

Table of Contents

Figures

Tables

List of Abbreviations

5G	.....	5th Generation Mobile Networks
APCERT	.....	Asia Pacific Computer Emergency Response Team
BRICS	.....	Brazil Russia India China and South Africa (Economies)
CaaS	.....	Cybercrime-As-A-Service
CAGR	.....	Compound Annual Growth Rate
CERT	.....	Computer Emergency Response Team
CERT-In	.....	Indian Computer Emergency Response Team
CI	.....	Critical Infrastructure
CIP	.....	Critical Infrastructure Protection
CoE	.....	Centre Of Excellence
CoE-IoT	.....	Centre Of Excellence for Internet of Things
CORAS	.....	Consultative Objective Risk Analysis System
CSIRT	.....	Computer Security Incidence Response Teams
DNS	.....	Domain Name Server
ERNET	.....	Education and Research Network (India)
EU	.....	European Union
FDI	.....	Foreign direct investment
GDP	.....	Gross Domestic Product
GDPR	.....	General Data Protection Regulation
GSAT-11	.....	Indian Geostationary Communications Satellite
HSD	.....	Hague Security Delta
IAMAI	.....	Internet and Mobile Association of India
ICANN	.....	Internet Corporation for Assigned Names and Numbers
ICS	.....	Industrial Control Systems
ICT	.....	Information and Communications Technology
IIoT	.....	Industrial Internet of Things
IIRA	.....	Industrial Internet Reference Architecture
IoT	.....	Internet of Things
IPV6	.....	Internet Protocol Version 6
ISAC	.....	Information Sharing and Analysis Centers
ISPs	.....	Internet Service Providers
IT	.....	Information Technology

ITES	.....	Information Technology Enabled Services
M2M	.....	Machine-2-Machine
NASSCOM	.....	National Association of Software and Services Companies (India)
NCIIPC	.....	National Critical Information Infrastructure Protection Center
NITI Aayog	.....	National Institute of Transforming India
OEM	.....	Original Equipment Manufacturer
OT	.....	Operational Technology
PIB	.....	Partners for International Business (Netherlands)
PPP	.....	Public-Private Partnership
R&D	.....	Research and Development
SCADA	.....	Supervisory Control and Data Acquisition
SMEs	.....	Small and Medium-Sized Enterprises
SOC	.....	Security Operations Center
SOPs	.....	Standard Operating Procedure
SPOC	.....	Single Point of Contact
UN	.....	United Nations

1. Introduction

Cyber attacks such as the "Stuxnet attack"[1] and "Attack on the Ukrainian Power Grid"[2] on industrial infrastructure indicate a new trend towards highly targeted attacks and sabotage by nation states. In May 2017, WannaCry ransomware had spread to over 300,000 systems in over 150 countries across the globe.[3] It struck more than 40,000 systems in India, affecting various organizations, mostly impacting essential service provider infrastructure including energy, transport, and health sectors.[4] After this incident, the Managing Director, Kaspersky Lab, South Asia, remarked that *"Most of the Indian organizations are still vulnerable to the attacks since the sophistication of these cyber threats is going up and many of Indian organizations including private and public sector still use outdated operating systems which make it easy for the cyber attackers to compromise the systems."*[5]

India today is in the 2nd largest internet markets[6] in the world with an opportunity to adopt the Internet of Things (IoT) technologies, through strong connectivity and effective use of next generation embedded devices for consumer usage, industrial control systems, and critical infrastructure. These systems generate, process, and exchange vast amounts of security-critical and privacy-sensitive data often using outdated operating systems which makes them attractive targets of cyber-attacks. This demands cyber threat intelligence for industrial control systems.[7] Cyber physical systems are ubiquitous; hence cyber-attacks on these IoT systems are critical. The complexity of these systems makes them vulnerable to possible cascading effects, often caused by the lack of critical infrastructure cross sector dependency analysis. Cyber attacks impact not just the nation but also across the board, e.g. the Internet Service Providers (ISPs), smart device hardware and software enterprises, the government, cyber security firms, and users.

Dr. VK Saraswat[8], Member, National Institute of Transforming India (NITI Aayog), pinpoints that, due to the rollout of sensor-packed Internet-connected devices, the IoT ecosystem remains the weakest environment for defense. This is due to the fact that these devices lack basic security features and are configured with simple default passwords, and these vulnerabilities allow hackers to exploit with brute force attacks. Justice B N Srikrishna, Chair of the expert committee appointed to draft the new data-privacy laws, commented prior to its first draft in June 2018 "*India has accelerated from a bail gaadi economy to a silicon-chip economy*", using the Indian national

[1] Karnouskos, Stamatis. "Stuxnet worm impact on industrial cyber-physical system security." IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society. IEEE, 2011.
[2] Case, Defense Use. "Analysis of the cyber attack on the Ukrainian power grid." Electricity Information Sharing and Analysis Center (E-ISAC) (2016).
[3] Saiphani, Kv, and G. Venugopal. "RANSOMWARE AND ITS IMPACT IN INDIA-A LITERATUER STUDY."
[4] Idem
[5] ET Bureau. "India Third Worst Hit Nation by Ransomware Wannacry; over 40,000 Computers Affected." The Economic Times, Times Internet, 17 May 2017, economictimes.indiatimes.com/tech/internet/india-third-worst-hit-nation-by-ransomware-wannacry-over-40000-computers-affected/articleshow/58707260.cms.
[6] Miniwatts Marketing Group. "Internet Top 20 Countries - Internet Users 2018." Senegal Internet Usage and Telecommunications Reports, 15 Dec. 2018, www.internetworldstats.com/top20.htm.
[7] Sadeghi, Ahmad-Reza, Christian Wachsmann, and Michael Waidner. "Security and privacy challenges in industrial internet of things." Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015.
[8] Indian Government, Vigyan Bhavan, and V.S. Saraswat. "NITI ." NITI , NITI Aayog, 2018. niti.gov.in/writereaddata/files/document_publication/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf.

language expression 'bail gaadi' for OX CART, "*but privacy and data regulation rules are still far behind*".[9] India is determined to protect its data and secure its citizens while modernizing the country's economy.

In the coming years, India needs priority action to strengthen the security of its operational technology (OT) and information technology (IT) infrastructure. This will guarantee fast and efficient information sharing between government to government, private to government, and private to private agencies with suitable security policies and guidelines to meet the upcoming security and privacy challenges in the Indian industrial IoT ecosystem.[10] These security and privacy issues for India attracts policy makers' and researchers' attention to design frameworks for setting objectives and recommendations to enhance cyber security. The objective of these policies and derived frameworks is to secure an industrial IoT ecosystem, accelerate innovations and invest in Industry 4.0 revolution, achieving a holistic cyber security framework for India to protect against industrial espionage and privacy of enterprises, customer and employees.

The Indian telecom infrastructure is positioned as a critical and essential sector that forms the backbone of emerging digital technologies like IoT. Hence, it is absolutely essential and crucial to uphold such essential sectors secure from cyber-attacks. Critical infrastructure (CI) extends essential services to all citizens where multiple players from both public and private sectors participate to build and operate a secure industrial IoT ecosystem. Possible cyber-attacks on such an essential service sector can have cascading effects and cause enormous impact on citizens' services and national security. In spite of a public private partnership (PPP) cyber governance in place, Indian CIs were impacted by WannaCry ransomware in 2017. Therefore, the cyber security governance accordingly needs to be aligned from an 'enhancing efficiency' mindset towards that of an 'enhancing security' mindset in all critical infrastructures (CIs) by a public private partnership (PPP) network governance structure with necessary policy adjustments and outlook.

The focus of the research described in this thesis is on improving the current public and private partnership (PPP) governance policies in India, to advance cyber security in industrial IoT.

1.1 Research Goal

The purpose of this research is to design governance policies to stimulate public private partnership (PPP) networks, and to deal with the risks in Indian industrial IoT. This includes a case study executed in the telecom sector. We discuss the unstructured issues of government, the public and private sectors as stakeholders in cyber security, with a focus leading to building governance policies in the IoT ecosystem based on existing experience and expertise. The derived policies are expected to bridge the tensions and challenges between public and private organizations. Implementing these policies are believed to enhance cyber security in critical infrastructure, which will in-turn strengthen the national security.
To achieve this goal, the central research question is framed as:

(RQ) Which PPP policies are required for enhancing cyber security in Indian Industrial IoT?

The below sub-research questions are formulated to enable our research towards the goal in a step by step manner.

[9] Rai, Saritha. "This Indian Judge Is Making Google and Amazon Nervous." Bloomberg.com, Bloomberg, 10 June 2018, www.bloomberg.com/news/articles/2018-06-10/tech-giants-nervous-as-judge-drafts-first-data-rules-in-india.
[10] Ministry of electronic and information technology. 12th Plan Report on Cyber Security. Government of India, 12th Plan Report on Cyber Security, meity.gov.in/writereaddata/files/downloads/Plan_Report_on_Cyber_Security.pdf.

Sub-Research Questions

(RQ1) What are the present policy instruments and institutions available to create a cyber secure environment in the Indian industrial IoT ecosystem?
(RQ2) What are the key areas of attention for designing PPP policies to enhance cyber security in Indian IIoT: A case study

(RQ3) What are the policies for effective PPP meta-governance in Indian IIoT implementation?

These are elaborated in the next sections of this thesis.

1.2 Methodology

The methodology applied in this research is a combination of Hevner's design approach and the Dunn-Cavelty PPP meta-governance conceptual framework. Hevner's design approach provides a continuous feedback assessment and Dunn Cavelty gives a governance model for the PPP critical infrastructure protection. The combined framework is intended to derive continuously improving policy artifacts for PPP meta-governance to address ongoing challenges in the context of this research.

1.2.1 Hevner's Design Science

The Hevner's approach describes the performance of design science research in information systems via a concise conceptual framework for clear guidelines for understanding, executing and evaluating the research as shown below:[11]

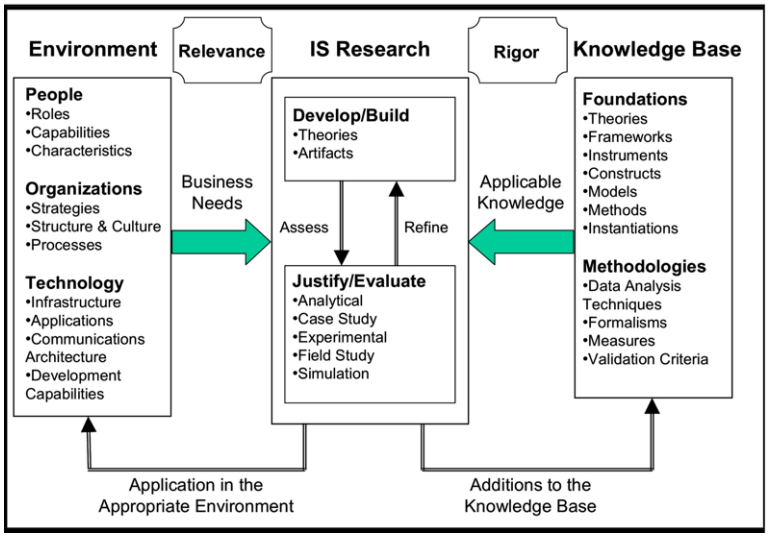

Figure 1 - Information systems research framework [23]

The core of this research consists of Hevner design science approach with three types of knowledge sources: 1) scientific theories and methods; 2) experience and expertise; and 3) meta-artifacts.[12]

[11] Hevner, Alan R., et al. "DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH." MIS Quaterly, Mar. 2004, wise.vub.ac.be/sites/default/files/thesis_info/design_science.pdf.
[12] Thuan, Nguyen Hoang, Pedro Antunes, and David Johnstone. "A Design Science Method for Emerging Decision Support Environments." arXiv preprint arXiv:1605.04725 (2016).

In the emerging Indian IoT based critical infrastructure, the unstructured issues of the government, public sector and private sector as stakeholders in cyber security can be addressed with this design approach since it combines a focus on problem relevance areas with meta-artifacts, thus solving real world problems.

1.2.2 Dunn-Cavelty PPP Roadmap for CIP Meta-Governance

Dunn-Cavelty proposes a four step approach for CIP meta-governance as below[13]:

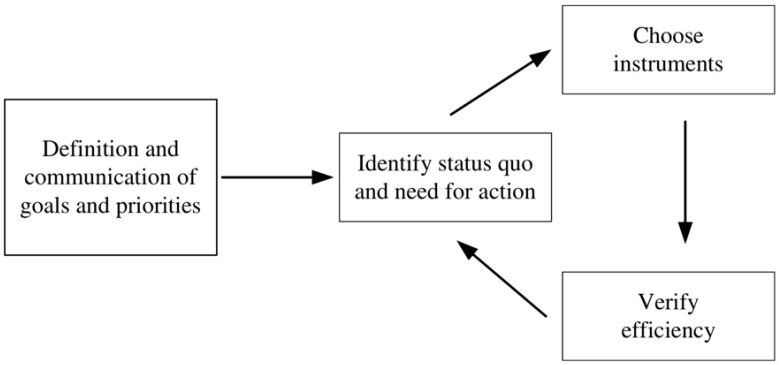

Figure 2 - The meta-governance process. [12]

Step 1: Define and prioritize PPPs goals in the larger security, economic and social context.

Step 2: To analyze the status quo and identify where action is required for effective functional PPP networks.

Step 3: Identify sector-wise suitable instruments to achieve self-regulating PPP networks.

Step 4: Efficiency of selected governance instruments measured on the goals and priorities set.

Thus, the final step leads as feedback to the assessment of the status quo (Step 2). As the following illustration shows, meta-governance is a continuous process. This provides a 'middle path' of critical infrastructure protection policies between interventionist and hands-off governance to protect the national security, which is a core function of the national government.

1.2.3 Design approach

The methodology being used here is to design PPP policy recommendations with innovative application in the IIoT ecosystem through a collaborative approach by networking and self-regulation among all stakeholders. The collaborative approach is the design activity necessary for the alignment of the Indian government strategy on IoT adoption.

[13] Dunn-Cavelty, Myriam, and Manuel Suter. "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." International Journal of Critical Infrastructure Protection 2.4 (2009): 179-187

Hevner's design approach can be used to build PPP governance policy artifacts for enhancing the cyber security in industrial IoT ecosystem based on existing experience and expertise.

Figure 3 below is constructed from the Dunn- Cavelty PPP model based on the network governance in Hevner's seven step approach. The design model is a concrete case for PPP in securing cyber domain to enhance cyber security in the Indian industrial IoT meta-governance. The unit of this design is the PPP governance in enhancing cyber security in the Indian industrial IoT incident management. This leads to creation of a meta-design on cyber security governance, which in practice should work.

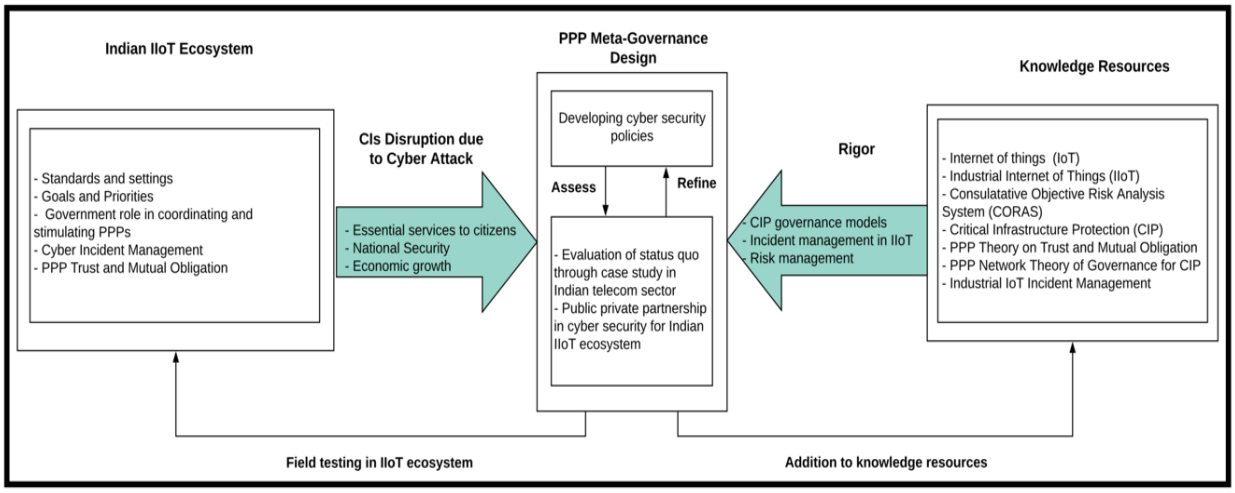

Figure 3 - The design of PPP meta-governance in Indian IIoT (adopted from (Hevner et al. 2004) and Dunn-Cavelty (2009))

The arrows used in the figure represent a continuous feedback loop to verify efficiency of the present cyber security policies, organizational goals and priorities, and government stimulation mandates. This allows the government to create policy artifacts that are suitable to meet the meta-governance of present day business needs through a harmonious PPP model. Ultimately, this self-regulatory model would recommend the required India-specific cyber incident management policies for IIoT adaptation to changes in every day societal needs

1.2.4 Validity

In this section, the validity of the chosen methodology is discussed. The operationalization of process steps is derived from the literature review of the elements in the Dunn-Cavelty meta-governance model. This is reinforced by the literature on the PPP trust element of Madeline Carr's national cyber security strategy. The above two literature reviews have been used to derive a design science approach using Hevner's design science to conceptualize the framework for operationalization in this research. Having a rational conceptual framework supports the validity of analysis on "The National digital communication policy 2018", "The Draft IoT policy 2015" and "The Indian Cyber Security Strategy" in cyber incident management of critical infrastructure using IoT. Indian government, public sector, private sector, academia, and international experts were interviewed. Questions were posed around perceived PPP experiences with the elements of security procedures, trust, accountability and responsibility, and information sharing practices in the Indian cyber security and evolving industrial IoT.

Responses of the dialogues are used to cross-validate the model to ensure the validity of the design steps followed. The questions conducted in the expert dialogue interviews are enclosed in Appendix I.

1.3 Structure

Chapter 2 answers (RQ1) by explaining the existing policy instruments and the institutions contributing to create a cyber secure environment with effective incident management in the Indian industrial IoT ecosystem. With the above policy instruments and institutions, the cyber governance mandates a socio-technical context for achieving cyber security within the Indian IIoT context. The three layer model as introduced by Van den Berg et al. which summarizes, *"both the technical and the socio-technical layer are governed - in complex ways - by a huge variety of human actors and organizations: this creates the so-termed governance layer of cyberspace"*[14] identifies the governance of cyber security as a key topic to address national security in the IIoT domain.

Chapter 3 describes a case study on Indian telecom as a non-experimental use case that relies on our interpretation of Indian policy instruments and interaction with field experts. The literature review is based on the latest Industrial Internet Consortium reference architecture of IIoT, and the Consultative Objective Risk Analysis System (CORAS) risk assessment. The incident management results in our understanding of the critical risks to be mitigated for achieving business continuity. The analysis of these critical risks leads to the identification of the attention points to arrive at design requirements for appropriate policy instruments. An expert dialogue with domain knowledge and policy makers has been conducted to add to the present knowledge base to help validate attention points for the design. The results of this case study provided an answer to (RQ2).

We argue in chapter 4, how the methodology framework as shown in Fig: 3 is suitable for the research design to create policy artifacts for the PPP meta-governance. The four areas of (i) Indian government IoT policy goals (ii) Trust and mutual obligation (iii) Incident management (iv) Indian government coordination and stimulation, are identified for further analysis within the Indian IIoT ecosystem. The interdependencies among these four areas will necessitate the PPP collaboration in cyber security for a secure IIoT ecosystem. Based on the results from the sub-research questions, and by the methodology framework, the PPP meta-governance design yields policy recommendations to achieve the research goal.

The policy recommendations are listed in chapter 5 and provide the answer to research sub-question (RQ3).

Expert dialogue interviews in a techno-social context have been held to substantiate validation. A discourse analysis revealed "*ongoing conversations, important debates, and interpretative conflicts existing in society*".[15] This methodological triangulation attested to the reliability of the findings.[16] In our research, expert dialogue interviews from the Indian government, public sector, private sector, academia, and international experts having knowledge of cyber security and PPP experience, appeared to be useful for two purposes. Firstly, to acquire the ground reality of the attention points through a case study. Secondly, the interviews helped to evaluate the existing policies and processes in identifying the requirements and design of the policy recommendations for the PPP meta-governance in the Indian IIoT ecosystem.

[14] Jan van den Berg, Jacqueline van Zoggel, Mireille Snels, Mark van Leeuwen, Sergei Boeke, Leo van de Koppen, Jan van der Lubbe, Bibi van den Berg and Tony de Bos, On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education, NATO STO/IST-122 symposium in Tallin, (c) pages 1-10, 2014.
[15] Talja, S. (1999). Analyzing qualitative interview data: The discourse analytic method. Library & information science research, 21(4), 459-477.
[16] Idem

2. Indian IIoT Ecosystem

In this chapter, the status of the Indian IIoT ecosystem is presented based on literature review available in the public domain. The understanding of the Indian industrial IoT is explained, including its reference architecture, current IoT policy standards and settings, goals and cyber incident management practices. The present cyber security institutions and their hierarchy in the Indian government with the perceived trust and mutual obligation of all stakeholders in the growth of Indian IoT ecosystem will be discussed.

2.1 Internet of Things (IoT)

Computing is a significant part of our lives which resulted in many developments during the past two decades. Mark Weiser (1991) coined the term "*Ubiquitous Computing*". He emphasized that computer devices will be embedded in everyday objects and communication networks will connect these devices to facilitate anywhere, anytime, always-on real time communications. This creates an era of ubiquity, where anything to anything communication generates big data traffic flow on the internet highways, thereby creating an "Internet of Things".[17]

The availability of Internet through wireless technologies, cloud computing and convergence of interdisciplinary technologies where IT hardware, software, network and domain skills are necessary, has led to an Internet of Things (IoT) revolution. The IoT as defined by the European Research Cluster on the Internet of Things (IERC) is: "*A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities, use intelligent interfaces and are seamlessly integrated into the information network.*" Three communication patterns co-exist: namely human-to-human (H2H), human-to-thing (H2T), and thing-to-thing (T2T).[18]

2.2 Industrial Internet of things (IIoT)

The present IoT developments are creating dynamic networks of physical devices and infrastructure with embedded intelligence towards usage in creating industrial environment for different types of goods and new services. This helps to accomplish present day real time needs to control the operational technology hardware and processes (e.g. sensor data in the healthcare domain, financial process data etc.). Identification through cyber-physical systems in the world of ubiquitous computing demands IIoT usage in industrial sectors. The real time sensory demands in

[17] Peña-López, Ismael. "ITU Internet report 2005: the internet of things." (2005)
[18] SRIA 2014. "Internet of Things." IERC-European Research Cluster on the Internet of Things, www.internet-of-things-research.eu/about_iot.htm.

IIoT systems/process failure may create downstream cascading impacts due to interdependencies among CIs, that can often result in critical emergency situations.[19]

The IIoT is a part of the larger concept of IoT, which is an intelligent interconnected network of devices, computers, and applications that collect and process huge amounts of data. In comparison to the data generated by IoT, the IIoT generates massive amounts of data or information to process big data, and so cloud computing, automation and machine learning come into prominence. Both the consumers' lives and the efficient management of the entire supply chain is enhanced.[20] Applicable to several industries such as manufacturing, oil and gas, chemical, logistics, aviation, and many others, a typical Industrial Internet Reference Architecture (IIRA) is shown in figure 4[21].

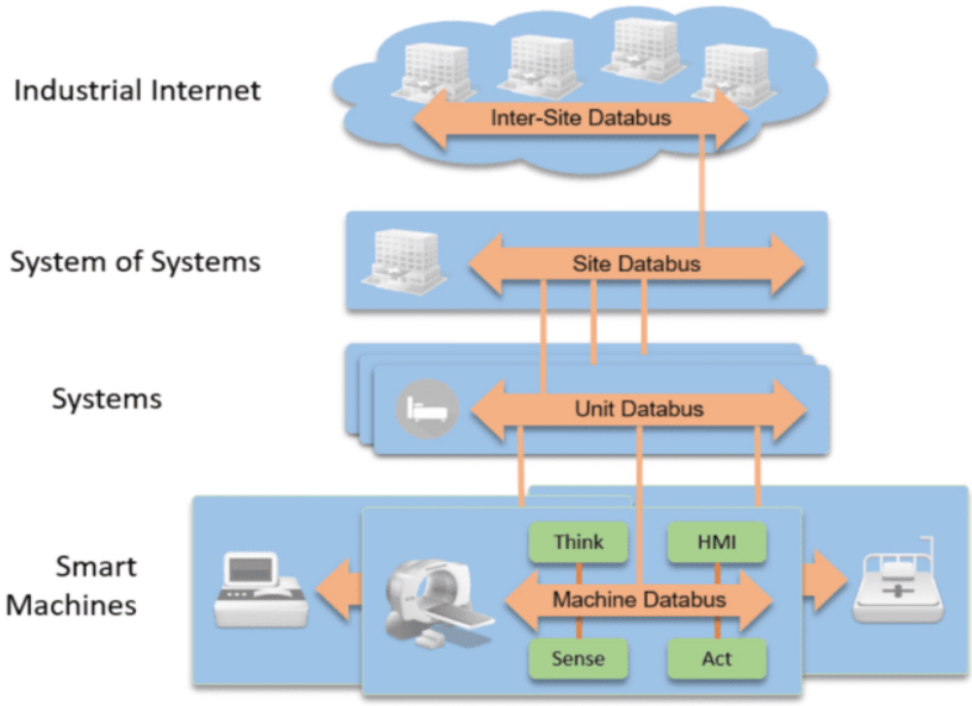

Figure 4 - Typical Industrial Internet Reference Architecture [29]

The IIRA document outlines the standards and methodology of the Industrial Internet of Things (IIoT) design including the latest advancements for the development of interoperable IIoT systems applicable across industrial sectors summarized below:[22]

- Includes the Layered Databus Architecture Pattern, Crosscutting Functions and Key System Characteristics, Functional Domain and Compute Deployment Model;
- A new appendix on Design Space Considerations that provides an illustrative overview of possible IIoT design parameters and constraints;
- Revisions to enhance clarity, which specifically reinforce the idea that 'the architecture patterns are only representative and not intended to be all inclusive'; and

[19] Peña-López, Ismael. "ITU Internet report 2005: the internet of things." (2005)
[20] Raut, Sandeep. "What Is The Difference Between Consumer IoT And Industrial IoT (IIoT)? | Articles | Internet of Things." Articles | Finance | Innovation Enterprise, 20 Feb. 2017, channels.theinnovationenterprise.com/articles/what-is-the-difference-between-consumer-iot-and-industrial-iot-iiot/
[21] Lin, S. W., et al. "The Industrial Internet of Things, Volume G1: Reference Architecture." Industrial Internet Consortium (2017).
[22] Idem

- As the IIRA is applicable to a broad spectrum of public sector operations and private sector industries, the IIRA does not define a specific architecture. It does, however, include several example architecture concepts and patterns to assist IIoT System architects in defining the optimal pattern for their specific set of requirements.

Clearly, IIoT is expected to deliver value to transform the business. The IIRA provides a framework for organizations to derive expected business value from IIoT projects from a business viewpoint.[23]

Data security in IIoT ecosystems is a challenge during transit and storage which contributes to the IoT ecosystem security posture. Therefore, it is essential to formulate policies for regulatory governance in protecting the supply chain to ensure confidentiality, integrity and availability in industrial IoT.

2.3 Draft Indian IoT Policy – A Snapshot

The draft IoT policy for India was rolled out in 2015 with a vision statement "*to develop connected and smart IoT based system for our country's economy, society, environment and global needs.*"[24] This section details the contents of the draft IoT policy to penetrate IoT adoption at multiple levels of governance, both central and regional states in a federal structure, with a view to create a secure IoT ecosystem.

Many public and private organizations are yet to mature in cyber-breach prevention, detection and incident response capabilities. Considering this, the response to cyber risks in protecting critical infrastructure (CI) is not robust and one of the key challenges for Indian policy makers is to ensure that the cyber security of Indian CI organizations is not to be viewed as an "IT issue".[25]

Ambitious plans through digitization for rapid social transformation, inclusive growth and India's prominent role in the IT global market led to focus on a suitable cyber secure ecosystem in the country, in time with a globally networked environment. By virtue of ongoing initiatives on Indian cyber security and IoT governance, India has garnered a ranking of 23 as per the UN cyber security index 2017 report scoring 0.683 percentile, ahead of Germany and China.[26]

It has been envisaged that by 2020 India would have a share of 5-6% of global IoT industry.[27] According to the draft IoT policy, and based on current situation and the future ambition portrayed above, India is considering a framework to make advancements in IoT via a multi-pillar approach. The approach is based on the following 5 guiding pillars[28] as highlighted in figure 5:

[23] Lin, S. W., et al. "The Industrial Internet of Things, Volume G1: Reference Architecture." Industrial Internet Consortium (2017).
[24] Ministry of Electronics & Information Technology. IoT Policy Document. Government of India, 2015, IoT Policy Document, meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.
[25] EY. Path to Cyber Resilience: Sense, Resist, React Global Information Security Survey 2016-17. 2017, Path to Cyber Resilience: Sense, Resist, React Global Information Security Survey 2016-17, www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2016-17-india-report/$FILE/EY-global-information-security-survey-2016-17.pdf.
[26] Brahima, S. "Global Cybersecurity Index 2017." International Telecommunication Union (ITU) (2017): 1-77.
[27] Ministry of Electronics & Information Technology. IoT Policy Document. Government of India, 2015, IoT Policy Document, meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.
[28] Idem.

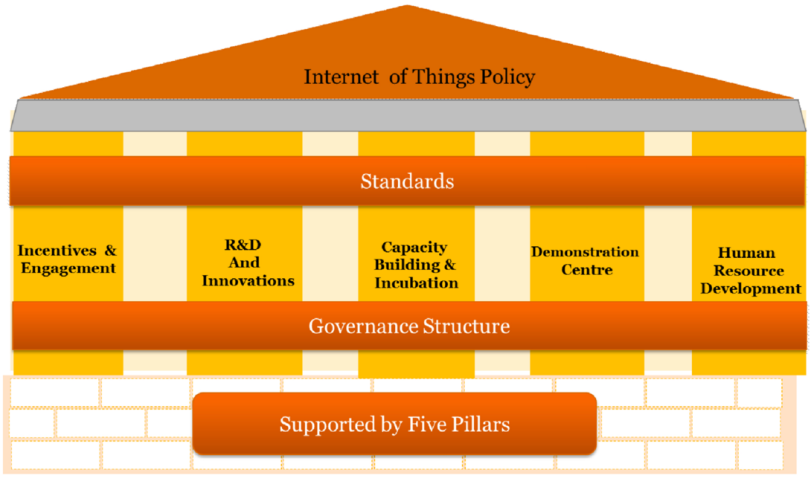

Figure 5 - Pillars of IoT as in draft Indian IoT policy, 2015 [31]

Below are the salient features of the five pillars of the policy draft.

- Incentives and engagements
- R&D and Innovation
- Capacity building and incubation
- Demonstration Centre
- Human Resource Development

The standards and governance layers cut across the five pillars as described below.[29]

Standards are defined:

- to facilitate global and national participation of industry and research bodies;
- to promote common standards around IoT technologies developed in the country; and
- to appoint relevant nodal organization for driving and formalizing standards related to technology, process, interoperability and services.

Governance Structure aims:

- to set up a public private partnership (PPP) model; and
- to set up and a high level Advisory Committee (AC) including representatives from the government, industry and academia to provide ongoing guidance in the emerging area of IoT.

The objectives of the draft IoT policy 2015[30] released by the Indian government is to build capacity for the IoT industry through the Centre of Excellence for the Internet of Things (CoE-IoT). The policy further mandates the IoT incubation infrastructure to support start-ups under PPP mode with the Indian IT trade association and the National Association of Software and Services Companies of India (NASSCOM).[31]

[29] Ministry of Electronics & Information Technology. IoT Policy Document. Government of India, 2015, IoT Policy Document, meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.
[30] Idem
[31] Idem

With expanding internet user base in India, cyber experts recommend building a digital infrastructure to predict and prevent cybercrime which is an impediment to IoT adoption.[32] On these grounds, the draft IoT policy lays emphasis on setting standards and creating supporting policies in monitoring incident response and disaster recovery capability. It also addresses the governance structure in determining the risk appetite of all public and private CI organizations as part of information risk management policies. Few policy recommendations on cyber security to the regional state governments are to establish state cyber emergency response teams (CERTs) to operate in conjunction with the Indian cyber emergency response team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC), and to implement periodical cyber drills on identity theft and security incidents.

The cyber security strategy 2013[33], provides some guideline and recommendations for the cybersecurity framework for Indian regional states under two categories (i) the PPP Model for cybersecurity and (ii) the Information security policy and practices. The PPP Model for Cybersecurity envisages the national cybersecurity framework and the government shall partner with the private sector and academia to strengthen cybersecurity posture of all citizens and businesses. The information security policy and practices shall be mandated at government functionaries and service providers, and the security audit adherence to international standards enforced along with the deployment of cybersecurity plans.

Thus, the national draft IoT policy lays guidelines to the cyber security at the national, strategic, tactical, and regional state levels for consumer and industrial usage implementation.

2.4 Indian IoT Growth Trends

Indian IoT startups are anticipated to consume 60% of the IoT ecosystem.[34] Speaking at the IoT India Congress in September 2017, Ms. Aruna Sundararajan, secretary of the Department of Telecommunications, Government of India, predicts that 10-15 million jobs are expected to be created through IoT, primarily by the growth of startups.[35] A regulatory framework is being outlined on how the information security will be addressed by the startups/SMEs working on IoT to deliver smart solutions. One of the priority focus of India is to supply health, education and financial services to remote geographical regions by fostering IoT initiatives for governance. These initiatives will bridge the Indian rural and urban digital divide to empower millions and address the needs of rural Indian citizens. Both cyber security and data protection should be ensured to create value propositions in the IoT ecosystem.

The regulatory framework by the Indian government includes (i) the Draft Indian IoT policy 2015, (ii) the Personal data protection bill 2018, (iii) the Cyber security strategy 2013, (iv) the 12th plan of cyber security 2018, and (v) the National Digital Communications Policy 2018 to address all the security and privacy challenges in cyber space. The objectives of these policies and derived frameworks are also relevant to the IIoT ecosystem to accelerate innovation and investment in the Industry 4.0 revolution. This results in a holistic cyber security framework for India to protect against industrial espionage, security and privacy of enterprises, customers, and employees.

The Indian industry 4.0 revolution is bringing the country into an arc of progress sweeping the world by rapidly adopting technology involving artificial intelligence (AI), the IoT, 3D-

[32] Kumar, Chethan. "One Cybercrime in India Every 10 Minutes - Times of India ►." The Times of India, Business, 22 July 2017, timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms.
[33] NCIIP: MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY. "National Cyber Security Policy, 2013." National Cyber Security Policy, 2013, 2013.
[34] Christopher, Nilesh. "IoT Alone Will Create 15 Million Jobs: Aruna Sundararajan - Times of India." The Times of India, Business, 15 Sept. 2017, timesofindia.indiatimes.com/people/iot-alone-will-create-15-million-jobs-aruna-sundararajan/articleshow/60524382.cms.
[35] Idem

printing, advanced robotics, and neurosciences.[36] The IIoT connectivity drives rapid convergence between the operational technologies (OT) used in SCADA systems and the information technology (IT) software and back office systems. IT and OT needs different product design. India's aspiration to seize the industry 4.0 revolution is evident by the MoU signed by BRICS in its annual meeting in July 2018 in South Africa on the cooperation to develop skills on cyber security, IoT, data analytics, and the IIoT.[37] In contrast to this ambition, it is observed that the budget allocation for year 2018 for digital transformation is a meager 0.15% of the budget of India, which is clearly insufficient to realize the policy execution.

The Dutch Trade Network in India (TNI)[38] indicates a highly promising potential for growth of cyber security stating that "*the current size of the Cyber Security industry in India is estimated to be USD 3.8B. Market watchers estimate that the Indian Cyber Security market would grow at a compounded annual growth rate (CAGR) of 15 – 20% during the years 2018-2023.*" Based on this estimation on the mega growth trend in the Indian cyber security industry including IIoT, regulation towards cyber security becomes compulsory to facilitate the trends, technology and supply chain in order to accelerate the emerging economy of India.

2.5 Cyber Risk Management

In the context of risk and incident management, CERT-In, under the Ministry of IT, Government of India is established to operate in conjunction with all the support framework to handle effective risk and incident management and prevent cybercrime. It is responsible to provide incident prevention and response services, security, quality, and raising security awareness among public citizens with a vision statement of "*proactive contribution in securing India's cyber space*".[39]

Dr. VK Saraswat, Member, NITI Aayog and Chancellor of Jawaharlal Nehru University, New Delhi, presents IoT cyber trends, challenges and threats for 2018[40] as

"The IoT is a weak link.

- *We're rolling out more and more sensor-packed, internet- connected devices, but the Internet of Things remains a major weak point for defenses.*
- *All too often these devices lack basic security features, or they aren't properly configured and rely upon default passwords that can give attackers easy access.*
- *This in turn is giving rise to botnets, which can be used for volumetric attacks, to exfiltrate stolen data, to identify further vulnerabilities, or for brute force attacks. We need to properly secure the IoT or it will continue to be a big issue in 2018."*

The Indian cyber emergency response team (CERT-In) reported 53081 cyber incidents in its annual report 2017.[41] Analysis of global data from 2013 to 2016 predicted the increasing trends in cybercrime-as-a-service (CaaS) besides ransomware attempts. The "Global Information Security

[36] Sharma, Pranjal. "What the Fourth Industrial Revolution Means for India." World Economic Forum, 3 Oct. 2017, www.weforum.org/agenda/2017/10/kranti-nation-india-and-the-fourth-industrial-revolution/.
[37] Department of International Relations and Cooperation. "10th BRICS Summit: Johannesburg Declaration." Government Programmes, Projects and Campaigns | South African Government, 27 July 2018, www.gov.za/speeches/10th-brics-summit-johannesburg-declaration-27-jul-2018-0000.
[38] RVO Netherlands. Cyber Security in India Opportunities for Dutch Companies . Rijksdienst Voor Ondernemend Nederland, 2018, Cyber Security in India Opportunities for Dutch Companies .
[39] CERT-In. "Indian - Computer Emergency Response Team." Indian - Computer Emergency Response Team, www.cert-in.org.in/.
[40] Indian Government, Vigyan Bhavan, and V.S. Saraswat. "NITI ." NITI , NITI Aayog, 2018. niti.gov.in/writereaddata/files/document_publication/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf.
[41] Annual Report (2017)Indian Computer Emergency Response Team (CERT-In) Ministry of Electronics & Information Technology Government of India 9th April, 2018

Survey 2016-17 - India Report"[42] focuses on cyber risks, suggesting that the increased levels of sophistication by CaaS syndicates are targeting employee weaknesses and carelessness in Indian organizations.

The recent SANS report[43] on securing industrial control systems(ICS) 2017, discusses the trends and other changes across companies that make active use of ICS as a core enabler for business imperatives. This report is in line with the Indian cyber risks in the industrial IoT organizations. The survey results in figure 6 indicate the top three threat vectors in ICS as: (i) 44% are devices and "things" that cannot protect themselves, (ii) 43% that are accidental internal threats, and (iii) external threats from hacktivists or nation-states that came in third at 40%.

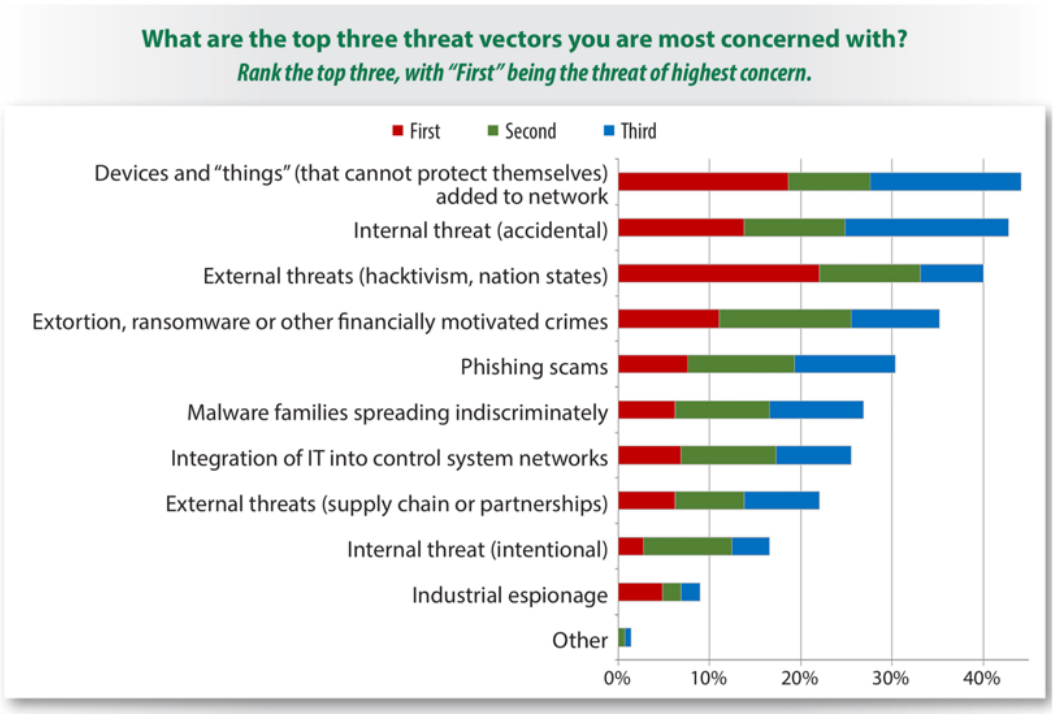

Figure 6 - Top threat vectors [20]

The observed concerns are the internal threat (accidental) and the increasing presence of connected devices, many insecure by design, in and around ICS environments. This is also an indication of the movement toward what is broadly called the Industrial Internet of Things (IIoT).[44]

For a true IIoT solution, the OT connectivity with internet based services brings interdependencies, as presently the lack of reference architecture embodies a standard in pursuit of reducing security risks to IIoT solutions. Multivendor product procurement and their interoperability issues is an impediment to achieving a consistent risk mitigation standard hampering the security posture of IIoT devices and systems.

[42] EY. Path to Cyber Resilience: Sense, Resist, React Global Information Security Survey 2016-17. 2017, Path to Cyber Resilience: Sense, Resist, React Global Information Security Survey 2016-17, www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2016-17-india-report/$FILE/EY-global-information-security-survey-2016-17.pdf.
[43] Gregory-Brown, Bengt. "Securing Industrial Control Systems-2017." A SANS Survey. SANS Institute (2017).
[44] Idem

Indian Cyber Security Governance Framework

All the central government ministerial agencies in the Indian cyber security hierarchy as mentioned in table 1 are responsible to develop policy strategies and coordinate with the state governments in the implementation of those policies. Additional responsibility of these government agencies is to issue specific standard operating procedures (SOPs) for securing the cyber space with the help of private sector and their third parties.[45]

Table 1 - Indian Cyber security governance framework (1) [24]

CYBER SECURITY HIERARCHY IN INDIA (1/2)					
PM OFFICE/CABINET SECY (PMO/CAB SEC)	MINISTERY OF HOME AFFAIRS (MHA)	MINISTRY OF EXTERNAL AFFAIRS (MEA)	MINISTRY OF DEFENCE (MOD)	MINISTRY OF COMMON INFO TECHNOLOGY (MCIT)	NON GOVT ORGANIZATION (NGO)
National Security COuncil (NSC)	National Cyber Corrd Centre (NCCC)	Ambassadors & Ministers	Tri Service Cyber Commad	Department Of Information Technology (DIT)	Cyber Security And Anti Hacking Organisation (CSAHO)
National Technical Research Org (NTRO)	Directorate of Forensic Science (DFS)	Defence Attaches	Army (MI)	Department of Telecom (DoT)	Cyber Society of India (CySI)
National Critical Info Infrastructure Protection Centre (NCIIPC)	National Disaster Mgt Authority (NDMA)	Joint Secretary (IT)	Navy (NI)	Indian Computer Emergency Response Team CERT-IN	Centre of Excellence for Cyber Security Research & Development in India (CECSRDI)
Joint Intelligence	Central Forensic Science Lab (CFSLs)		Air Force (AFI)	Educational Research Network (ERNET)	Cyber Security of India (CSI)

Table 2 - Indian Cyber security governance framework (2) [24]

CYBER SECURITY HIERARCHY IN INDIA (2/2)					
PM OFFICE/CABINET SECY (PMO/CAB SEC)	MINISTERY OF HOME AFFAIRS (MHA)	MINISTRY OF EXTERNAL AFFAIRS (MEA)	MINISTRY OF DEFENCE (MOD)	MINISTRY OF COMMON INFO TECHNOLOGY (MCIT)	NON GOVT ORGANIZATION (NGO)
National Crisis Management Committee (NCMC)	Intelligence Bureau (IB)		Def Info Assurance & Research Agency (DIARA)	Informatics Center (NIC)	National Cyber Security of India (NCS)
Research & Analysis Wing (RAW)			Defence Intelligence Agency (DIA)	Centre for Development of Advanced Computing C-DAC	Cyber Attacks Crisis Management Plan of India (CACMP)
Multi Agency Center			Defence Research Dev Authority (DRDO)	Standardisation, Testing and Quality Certification (STQC)	
National Information Board (NIB)					

[45] Indian Government, Vigyan Bhavan, and V.S. Saraswat. "NITI ." NITI , NITI Aayog, 2018. niti.gov.in/writereaddata/files/document_publication/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf.

Non-governmental agencies as indicated in table 2 participate (i) actively to highlight the industry issues (ii) in the consultative process to give feedback for all the central government policies so that the ground realities can be projected to achieve common Indian standards (iii) to create platforms for private sector players to engage in consultations (iv) to provide feedback on both technical standards and economic viabilities (v) to strive for achieving need for international standards (vi) to stimulate the private players and project it to government and (vii) to engage international businesses with central government to solve the identified issues.[46]

To achieve all the above initiatives, information sharing on cyber vulnerabilities and threat intelligence is an obligatory part of cyber risk management. These organizations which constitute the risk management framework need to coordinate across government and non-government organizations together with private players both in the form of partnerships and regulatory controls.

Apart from the national high level cyber security framework available, the national cyber security coordinator recommends a regional cybersecurity framework for all states that is envisaged in a PPP model. A certain level of autonomy is thus provided to the state governments for the responsibility of ensuring cyber security in their region. The regional frameworks are yet to be implemented across pan India as on date.

As per the present Indian cyber security governance, there is a requisite for the mitigation of cyber security risks in the IIoT ecosystem due to interdependencies. The present Indian IoT policy objective is to encourage PPPs to secure the critical infrastructure in the IoT domain. The governance of PPPs requires suitable regulating procedures for the stakeholders to contribute to the IIoT ecosystem. Building trust and motivating the PPPs by addressing possible disjunctive elements with network governance approach becomes vitally important to enrich cyber security in the process of digitization of Indian essential service infrastructure.

2.6 Co-ordination and Stimulation

Through the Information Technology Act 2000, a law was created in India by the Industry initiatives resulting in the creation of several institutions and agencies relevant to the area of cyber security such as the NCIIPC. Following the best practices in the area of cyber security power sector information sharing and analysis center, the ISAC power was created. Sectorial CERTs and the national information sharing and analysis center (ISAC) are still in the process of evolution. NASSCOM, a chamber of commerce of the IT and ITES industry is also licensed with all CIs to embrace various national and international standards and acts as a benchmarking framework for regulatory compliance. The Government of India has thus created a PPP model with the public and private sectors together the academia for rolling out a security framework to strengthen cyber security posture of the nation.

In the Indian context, CERT-In and the National Cyber Coordination Centre (NCCC) collaborate to raise cyber security at national, strategic and tactical levels. Few available regional state SOCs coordinate at individual state levels. Non-governmental agencies actively participate in highlighting the industry issues, providing consultation and feedback for all the central government policies. Through this, the ground reality is projected to achieve common Indian standards and leverage collaboration among all the stakeholders. Multi stakeholders are engaged by the

[46] Indian Government, Vigyan Bhavan, and V.S. Saraswat. "NITI ." NITI, NITI Aayog, 2018. niti.gov.in/writereaddata/files/document_publication/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf.

government for technical cooperation, to strengthen CI cyber preparedness, and to examine incident response processes. This results in enhanced information sharing in the nation to achieve and implement the national cyber security strategy by safeguarding public-private cooperation. Following the policy guidelines, a center of excellence (CoE) for IoT at Bangalore, India was launched in PPP collaboration with the Ministry of IT, NASSCOM, Tata Consultancy Services, Intel Corporation, Amazon web services, and FORGE enterprises.[47] An IoT hub in the Indian state of Andhra Pradesh is proposed to foster innovation and startups to create 50,000 jobs and grab a market share of USD 1.5 Billion by 2020.[48]The other Indian state governments are yet to initiate such PPP collaboration measures in IoT.

The draft IoT policy fosters PPP collaboration initiatives for developing new IoT and M2M solutions, primarily to focus on IoT industry enablement, to help central government and state government in tackling the urban and rural digital divide. The key stakeholders in the IoT initiatives are the citizens, the government and the industry. According to Gartner, the government IT in India was on track to spend USD 7.2 billion in 2016 as part of the digital India program.[49] PPP has played a vital role in this to support the rollout of digital India initiatives both at Indian central government and state government levels.

Thus, the public-private partnership (PPP) serves as the cornerstone of the national cyber security strategy, as addressing the challenges by the Indian government independently is impossible. Accordingly, Dr. Gulshan Rai[50], NCCC India, affirms that the government and private sector understand the need to enhance cyber security posture in a PPP model. The IoT policy, therefore, focuses on adopting the PPP model and proactive cyber incident management to instill trust and encourage information sharing of incidents and best practices to enhance the cybersecurity in IIoT across all industry sectors, regional and central government agencies.

2.7 Sub-Conclusion

Presently, the Indian government has in place the policy instruments such as (i) the Draft Indian IoT policy 2015, (ii) the Personal data protection bill 2018 (iii) the Cyber security strategy 2013 (iv) the 12th plan of cyber security 2018 and (v) the National Digital Communications Policy 2018 to address all the security and privacy challenges in cyber space. The IoT policy focuses through PPP models to enhance cybersecurity in IIoT.

Supporting the implementation of the above policies are various governmental, non-governmental and private agencies such as NCCC, NCIIPC, CERT-In, and NASSCOM institutions working in PPP mode to enforce cyber security. The objective of these policies and derived frameworks is to enable an IIoT ecosystem, accelerate innovations and invest in the Industry 4.0 revolution. This will achieve a holistic cyber security framework for India to protect against industrial espionage, security and privacy of enterprises, customer and employees.

With the above policies and framework, the draft Indian IoT policy aims to grab a share of 5-6% of global IoT industry by 2020.

[47] Gupta, Monika. "Indian Telecom Industry Getting Ready for M2M/IoT." Indian Telecom Industry Getting Ready for M2M/IoT, Aug. 2017
[48] Ministry of Electronics & Information Technology. IoT Policy Document. Government of India, 2015, IoT Policy Document, meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.
[49] PTI. "Govt's IT Spending to Hit $7.2 Bn in 2016: Gartner." The Economic Times, Economic Times, 3 Oct. 2016, economictimes.indiatimes.com/tech/internet/govts-it-spending-to-hit-7-2-bn-in-2016-gartner/articleshow/54658528.cms.
[50] EY. Path to Cyber Resilience: Sense, Resist, React Global Information Security Survey 2016-17. 2017, Path to Cyber Resilience: Sense, Resist, React Global Information Security Survey 2016-17, www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2016-17-india-report/$FILE/EY-global-information-security-survey-2016-17.pdf.

The Draft IoT policy 2015 is very ambitious in its objectives, however this is not very realistic due to significant reasons. With the aim of the Indian IoT industry to reach USD 15 billion by 2020, the budget allocation by government of India is by contrast a meagre 0.15% of its national budget for 2018. This works against the Indian aspiration of seizing the industry 4.0 revolution in view of the MoU signed in BRICS summit in July in South Africa focusing on cyber security, IoT, data analytics, and IIoT. The policy aims to foster innovation and startups, and a project to position the Indian IoT hub at Andhra Pradesh state by 2020 is proposed, but till date no infrastructure capacity building has been initiated. The PPP model implementation of the policy is ambiguous with different PPP types and the government is currently adopting a top down approach to implement the PPP strategy which is hindering the mutual cooperation between the various parties. For this reason, many public and private organizations are yet to onboard and become mature in cyber-breach prevention, detection and incident response capabilities. In a true IIoT solution, the OT connectivity with internet based services brings interdependencies. The Indian industrial IoT solutions are in want of a standard to reduce security risks which is presently incomplete due to the lack of an implemented IIoT reference architecture.

In the context of IoT deployment in CIs, the implementation of the IoT policy is analyzed for improvement of the PPP policies for enhancement of cyber security in Indian IIoT as a case study.

3. Case: Indian Telecom Sector in IIoT

Despite the existing Draft IoT policy 2015 guidelines on incident management strategies, recent attacks such as the 2017 BOTNET attack on the customer remote modems in the Indian public telecom network raise a need for enhanced cyber security. Therefore, a case study in the telecom sector is used to identify the PPP governance attention points that are required to determine gaps in the current implementation of cyber security policy instruments in the Indian IIoT. Industrial IoT market in India currently stands at $130 million annually in revenues of which telecom sector earns highest revenue of $47 million.[51] Hence it is justified to consider the telecom sector as a case, the findings of which can be extrapolated to other sectors of Indian IIoT.

3.1 Threat Landscape and Security Impact

The Government of India has big ambitions in the area of IoT with its National Digital Communications Policy 2018. One of the key objectives of this policy is to enhance the contribution of digital communication sector from 6% India's capital GDP in 2017 to 8 % and contribute to the global value chain ensuring Indian sovereignty by 2022.[52] The ambition to rapid expansion exposes an increased threat landscape. A comprehensive data protection regime for both consumer and industrial IoT applications is therefore important to secure digital communication infrastructure services and privacy to its citizens and businesses.

Strong IoT security would be a win-win proposition for Indian manufacturers, providers and purchasers unleashing significant economic growth across the nation. The Indian government needs to rollout initiatives to take multi-stakeholder positions towards the IIoT ecosystem development and deployment. Hence, both the public and private sector should co-operate in a PPP model to harness synergies with the IoT initiatives of Indian central and state governments.

The current physical systems treat IT and OT independently but they are mutually dependent in cyber physical systems of an IIoT ecosystem. Due to this impact, protecting the IIoT ecosystem from cyber attacks requires identification of appropriate risk analysis models. This is currently a key challenge within the existing PPP governance in digital communications.

The case study analysis is focused on the areas of governance for success of PPP models in the Indian Telecom sector IoT deployment. The technical security vulnerabilities in the IIoT ecosystem are excluded from the scope of this case study.

[51] Exhibitions India Group. "3rd Internet of Things India Expo 2019." IoT India, 2019, www.iotindiaexpo.com/iot-india-expo.aspx.
[52] Department of Telecommunications. "National Digital Communications Policy 2018." Department of Telecommunications, 2018, dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf.

3.2 Cybersecurity and Risk Identification

Risk is defined as the combination of the consequences and the likelihood of an unwanted event. The process to understand the nature of such risk and determining the level of risk is known as risk analysis.[53] A risk analysis may target any system, including systems of systems. When the analysis targets complex systems, the analysis should be fragmented, carried out independently for each sub system.[54] For the purpose of this thesis, the telecom sector is considered as a sub system in the complex IIoT ecosystem.

Telecommunications provide information networks and can be a single point of failure for critical infrastructures (CIs) across sectors, which are vital for growth of the Indian economy. The Consultative Objective Risk Analysis System (CORAS) addresses key challenges in protecting critical infrastructures with an integrated risk reduction of information based infrastructure systems.[55] If they are legitimate, CORAS risk assessment is able to handle arbitrary long chains of dependencies.[56] The IIoT ecosystem with security and privacy challenges of required encryption level, stealthy malware, access control, integrity and incident management of all the smart devices can be assessed by applying dependent CORAS diagrams in other critical infrastructure sectors. Considering these security and privacy challenges in the Indian telecom, respondent 8 states that "*all the experts will sit together and prepare the risk treatment plan using CORAS modeling. After this, we will discuss with each asset owner and servicing party to share the timeline and execution for good cyber hygiene. Continuous improvement with multiple iterations continues every quarter.*" This emphasizes the necessity of risk identification through CORAS modeling to protect the IIoT ecosystem from cyber-attacks and deliver efficient PPP models contributing to the Indian Telecom sector.

Figure 7 shows an overview diagram to capture threats, vulnerabilities and impact through the CORAS risk modeling in a deployed IoT Telecom network system using PPP. During this study, the CORAS process steps (four out of eight) have been followed to the extent applicable to the Indian Telecom domain. The non-relevant CORAS process steps are ignored in this analysis such as step 2 on the customer presentation of the target; step 4 on the approval of the target description; step 6 on the determination of risk levels; and step 7 on the acceptable risk of indirect assets. The below CORAS steps are applied for our analysis:[57]

- Step 1 is the initial preparation for context identification in the telecommunications domain.
- Step 3 is aimed at understanding the main telecom service assets.
- Step 5 is the risk identification step. To identify risks, CORAS make use of structured brainstorming that yield CORAS threat diagrams. These threats gave us unwanted incidents for telecom service business continuity.
- Step 8 deals with the risk treatment for protecting assets in telecom operations with a PPP model.

In the example, we have assumed three threat scenarios: (i) the deliberate human threat sabotage (hacker), (ii) an internal employee in an organization causing cybersecurity incidents from within, and (iii) the non-human threat due to sudden malfunction of the server, such as Programmable Logic Controller (PLC) in an IIoT ecosystem. The target of analysis in the example is limited to create an effective PPP model without any disjunctive elements. Similar threat scenarios can be extended to its dependencies.

[53] Brændeland, Gyrd, Atle Refsdal, and Ketil Stølen. "Modular analysis and modeling of risk scenarios with dependencies." Journal of Systems and Software 83.10 (2010): 1995-2013.
[54] Idem
[55] Idem
[56] Idem
[57] Stoelen, Ketil, and Gencer Erdogan. "The CORAS Method." The CORAS Method, 16 Nov. 2015, coras.sourceforge.net/.

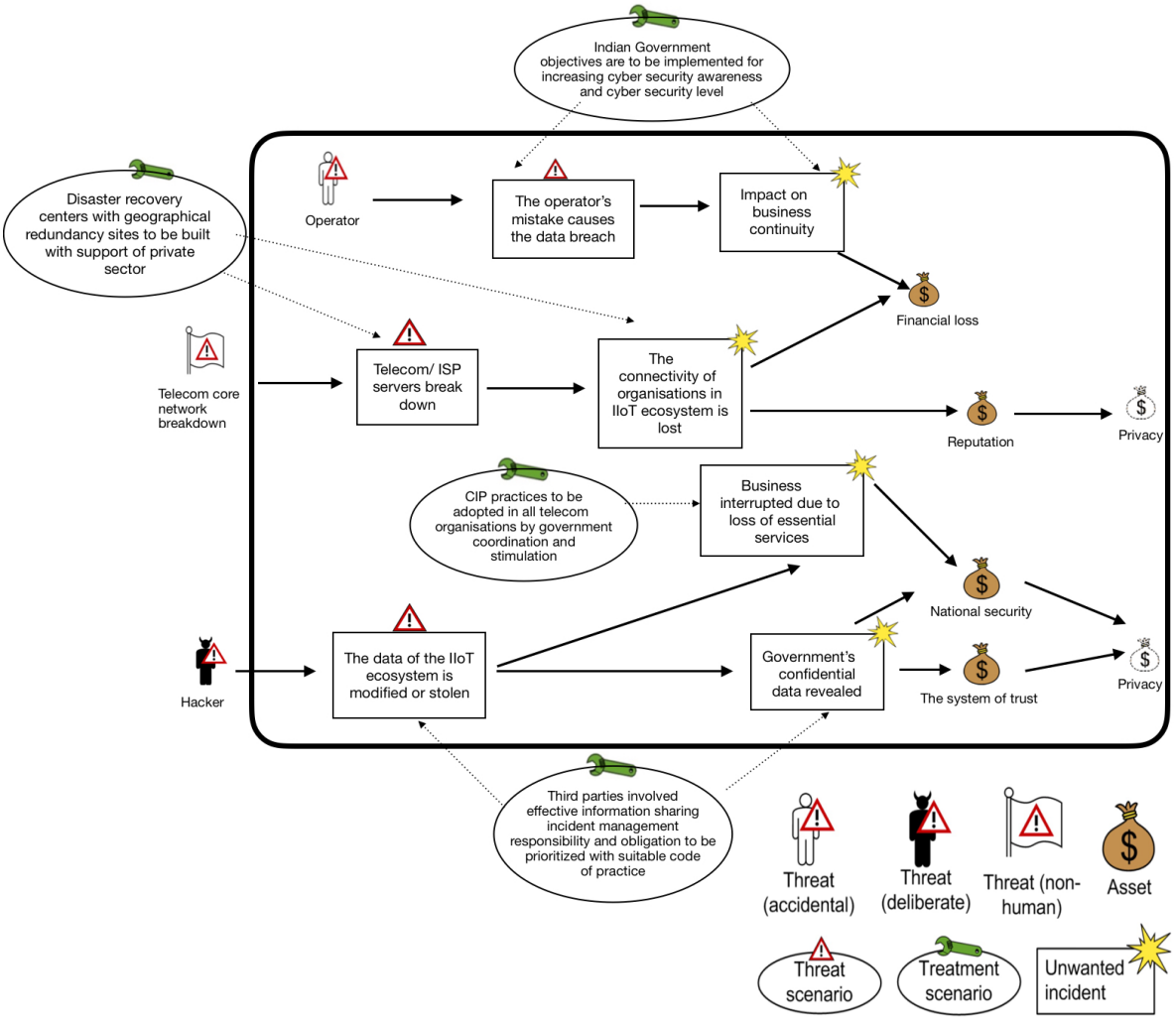

Figure 7 - CORAS Overview on Telecom Network with IoT: Threat, Incident and Treatment Diagram

Incidents considered for analysis in the diagram are: (i) loss of business continuity, (ii) lost network connectivity in IIoT ecosystem due to system breakdown, and (iii) breach to the government's confidential data.

In figure 7, the assets - financial loss, national security, reputation, system of trust and privacy are a product of the depicted incidents caused by the threat actors (hacker and operator) together with an unwanted incident disrupting the core telecommunication networks.

The risk treatment for the above identified incidents can be stated as follows: (i) Redundancy sites and disaster recovery centers should be built to ensure connectivity of IIoT ecosystem at all times. (ii) Indian government objectives should be implemented for cyber security awareness and levels in the organization. (iii) Third parties' involvement and information sharing for incident management obligation is necessary to thwart state/non-state hacking. These risk treatment options require committed PPP cooperation and collaboration to build trust and maintain a resilient and cyber secure IIoT ecosystem. The government should work with the private sector to build capacity and capability to address these risks independently.

The supply chain in the Indian telecom sector mostly relies on PPPs and their 3rd parties. These are outsourced or cloud based technology services due to which the 3rd parties should be made accountable as per policy for protecting the CIs. Therefore, public and private telecommunication agencies contributing to create an IIoT ecosystem should be tasked with raising cyber security awareness and cyber security levels.

From the CORAS analysis above, risk areas in a PPP model are identified as areas of business continuity, risk mitigation, establishing government objectives for a strong security framework in IIoT ecosystem, and building trust and capabilities among the partners.

3.3 Security Focus Areas in Telecom IoT

The Indian IoT ecosystem has its dependencies from both public and private sectors on telecommunications. The improvement points identified by the CORAS risk analysis are extrapolated to the PPP context in the Indian telecom and the four risk areas are derived: (i) objectives of the Indian government (ii) trust and mutual obligation (iii) incident management and (iv) coordination and stimulation by the Indian government. These are evaluated in further detail to identify them as PPP focus areas for the priority attention of the Indian government to achieve their IIoT objectives.

The IoT policy risk identified from the CORAS risk analysis are elaborated combining the views of Indian experts from public and private telecommunications, senior telecom officials and academia through interviews. These interviews provide validation and understanding of the ground implementation status of security and PPP models in the Indian IoT deployment in the Telecom sector.

3.3.1 Indian Government Objectives

India has a policy framework in place to implement its IoT objectives. The New Digital communication policy 2018 provides the necessary policy framework and states that "*it will enforce accountability through appropriate institutional mechanisms to assure citizens of safe and secure digital communications infrastructure and services."*[58] The Personal Data Protection Bill, 2018[59] gives "*the right to informational privacy which meant the use of data as a critical means of communication between persons thus fostering a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation, and to establish a Data Protection Authority for overseeing processing activities."* The Draft IoT policy 2015 gives a vision[60] "*to develop connected, secure and smart IoT based system for our country's economy, society, environment and global needs*." These three policies constitute the Indian regulatory framework to achieve digital transformation objectives.

The Telecom industry follows the national IoT standardization in technology, process, interoperability, services, security and privacy. In a discussion on the PPP model for Indian government objectives on the telecommunications security policy, respondent 4 states that "*the security policy talks about what measures the organization is supposed to take. So, all these entities within the organization would be following these policies. To define the requirements are of a standard*

[58] Express Web Desk. "What Is New National Digital Communications Policy-2018?" The Indian Express, The Indian Express, 26 Sept. 2018, indianexpress.com/article/india/what-is-new-telecom-policy-2018-digital-connectivity-communications-5375761/.
[59] Ministry of Electronics & Information Technology. Personal Data Protection Bill. Government of India, 2018, Personal Data Protection Bill, meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill, 2018.pdf.
[60] Ministry of Electronics & Information Technology. IoT Policy Document. Government of India, 2015, IoT Policy Document, meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.

baseline security policy, a document was worked out by the entities within the government and the public and private sector service providers." In continuation to this, respondent 4 also details about the content of minimum standards security requirement policy document stating, "*when preparing a policy document, we expect that the clauses provided in the document, the minimum requirements should be covered. They can have over and above that. For them to prepare their own security policy, there should be consistency across the industry and it provides a minimum for the security audit."* This clearly indicates that the Indian government is focused on implementing the security policy and the standardization of its data communications by contribution of both public and private sectors, telecom service providers (TSPs) and internet service providers (ISPs).

On further discussion of the role of private sector in contribution to the Indian telecom sector, respondent 3 states that "*the government recognizes that a lot of expertise in the security field exists outside the Government in addition to the expertise it already has. The outside expertise is always leveraged, coming up with solutions and frameworks in securing the network."* Here the government is said to be accepting the expertise of private sector and their third parties to deploy secured IoT in telecom networks and public-sector contribution. Thus, it is essential that the PPP governance policies are revisited to build IoT infrastructure in proposed smart cities and achieve targeted growth of the Indian IoT ecosystem. A complete engagement and partnership with private sector telecom network providers is missing, which is a key attention point for the Indian government to achieve its objective towards the standardization of the IIoT ecosystem.

3.3.2 Trust and Mutual Obligation

Due to multi-stakeholder concepts in telecommunications and national security for India, PPP models are being adopted to achieve cyber security. PPP models are in nebulous arrangements, implying a problematic structure in the context of critical infrastructure protection.[61] Private ownership of the critical infrastructure is also more vulnerable for national security thus encouraging intelligence sharing between private and government agencies as an essential mandate for network securities.[62] Results of the CORAS risk identification threat diagram from figure 7 suggest that national security and the trust element are important assets for deployment of IoT in the Indian telecom sector. In the process of industrial IoT adoption towards achieving the government's goal of smart city projects, private sector partnerships are in progress. Fundamental disjuncture in PPP from perspectives of two partners' i.e. government and private CI operators is a challenge for the government to manage national cyber security due to responsibility and accountability.[63] Accordingly, trust plays a vital role for maintaining business continuity, resulting in higher levels of service and trust between the service provider and the client.[64]

In the Indian context, the IoT policy framework for governance mentions that [65] "*a Program Management Unit (PMU) will be established to provide ongoing support in identification of various initiatives for operationalization of the IoT Policy and ongoing 100 smart cities project.*" This indicates that there could exist some gray areas in the policy objectives and expectations for the IoT initiatives and operationalization. When enquired about the effectiveness of the present IoT policy, respondent 1 states that "*it is the responsibility of private sector to invest and coordinate for industry 4.0 growth.*" This response reflects that the government clearly has high expectations on private sector investments in the Indian IoT growth although there could be ambiguity on expectations and obligations with respect to operationalization. Consequently, enhanced trust between government

[61] Carr, Madeline. "Public–private partnerships in national cyber-security strategies." International Affairs 92.1 (2016): 43-62.
[62] Idem
[63] Idem
[64] Idem
[65] Ministry of Electronics & Information Technology. IoT Policy Document. Government of India, 2015, IoT Policy Document, meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.

and private sector is essential by demonstrating suitable financial instruments that these private telcos are certain on return on investment (ROI).

In reply to a question on the general trust issues of government versus that of private sector, respondent 8 states that "*with the private parties, there is no trust. We have to finish the work. We trust the government because a government means a 100% public focus. We have to contribute from our side also, as if we are a part of government, because we are part of the country. Corporate responsibility from our end.*" On the topic of information sharing experiences, the same executive replied that *"information sharing experience - we don't share emails because it is a company policy. We cannot attach any .EXE files, only we can enter the information in the mail body but we are not giving any attachments. So that way we are securing our information from leakage."* When questioned on the accountability and responsibility of both public and private stakeholders in the PPP governance, an interesting point of view is expressed by respondent 5 "*they are all defined by agreements which are very clear in stating the responsibility matrix and escalation matrix. Contractual agreements are the solution for maintaining the responsibility and you can derive security.*"

In view of the above discourse, it can be inferred that there is no trust deficit from private TSPs to the Indian government in general. But regarding sharing of information for both operational and national security importance it can be argued that private TSPs don't trust each other and follow by regulation and formal contracts. They follow standard operating procedures (SOP) to share organization specific information and treat each other as a security risk to be controlled. Lack of trust among PPPs could result in personal data breaches and cybercrime impacting the end user in an IIoT ecosystem. Considering the above, maintaining the trust factor among PPPs is identified as a key attention area for the Indian government in the telecom policy implementation for IoT adoption.

Generating trust through clarity in IoT policies, transparency and mutual obligation with effective information sharing initiatives is a point of attention among all stakeholders in PPPs with a goal towards creating self-regulating networks.

3.3.3 Incident Management

CERT-In handles incident notification, incident response activities and provides periodical advisories and cyber security alerts for the telecom sector. NITI Aayog has proposed to establish sectorial and regional state government CERTs to operate in conjunction with CERT-In and coordinate with National Critical Information Infrastructure Protection Centre (NCIIPC), designated as the national nodal agency responsible for critical information infrastructure protection for India.

Analysis of cyber incidents from 2013 to 2016 resulted in virus or malware accounting for 17.2% of all the reported incidents.[66] According to PwC global state of information security 2016, IT security incidents in the telecom sector increased by 45% in 2015 compared to 2014.[67] Referring to statement of increased IT security incidents respondent 2 remarked that "*The Indian telecom has legacy systems and non-updated security practices.*" Hence, this determines a clear need for the Indian government to harmonize regulatory compliance and structure incident management. The Indian telecom governance with such incident management practices in a PPP model should build

[66] Kumar, Chethan. "One Cybercrime in India Every 10 Minutes - Times of India ►." The Times of India, Business, 22 July 2017, timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms.
[67] PWC. "Turnaround and Transformation in Cybersecurity: Key Findings from The Global State of Information Security® Survey 2016." PWC, 2016, www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf.

confidence in information sharing and notification which supports incident response process from all stakeholders.

On an inquiry on public and private TSPs/ISPs information sharing practices of cyber incidents, respondent 4 states that "*what information the TSPs and ISPs provide to Government of India is OK, but I see that the ISPs and TSPs are not having all the information because the equipment, the network elements are mostly from international Original Equipment Manufacturers (OEM), they need to know what is the latest software that is required to face the current threats and vulnerabilities in the network.*" Further detailing on the incident notification and incident response in the Indian telecom context, the technocrat defines that "*both proactive and reactive responses are included. Proactive measures mean putting systems and detection mechanisms in place and incident response based on mechanism for responding towards that incident.*" Here the government acknowledges the fact that the policy framework is in place as per the expectation of the TSP/ISPs.

However, due to the fact that many telecom network elements are from international 3rd parties from both public and private sector, any cyber attacks require the OEM expertise to mitigate the cyber incident and reduce the response time. The lack of suitable intrusion detection systems impacts these telecom service providers' incident identification capabilities. The trust factor is also missing due to high penalties levied by regulators on notification of cyber attacks, and this is being considered as a threat to their business models hence the OEMs are expostulating towards proactive incident notifications.

Presently the incident response is fragmented across the government departments due to lack of regional state and sectorial CERTs. Unified approach for incident management renders awareness and understanding in PPPs to contribute to an effective IIoT ecosystem. Clear procedures on incident reporting for effective information sharing among the PPPs is essential but currently missing.

For an effective governance of incident management in a PPP, a balance between IoT security, network security and the telecom ISP's responsibilities to reduce the cyber threat landscape is necessary. Though mandated by policy, the telecom sector CERT is currently not established, and thus the confidence building among PPP stakeholders is not at the desired level. This remains an attention point for the Indian government to establish the right governance and security in cyber incident management in an IIoT ecosystem.

3.3.4 Indian Government Coordination and Stimulation

The Indian telecom private sector initiatives in February 2018 resulted in a partnership with Samsung Inc. for nation-wide deployment of narrow-band IoT network in consumer and enterprise IoT applications. This is confirmed by respondent 1 on the status of digital transformation in India and evolving Indian IoT ecosystem stating *"from the infrastructure perspective, we have some limited narrow-band IoT, the organizations have to build the network from the core network to the reliance network. So, the operators will do their job, and the government also have to give a nudge, because it goes both ways. Great policy and framework, software, hardware and electronics - next 2 to3 years expect a lot of IoT deployment to take place. So, government can really push the ecosystem toward realization."* This confirms that there is expectation on Government of India to promote the private sector and 3rd parties to share their expertise in Cyberspace. It is an attention point for the government to address all disjunctive elements in PPP model and achieve the telecom policy goals by contributing to secure IoT technology deployment.

The Unified Access Service License (UASL) amendment[68] by the Indian regulatory authorities mandates that TSPs are responsible for continuous assessment and risk controls definition to mitigate risks emerging from new technologies. It also expects that TSPs should monitor all intrusions, attacks and frauds and report the same to licensor and to CERT-In. Penalty applicable for non-compliance will create adverse impact for the telecom business environment. To mitigate such impact, the continuous engagement of all stakeholders to ensure that trust and government objectives are met is essential. Coordination with the stakeholders in PPP models will yield price reduction in telecom services for citizens and financial benefits for all TSPs/ISPs.

To take steps towards Indian telecom resilience, identification of the most vulnerable parts to cyber-attacks of IoT ecosystem and early warning mechanisms are crucial. This helps to mitigate the impact on the organizations and act as a preventive framework. CERT-In is a single point of contact (SPOC) for incident reporting and shares advice on vulnerabilities across both public and private sectors. The top down approach of information sharing practices by CERT-In restricts transparency of incidents due to imposing penalties on the TSPs/ISPs who report the incident. In response to a question on the present information sharing practices with CERT-In, respondent 4 states that "*There are some conditions where there is a process up to ~7million USD per cyber security incident which actually dissuades TSPs/ISPs from being in the open about sharing information on incident occurrence.*" This is an attention point that needs to be addressed by the Indian government through coordination and stimulation to have better information sharing.

Challenges in meeting network security regulations in the telecom sector requires effective telecom policy enforcement, regulation, monitoring and periodical security audits. Establishing a security governance framework and collaborating with specialized skilled and experienced professionals ensure robust security controls. Prevention of any possible cyber attack become a challenge and requires the participation of every PPP stakeholder in the telecom ecosystem including third parties. Hence the government should address this attention point by PPP coordination and stimulation through stakeholder networking.

3.4 Sub-Conclusion

The CORAS threat diagram scenarios resulted in identifying the crown jewels such as financial loss, reputation, trust and privacy. These assets can be protected by PPP models. The Indian IoT ecosystem has its dependencies on both public and private sectors on telecommunications, intertwined through critical cyber-physical systems and key administrative systems. Accordingly, the disruption of telecommunications is in itself a cyber threat which impacts national security.

The risk treatment identified by the CORAS risk analysis are extrapolated to the PPP context in the Indian telecom and four attention points are identified: (i) objectives of the Indian government, (ii) trust and mutual obligation, (iii) incident management, and (iv) coordination and stimulation by the Indian government. These were evaluated in further detail to identify them as PPP challenge areas for the priority attention of Indian government to achieve their IIoT objectives.

Through this case study, the following conclusions were derived. The attention points to design PPP policies for enhancing cyber security in the Indian IoT telecom sector are listed below.

- *Indian Government Objective*: There is a huge dependency of the Indian government on public, private and third-party organizations to execute its IoT policy. The public and private sector together with third parties, however, have demanding issues to deploy

[68] Gupta, Atul. "Information Security in Telecom Sector." KMPG, 2011, www.kpmg.de/docs/Information-Security-in-Telecom-Sector.pdf

secure IoT solutions to telecom networks mostly in contribution to building infrastructure in smart cities to achieve growth of Indian IoT ecosystem.

- *Trust and Mutual Obligation*: The overall trust levels of the private sector with the government, its telecom regulatory bodies, and financial framework are adequate for their IoT contribution. However, for sharing of information of both operational and national security importance, it seems that private TSPs don't trust each other and prefer to follow regulations/contractual agreements, which limits the overall cyber incident response and preventive measures. The organization specific information is shared between private parties via standard operating procedure (SOP) with wariness rather than with trust.

- *Incident Management*: The incident response is fragmented across the government departments due to a lack of capacity and required CERTs. Unified guidelines on incident reporting and effective information sharing for stakeholders contributing to enterprise IoT ecosystem are missing. Confidence building measures for all TSPs/ISPs is an attention area and the Indian government's investments are necessary towards creating industry specific sectorial and regional government CERTs.

- *Indian Government Coordination and Stimulation*: Meeting network security regulations and compliance in the telecom sector requires a lot of coordination and stimulation from the Indian government in order to support various public and private organizations. Establishing a security governance framework, identifying areas of vulnerability, early warning mechanisms to improve resilience, and involving third parties as key stakeholders identify coordination and stimulation as a key focus for a holistic view to enhance cybersecurity. A holistic integrated security framework using network governance is an attention point in PPPs when aiming towards the growth of industrial IoT for which the telecom sector is the backbone.

From this case study, four attention points to address security concerns in IIoT domain through the existing PPP policy have been identified. Building networks through network governance approach[69] between public and private sector will add value to the existing practices in the telecom domain. Hence, the problem relevance areas identified as (i) objectives of the Indian government, (ii) trust and mutual obligation, (iii) incident management, and (iv) coordination and stimulation by the Indian government should be refined and reassessed to arrive at requirements for designing significant policy changes to enhance the cyber security in the Indian telecom sector. This can be addressed through the PPP meta-governance design.

[69] Dunn-Cavelty, Myriam, and Manuel Suter. "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." International Journal of Critical Infrastructure Protection 2.4 (2009): 179-187

4. Design and Validation

The method of research, present status of the Indian IIoT ecosystem, and the Indian telecom sector case study discussed in the previous chapters led to the identification of four attention points which are namely: (i) Indian government objectives, (ii) Trust and Mutual obligation, (iii) Incident management, and (iv) Indian government Coordination and stimulation. The results of the telecom case study are extrapolated to the other Indian CIs to evaluate the design requirements for PPP policies to enhance cyber security and arrive at suitable policy recommendations.

We created a framework using the Dunn-Cavelty meta-governance and Hevner's design approach as presented in figure 3. This chapter provides a design of policy recommendations to enhance cyber security for a PPP model with a network approach in the interdependent essential services in industrial IoT ecosystem.

4.1 Relevance of Dunn-Cavelty Model for PPP Meta-Governance

Analysis of the Dunn Cavelty model [70] is performed for measuring suitability of application of the model for PPP meta-governance in the Indian context.

Figure 8 depicts the dependency analysis[71] of serious critical infrastructure disruptions (2005 -2018) in the EU based on 4175 incident reports from public sources. The interdependencies show the cascading effect of these incidents (including cyber-attacks) on the Critical Infrastructure (CI) of essential services generating a much larger impact on societies. These essential services are often maintained by multiple vendors, both public and private players.

[70] Dunn-Cavelty, Myriam, and Manuel Suter. "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." International Journal of Critical Infrastructure Protection 2.4 (2009): 179-187

[71] Luiijf, Eric. Personal Interview. 24 November 2018. Unpublished.

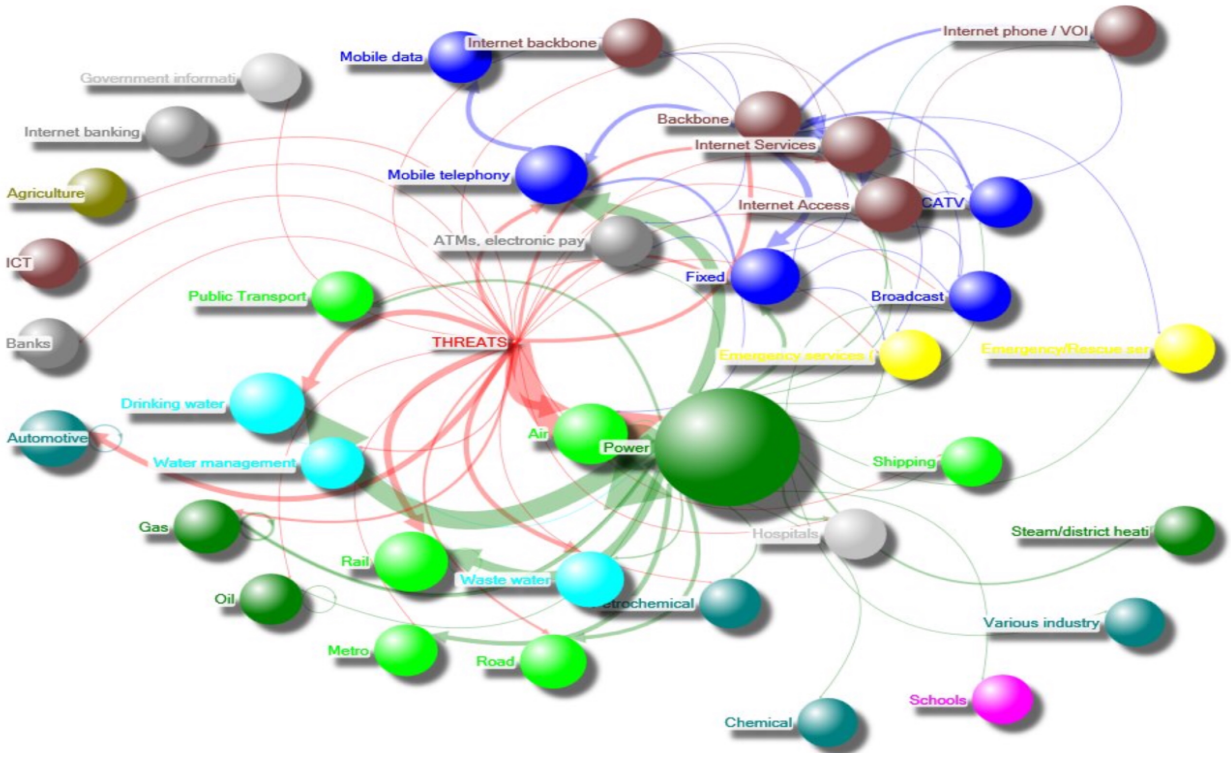

Figure 8. Dependency analysis of serious critical infrastructure disruptions (2005 -2018) in the EU based on 4175 incident reports from public sources[72] [30]

In figure 8, the essential services are denoted by the spheres (larger the sphere, larger the threat to citizens) and the interdependencies of the essential services are connected by arrows. Thus, a threat originating in one area is shown to cause domino impact on multiple other services and the thickness of the arrow denotes the quantum of impact level to the citizens and nation. As an example, a threat on the power sector is simultaneously impacting the internet, mobile services, water management, and drinking water; in turn, these services are impacting the transport and other services.

Supported by the above information, continuous assessment of CIs and their business continuity is essential to refine, reassess and to identify significant policy requirements to enhance the cyber security. Similar assessment is applicable to PPPs of Indian IIoT ecosystem. Thus, a PPP model with a network of networks should be coordinated and stimulated by the government among all stakeholders. This helps the self-regulation of the organizations through meta-governance process to enhance the cybersecurity of CI in the Industrial IoT ecosystem.

Dunn-Cavelty suggests meta-governance as a process framework that allows for self-organizing networks of public and private institutions to help the governments achieve their public tasks. Cyber security of CI physical systems is one such task that requires meta-governance. The preferred way of self-regulation of networks should be through a "*shadow of the hierarchy*" to ensure all networked actors are in line with central and state institutions abiding by law.[73] The framework of meta-governance is to (i) activate networks, (ii) facilitate co-ordination, and (iii) promote required activities and harmonize them to achieve the defined public tasks. Governments should encourage public tasks met by PPP networks and decisions should be made with negotiations rather than with authority. Hence a governance is required to solve cyber issues with demand uncertainty and task

[72] Luiijf, Eric. Personal Interview. 24 November 2018. Unpublished.
[73] Dunn-Cavelty, Myriam, and Manuel Suter. "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." International Journal of Critical Infrastructure Protection 2.4 (2009): 179-187

complexity.[74] Apparently network governance is a dynamic process of constantly organizing the PPP networks.

Based on the above arguments, it is justified and relevant to follow the Dunn-Cavelty meta-governance process steps for PPPs. This is applicable to achieve our research goal "Which PPP policies are required for enhancing cyber security in Indian Industrial IoT?"

4.2 Process Steps for Developing PPP Meta-Governance

Dunn-Cavelty describes the design steps to achieve the desired PPP policy instruments as part of the meta-governance process for enhancing the cyber security in Industrial IoT. The three process steps are: (i) Indian IoT policy goals, (ii) PPP status quo and policy implementation gaps, and (iii) Policy instruments for closing the gaps through self-regulation. The fourth step of the Dunn-Cavelty design is not covered in this thesis which is the measurement of efficiency of selected governance instruments w.r.t. the policy goals. This can be only done by the Indian government after implementation of the recommended policies.

Of the attention points derived from the case study, the "Indian government IoT policy goals for PPP" will be covered in the immediate subsection below as this is the first step of Dunn Cavelty meta-governance. The attention points, "Trust and Mutual obligations", "Incident management", and "Indian government coordination and stimulation" along with "Indian government IoT policy goals for PPP" will be discussed as the second process step of the Dunn-Cavelty meta-governance to identify the requirements (Gap analysis summary). This is followed by the design which is the 3rd process step of the Dunn-Cavelty meta-governance to arrive at answering the research goal.

4.2.1 Indian Government IoT Policy Goals for PPP

This sub-section explains the Indian draft IoT policy 2015 which has been published to the IoT industry and all stakeholders with the vision on the objectives of the central government, technology standards, economic investment and growth perspectives as part of the first process step of the meta governance.

4.2.1.1 Government IoT Objectives

The Policy approach in building the Indian IoT ecosystem is a PPP with a multi pillar approach to overcome resource management problems. Initiatives on Cyber security in the Indian industrial IoT has started to deal with present and future requirements. For this, an initial framework with formal and informal institutions is in place.

The Draft IoT policy 2015 governance structure with PPP model aims "*to set up a high level Advisory Committee (AC) including representatives from the government, industry and academia for providing ongoing guidance in the emerging area of IoT*".[75] The policy is to foster IoT initiatives by the Indian government and to cross connect public and private sectors for unified synergies in delivering health, education and financial services to geographical isolated regions for e-governance through a PPP model. The unified synergies accelerate the innovations, capacity building and awareness as a priority to foster cyber security in the IIoT ecosystem. To create security expertise for

[74] Dunn-Cavelty, Myriam, and Manuel Suter. "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." International Journal of Critical Infrastructure Protection 2.4 (2009): 179-187

[75] Ministry of Electronics & Information Technology. IoT Policy Document. Government of India, 2015, IoT Policy Document, meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.

preventing possible cyber threats, set-up of incubation centers for capacity building requires the alignment of private sector investment and sharing.

4.2.1.2 Objectives for IoT Standardization

India is setting the standards as part of its five-pillar approach to facilitate the IoT industry and research bodies on the technology front. Consequently, the interoperability, compatibility, reliability, and security in the heterogeneous environment is maintained with international cyber security levels thus boosting innovation. An expert committee comprising of government with industry experts and academia is steering the PPP model for development of standards to support business organizations. This unleashes the commercialization of industrial IoT ecosystem with integration of sensory devices and early adaptation of standards relating to processes with interoperability.

Indian government is focusing on reducing the nation's dependency on import of IoT components and is promoting "Make in India" concepts so that IoT startups can consume 60% of the Indian IoT ecosystem. These activities are being proactively steered by ERNET through the Centre of Excellence for Internet of Things(CoE-IoT) and NASSCOM in PPP mode through seed funding by the Government of India.

Standard procurement policy encourages the Indian domestic companies to have a larger market. Realizing the low standards of in-house vendors, the procurement from international 3rd party expertise is still maintained to encourage and ensure the accelerated growth through PPP models in the Indian IIoT security.

Regarding a discussion on setting the standards for enhancing the present cyber security, a senior telecom policy adviser, respondent 4 states that "*a committee is constituted of representatives from the industry, the technical experts a security experts from public and private sectors' ISP operators. They send representatives and we have representatives from CERT-In and National Critical Information Infrastructure Protection Centre (NCIIPC) and this committee came up with a minimum standard baseline for what should be part of the security policy*." CERT-In is setting the baseline standards after elaborate discussions with all stakeholders in a PPP mode to achieve a coherent approach for the security standards and supporting policies.

In the IoT policy, standards are central to all approaches to harness the IIoT ecosystem. These standards give norms, objectives, and the lens to enhance cyber security. The standards-setting and the processes are derived in PPP mode through consultations from both state and non-state actors who are part of cyber security hierarchy framework. These standards are set to ensure responsibility and accountability from all stakeholders of IoT ecosystem as part of regulatory standard setting.

4.2.1.3 IoT Economic Growth Objectives

The Indian government road map for 2020 as per its draft IoT policy is to create an IoT industry with 2.7 billion connected devices leading to an IoT industry of $ 15 billion.[76] The huge transformation is projected to be achieved with PPPs accelerated participation to the growth of the IoT industry at CAGR >28% during 2016-2022.[77] The National Digital Communications Policy 2018 provides extensive stimulus to the IoT program in the machine – to – machine (M2M) space. This is thought to be achieved by encouraging a $100 billion foreign direct investment in the

[76] Ministry of Electronics & Information Technology. IoT Policy Document. Government of India, 2015, IoT Policy Document, meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.
[77] ETCIO. "India IoT Market to Grow over 28 Pc CAGR during 2016-22: Study - ET CIO." ETCIO.com, 8 Dec. 2016, cio.economictimes.indiatimes.com/news/internet-of-things/india-iot-market-to-grow-over-28-pc-cagr-during-2016-22-study/55874529.

communication sector, mostly for the advancement of industrial IoT in India's digital transformation.

The draft IoT policy acknowledges that the Indian government has allocated an amount of ~ $ 1 billion for developing 100 smart cities to proliferate IoT adoption in the country.[78] Budget of ~ $ 58 Million[79] has been allocated to develop demonstration centers for IIoT, capacity building resource centers and test beds, Center of Excellence (CoE) and for creation of young faculty chairs in academic institutions to nurture seed funding. Government expects that the residual funding would be procured by industry private players via NASSCOM or any other designated industry association. No specific incentives are proposed for the IoT sector, while the general approach of "Make in India" import tax holidays are applicable for new IoT startups.

4.2.2 PPP Status Quo and Policy Implementation Gaps

This subsection explains the implementation status of (i) Indian government IoT policy goals, (ii) trust and mutual obligation, (iii) incident management, and (iv) Indian government coordination and stimulation, in the PPP. The gap between the policy objectives and the field implementation practices is also identified. The implementation status quo provides an analysis of gaps to be bridged. This gap analysis summary gives the requirements for our design to arrive at suitable policy recommendations to enhance cyber security in the IIoT ecosystem through PPP meta-governance.

4.2.2.1 Indian Government IoT Policy Goals-Status Quo

The IoT policy has an objective to create awareness in IoT and developing skill sets for IoT at all levels. "*Poor communication between the technical and policy communities has been identified as one of the key impediments to informed policy decision making. This is not due to a lack of willingness but rather a lack of shared objectives between diverse actors.*"[80]

Low budget allocation from government is observed for capacity building of infrastructure and skills, forcing the investment by the private sector. Hence, shortage of internal expertise causes slow adoption rate of IoT technology in CIs. Due to lack of cyber security professionals in the market, capacity building of internal security professionals is a top priority towards achieving cyber security goals.

Private sector is also restricting its engagement activities from their budget provisions due to other priorities in their business models rather than focusing on cyber security. Corroborating this observation respondent 3 states that, "Basically *nowadays capability building is required a lot more, there are employers that are working on this but is not sufficient as of current date. So that is a reason nowadays employers are depending on people with multiple roles. One person is dealing with the actual core of the organisation but he's is also given a responsibility of taking care of the security of certain applications. Because security is so essential, capability building is very much required. It is very important and we are also bringing awareness to the employees in terms of preventive actions whenever we go for auditing.*" This identifies skill development as an area of focus for building scale and internal expertise. On the infrastructure front, the policy does not mention the scale of skill gap required to achieve the policy goals so the government should identify the prospect skilled manpower size to be developed across public and private organizations for the cybersecurity needs in the country.

[78] Ministry of Electronics & Information Technology. IoT Policy Document. Government of India, 2015, IoT Policy Document, meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.
[79] Idem
[80] Carr, Madeline. "PETRAS." EPSRC IOT Research Hub, www.petrashub.org/iot-governance-policy-cooperation-cyber-security/.

IoT technologies are dependent on 5G data connectivity to contribute to high positive impact in the industrial sector. "*The 5G standardization is still in progress in India and it may not be commercialized till 2020*" as per respondent 1, which is a huge impediment to the pace of growth projected in IIoT.

Standardization and harmonization is mandated for truly ubiquitous IoT. The standardization activities are focused in creating a security posture for the Indian IoT ecosystem to attract international investors. Respondent 4 shares his experiences of the regulatory objectives on the standardization of security policy in critical infrastructure by stating "*yes, the security policy talks about the measures all the organizations are supposed to take. So, the entities within the organization would be following these institutional policies. What are the requirements of a standard baseline security policy? - a document was worked out by the entities within the government together with the public and private sector service providers. And it was an elaborate exercise that took us almost a year to finish.*" The first standard baseline security with consultative approach for IoT connectivity is available, however this may not be sufficient for cyber intrusion detection mechanisms for IIoT ecosystem.

With reference to IIoT standards, in order to address the cyber incident management for incident prevention and response, it is essential to have a holistic approach with integrated IT and OT security. The IoT policy does not currently have equal emphasis on both IT and OT security in PPPs, thus the employee / operators are unable to transition from a state of 'cyber ignorance' to 'cyber awareness' in the IIoT domain. OT is more critical since it involves shutdown of CI for protection in case of cyber-attack. Restoration after cyber incident correction and reconciliation of missing data from shutdown period into the OT infrastructure also requires high attention. IoT policy should take necessary measures to address OT restoration standards for IoT ecosystem after cyber incidents in industrial usage. Policies on integration of the IT and OT security guidelines is a requirement from the government to ensure a holistic view to defend from cyber-attacks in the Indian IIoT ecosystem.

Indian government objective is to encourage startups to comply with the regulations, so that the contribution of startups reduces the import dependency of IoT products and services to Indian industries. It is observed that the Indian industrial IoT startups have received ~ $65 million investment from international investors which is very low.[81] Reduced investments towards industrial IoT startups is not aligned to Indian IoT policy objectives. This is hampering startups goal to achieve international standards contributing to failure to reinforce competitiveness among peers. The government should foster entrepreneurship towards IoT innovation for long term economic benefits and improvements in productivity and competitiveness. Low IT budget allocation and seed funding by government to create the infrastructure for startups are to be addressed.

The IoT policy aims growth of the IoT industry to $15 billion from the present $130 million annual revenues.[82] Most of the implementation of the IoT policy is dependent on private sector or FDI route. The budgetary impetus given in the industrial IoT by the government of India is limited in PPP mode and it is not visible. Bilateral Trade Engagements on initiatives by the Indian Union Minister for Electronics and Information Technology and in-depth meetings with private sector players and business leaders gathered some momentum on making international investments. Recently, Juniper networks, collaborated with the government of India towards digitization with an investment of USD 900 million for digital infrastructure installations.[83] Confirming such moves and future FDI proposals from the Netherlands as part of PPP, respondent 9 states that "*yes, in cyber security, at the moment we are trying to position these Dutch companies on the Indian market. So,*

[81] Press Trust of India. "Bluru Prime Destination for IoT Startups in India, Study ." India Today, India Today, 24 May 2017, www.indiatoday.in/pti-feed/story/bluru-prime-destination-for-iot-startups-in-india-study-931731-2017-05-24.
[82] Exhibitions India Group. "3rd Internet of Things India Expo 2019." IoT India, 2019, www.iotindiaexpo.com/iot-india-expo.aspx.
[83] ETTelecom. "Juniper Networks to Invest Rs 6,700 Crore in India to Back Digital Drive - ET Telecom." ETTelecom, 8 Dec. 2016, telecom.economictimes.indiatimes.com/news/juniper-networks-to-invest-rs-6700-crore-in-india-to-back-digital-drive/55882988?redirect=1.

this is step one. So hopefully this will lead to investments and returns etc. But at the moment we are quite in an early phase, working on it for about 3 to 5 years already, and now this program is signed and they can actually get to work. Now we are trying to spot the opportunities and get the businesses involved." Thus, the Dutch government is encouraging its private sector investments to explore business opportunities through cyber security expertise in the Indian markets.

As per the global competitive index 4.0 ranking data report 2018[84] India has been ranked 117 for the ICT adoption rate, ranked 118 for time to start a business and ranked 100 at administrative requirements for ease of business. A combination of all these parameters may affect the FDI participation in Indian IoT growth trends. The growth of IoT adoption may be impacted by the fact that there has been a 10% shortfall in FDI investment in 2017 from the previous year which is 4B USD as per the UN latest report.[85]

The IoT market in India currently stands at $130 million annually in revenues with more than 400 companies contributing to some form of IoT related services.[86] Low IT budget allocation on digitization from government conflicts with its intentions to motivate private sector investment in harnessing the IoT ecosystem. Moreover investors (international, private, and 3rd parties) need confidence in the Indian economy to motivate them to trust the Indian economic situation. The global competitive index 4.0 2018[87] states that India ranks 117 in ICT adoption which is not encouraging. Though 3rd parties are vulnerable to contribute to security risk, they also expect the judicial solution to solve any issues in their cyber security business partnerships. In the EU context, there is EU Joint Cybercrime Action Taskforce (J-CAT),[88] but such a judicial system is missing in the Indian context. Hence something similar will contribute to confidence building measures for international 3rd parties to contribute their cyber security expertise and investments to the Indian IIoT ecosystem. All Indian organizations when working with international partnerships (as per EU GDPR implementation) are mandated to comply on privacy, security and processing data which may create liabilities in the IIoT ecosystem. Proper judicial framework and insurance policies are not explicitly mentioned in the IoT policy for judicial solutions.

Overall draft IoT policy 2015, aims at creating an IoT ecosystem with PPP model but it is observed as a neo-liberal approach by Indian government in implementing the policy without clarity on shared goals. It still remains ambiguous how the unified contribution of multi stakeholders can achieve synergies for the holistic cyber security of the industrial IoT ecosystem.

4.2.2.2 Trust and Mutual Obligation-Status Quo

The draft IoT policy mandates PPP models for CIs, in transforming into digitized society. As discussed in the case study, instilling trust in PPPs is an attention point to stimulate smart, unambiguous policy making for cyber governance. Due to the fact that PPP models are nebulous arrangements, implying a problematic structure in critical infrastructure protection.[89] In a top down IoT policy implementation in PPP mode, it is a challenge for the government to assess tensions and maintain national cyber security posture due to expectations of overall responsibility and accountability without having the trust from supporting public-private parties.

In the case study discussed in chapter 3, section 3.3.2 indicates that there is no trust deficit from private TSP/ISPs towards Indian government. But regarding sharing of information on cyber incidents, it is observed that private telco's don't trust each other and also are more protective

[84] Schwab, Klaus, ed. "The Global Competitiveness Report 2018-2019." World Economic Forum, 2018.
[85] UNCTAD. "Investment and New Industrial Policies: The Way Forward." World Investment Report 2018 United Nations Conference on Trade and Development (UNCTAD) World Investment Report (WIR), 2018, pp. 165–178., doi:10.18356/9c309851-en.
[86] Exhibitions India Group. "3rd Internet of Things India Expo 2019." IoT India, 2019, www.iotindiaexpo.com/iot-india-expo.aspx.
[87] Schwab, Klaus, ed. "The Global Competitiveness Report 2018-2019." World Economic Forum, 2018.
[88] Europol. "Joint Cybercrime Action Taskforce (J-CAT)." Europol, 13 Sept. 2018, www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce.
[89] Carr, Madeline. "Public–private partnerships in national cyber-security strategies." International Affairs 92.1 (2016): 43-62.

with state government law enforcement agencies. Reinforcing the trust element with mutual obligation among partners in PPP is the responsibility of all stakeholders. Respondent 7 argues that trust is a mutual obligation from all partners and it is established over a period of time, stating that "*we don't share any information with trust, we first look at the authority, his powers and whether he is authorized to ask such information or not and thereafter the trust comes. Trust doesn't come over a short time. Working with a person or authority over a period of time then only trust builds. At times, local law enforcements authorities in India go over their limits then we have to be firm in our stand and insist them to go as per the SOPs and the law*". Trust element is a fundamental disjuncture in PPP from perspectives of both government and private CI operators in Indian IIoT. Hence, it is a mandatory requirement in the IoT policy and its implementation for an efficient cyber security ecosystem in Indian IIoT. Transparency in policy guidelines needs to be implemented to enhance the trust levels in the ecosystem.

Indian government expects investment and expertise through the PPP model to secure its IoT ecosystem in its draft IoT policy. It is acknowledged by respondent 4 that, "Licensor *(Indian Government) has instituted oversight mechanism in terms of the security audits for which the framework/template for audit has been prepared in consultation with the industry. The security of the network is a responsibility to operator. They are supposed to have a security policy. All operators are mandated to prevent cyber incidents, and responsible to CERT-In for incident notification.*" This indicates a strict accountability in a hierarchical approach and does not focus on achieving the mutual obligations of all the partners. More transparency and collaborative efforts is needed from both sides with information sharing to build the trust. Reiterating the dependency of trust on the PPP transparency and cooperation from government, respondent 9 in the Indian context states that "*The cooperation with government is good on both sides, we set up a mechanism where we can easily discuss these topics, so from that perspective the trust works in PPP*", clearly emphasizing that effective cyber security in the IIoT ecosystem requires more trust.

Policy areas should be identified to address trust deficit and resulting requirements to recommend policy making processes for government and regulatory bodies to promote cyber security in India industrial IoT.

4.2.2.3 Incident Management-Status Quo

CERT-In is the only single point of contact (SPOC), which is responsible for (i) incident response, (ii) security alert notification, (iii) information sharing, (iv) promoting effective security incident operational cooperation, and (v) security awareness campaigns for all regional states and citizens. CERT-In is expected to give guidance and enforcement of security standards and practices across India. CERT-In is leading two new working groups across APCERT, namely the IoT Security and the Secure Digital Payments to derive required standards. Cyber forensics is also recognized as an additional support area of CERT-In. For the defense and power sectors, separate CERTS are functional, but sectorial CERTs are yet to come up though they were to be implemented as part of cyber security strategy 2013.[90]

Moreover, as per annual report 2017[91] of CERT-In, the functions of Institutions like CSIRTS, ISACS, and SOCs are also embedded in CERT-In with only a limited technical staff of 70 for pan India. Talent gap is a bottleneck in CERT-In for timely cyber incident response, support system, incident prevention mechanism and best practices leverage across India for all sectors and regional states. Individual regional state CERTs are not yet established pan India, and this becomes an

[90] NCIIP: MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY. "National Cyber Security Policy, 2013." National Cyber Security Policy, 2013, 2013.
[91] Annual Report (2017) Indian Computer Emergency Response Team (CERT-In) Ministry of Electronics & Information Technology Government of India 9th April, 2018

impediment for holistic cyber security posture. PPP networks can bring in expertise and required infrastructure for early commissioning of state and sectorial CERTs.

Though a penalty of ~$7 million[92] is being imposed to enforce timely incident notification to motivate CIs, it is noticed that till date no penalty is levied on any of the organizations. On a discussion on cyber incident notification practices of both public and private sector, the respondent 3 states that "*We report incidents to CERT-In whenever organisations under our jurisdiction report. At times, it is also observed that some incidents are not reported by organisations due to penalties concern. So, basically incidents travelling from us to CERT-In do not happen at various levels and when it happens all the communications are going through fraction of seconds through emails and CERT-In also informs to us immediately. Maximum we have seen that CERT-In responses are immediate but the time they take for releasing the advisories are being delayed.*" As per the above statement, it can be interpreted that lack of skilled manpower is preventing the enforcement of penalties and cyber incident response follow-up activities. The non-compliance of organizations in addition to zero penalties levied emphasizes the need for in-house capacity building on priority to regulate these activities with the required talent.

On the initiatives taken by regional government of India for establishing cyber security cluster in the state of Telangana, in specific to HSD PIB, respondent 4 states that "*one thing is you do not compare India with any other country. In India, each state is equivalent to a country. Cyber now formulates all aspects of life, the number of infrastructure requirements in cyber space is humungous. So, we can't have one institutional mechanism for whole country and expect that to manage the whole show. So, individual organizations/states should develop their own expertise and institution for protecting their infrastructure.*" The above response substantiates the argument of enhancing the capacity building to establish sectorial and state CERTs in India. This is further emphasized by the fact that all the regional states have large number of SMEs which have low digital resilience and are prone to digital threats. This mandates for sectorial and state CERTs to be implemented for efficient cyber incident management.

In the Indian incident management context, due to low availability of skilled manpower in CERT-In, the susceptibility to cyber vulnerabilities is not being addressed timely and efficiently. Alerts from unified sources such as CERT-In on cyber security threat intelligence, cyber forensic and information assurance is essential to overcome cyber security threats. Collaboration is required among various IIoT stakeholders for efficient cyber incident management.

Without real time vulnerability and response information reciprocity, CERT-In as a single point of contact (SPOC) cannot serve the needs of IIoT ecosystem for early mitigation process as expected by the organizations during incident response. This may raise dependency and support from international ISACs, especially during network intrusions and cyber-attacks.

The top down approach of the cyber security strategy in incident management is limiting the scope of information exchange. With interdependencies in the IIoT ecosystem, the present form of centralised CERT-In information sharing is an impediment to all stakeholders that require more collaboration.

4.2.2.4 Indian Government Coordination and Stimulation-Status Quo

'Digital India' initiative is ambitious to improve online infrastructure by enhancing Internet connectivity. Indian Government is supported by international standardization bodies like ICANN that carried out the cryptographic key changes in October 2018 to protect DNS to counter

[92] Kharbanda, Vipul. "Incident Response Requirements in Indian Law." The Centre for Internet and Society, 28 Dec. 2016, cis-india.org/internet-governance/blog/incident-response-requirements-in-indian-law.

rising incidents of cyber attacks and improve network security of Indian TSPs/ISPs. New social and economic development is driven by market demand for wireless services to connect massive number of IoT devices enabled through the evolution of 5G.

The policy implementation for IoT deployment is executed by both public and private sector organisations. Policy objectives are not met due to implementation in a neo-liberal approach. Creating new PPP networks by orchestrating and modulating the existing PPP models should be the role of Indian government. Hence, holistic cyber security governance is the need to achieve cyber security in IIoT ecosystem. Respondent 4 on the status of holistic approach to achieve cyber security states "*We encourage self-regulating, especially because the cyber infrastructure coming into the organization is huge. And that has to be managed. So, maintenance of cyber hygiene in each organization is important. Understand on central level broad threat intelligence mechanism should be there but I think at the state level the expertise for maintaining cyber hygiene in each independent organization has to be achieved.*" This indicates that different public and private parties in the industrial IoT ecosystem are trying for self-regulation at organizational level but an integrated approach at sectorial, regional states and national level is yet to be accomplished.

Further in continuation on the responsibility and accountability within public and private partnership for pan India, respondent 4 mentions "*I think that the individual organization has to take responsibility for the infrastructure they have and they should be accountable for their own infrastructure.*" This gives focus on regulatory objectives of internal cyber security expertise to prevent cyber attacks. Respondent 5 is of the opinion that "*I feel that the expertise is much more available in the private sector. But when it comes to the actual hands on work and implementing the IT security solutions, then PPP is a must. Even private sector alone cannot do. Anything requires a policy and that policy is determined especially in IT field fundamentally by the nation's security which the government knows better than anybody else. So, the IT security policy of a nation must be determined by a nations security policies. Then it comes fundamentally from the government, top down, and for the implementation of it, every organization has to go for its own security policy.*" This can be considered as acknowledgement that the Indian government should encourage networks as part of meta-governance process by stimulating and coordinating with all PPP stakeholders to address cyber security requirements in IIoT adoption to extract synergies from PPP models being implemented rather than a neo-liberal governance approach.

Due to no explicit mentioning of information sharing in the draft IoT policy or in the digital communications policy no synergy is derived through exchange of cyber incident management practices until the policies are refined further. On a discussion using information sharing for protecting the organizations assets, respondent 8 states that "*We do share information as per regulators perimeter, for our organization redundancy method is there at equipment level, location level. Secondly our organization has our own standards. With our internal standards, we are establishing the connectivity with other operators*." IoT domain being a system of systems in a connected world, silos of protectionism cannot work for business continuity. Hence risk of fragmentation among public and private organizations in adopting IoT security may occur. This leads to coordination failure during cyber incident response due to unilateral standards and processes which needs to be addressed by Indian government.

The IIoT domain needs the cyber threat information sharing in real time, to have a secure environment and reduce the possible impact and its domino effect. Early warning mechanisms with information sharing requirements are to be in place for trusted PPP models. Impairment of IPV6 implementation creates uncertainty on Indian standards and generates information asymmetries which may lead to trust deficiency. Delayed standards implementation may restrain international investors and non-state actors' risk-taking abilities. Hence, network

standardization and security requires larger focus on participation of private sector and their 3rd parties in Indian IIoT.

From the results of the interviews with domain/policy experts of public and private sector TSPs and ISPs, and the available regulatory framework, it is recognized that there is a need to derive synergies leading to a secure IoT ecosystem. This is possible through coordination and stimulation of existing PPP networks and adding new networks in to the IIoT partnerships with an integrated cyber security framework. Strong engagement practices are required by government of India to make this happen.

Coordination and stimulation is the immediate requirement to be addressed by the government by making its intentions clear to all PPP stakeholders to achieve highest efficiency and institutional processes to achieve common objectives in industrial IoT implementation.

4.2.3 Gap Analysis – A Summary

Based on the analysis in the above sections of this chapter, it is observed that there are four striking areas that are prominent gaps in the efficient realization of the Indian IIoT. It is observed that the various gaps identified from the Indian policy implementation status quo fall under 4 major categories, which are listed here. For example, 'Talent Gaps' is identified as a requirement for multiple risk mitigation scenarios- to handle capacity for IoT growth, to build talent for CERT-In functions in incident management and also talent building for IoT policy implementation in startups. So, talent gap has been identified as a key gap. Similarly, aggregation has been done to arrive at the other 3 categories of gaps. These categories are further taken forward in the next section to identify actions and actors to bridge the gaps for enhancement in cyber security with suitable policy formulation.

Listed below are elaborations of the shortage of required talent, inadequate IoT standards and infrastructure, absence of right policy implementation and legal frameworks, and insufficient trust and collaboration.

Talent Gap:

1. Lack of Indian industry IoT adoption due to unskilled employees in the existing private and public organizations
2. Lack of skilled security professionals in the market for the capacity building of existing CERT-In is contributing to its inefficiency, and inability to create new state and sectorial CERTs
3. Identify the gap in manpower across public and private organizations for cybersecurity needs in the country

IoT Standards and Infrastructure Gap:

1. Only baseline security policies existing but not sufficient to handle cyber intrusion attacks
2. Integration of IT and OT security policies are not available
3. 5G standardization across the country is delayed impacting development of IoT
4. IPV6 protocol is partially penetrated in the industrial domain causing a hindrance to real time information sharing impacting IoT growth

Policy Implementation and Legal Framework Gaps:

1. Sufficient budget allocation for information security as per IoT policy mandates is not implemented to deliver projected growth rate, this impacts capacity building of infrastructure, skills and people

2. Fostering entrepreneurship for IoT startups and incubation centers not at desired level due to lack of incentives or tax holidays
3. Policies for enabling FDI of USD 100 Billion required for impetus to Indian IoT ecosystem
4. Legal framework not available for a secure IIoT domain, no law to check cyber-crime
5. Unified cyber incident management approach by all state governments in line with central governments is required
6. Compliance to GDPR enforcement on all international partnerships may increase the liability and obligation for Indian organizations

Gaps in Trust and Collaboration:

1. Collaboration between central and state government/non-government institutions through network approach is missing
2. Non-transparent and ambiguous policy guidelines to be addressed
3. Information sharing and early warning mechanisms through public and private participation is required
4. Synergy on exchange of incident management practices is insufficient

4.2.4 Closing the Gap: Self-regulating PPP networks

Based on the gap analysis identified in the previous section, requirements for our design are achieved to bridge the identified gaps in the areas of talent development, policy implementation and legal frameworks, IoT standards and infrastructure and Trust and collaboration in effective PPP models for IIoT domain to derive our research goal.

4.2.4.1 Closing the Talent Gap

There is a dearth of talent gap of existing employees /operators with information security skills in the CIs to adopt IoT technologies. In the Indian government, there are 98 ministries and each ministry constitutes of ~100 departments. As an estimation, every department needs a minimum of 4 security specialists to perform regulatory functions of oversight. In this scenario, shortage of skills for such cyber security professionals should be addressed by the Government of India through delegation of the task to Human Resource Development (HRD) ministry, academia and autonomous PPP educational organizations.

The IoT technologies are replacing the legacy systems in CIs, where the IT and OT skillsets are not the same. Treating both the technologies as similar patterns from security activity and prevention point of view will not yield a secure IIoT ecosystem. Many activities can be planned to address the talent and experience gap in adoption of Indian IIoT.

Talent gap is prevalent in 2 areas: (i) security skills in-house and (ii) expertise from the market. This can be addressed through the Indian government initiatives by collaborating with skill developers about industry need: (i) help academia build a talent pipeline that meets skill demand, (ii) offer internship programs to gain industry experience, (iii) send in-house people to cyber security training courses in areas of interest, and (iv) retention of in-house experts apart from nurturing existing talent.

CERT-In drives critical jobs by the software specialists with proactive steps to bring together the organizations and citizens with vulnerability awareness, incident management and national security operation center activities. Respondent 3 expresses that the analysis of incidents reported, are being delayed to give advisories to the organizations. Such delays are mainly caused due to shortage of skilled security professionals who can execute the job. Moreover, non-availability of security professionals and insufficient government budget allocation are also a bottleneck to establish regional state CERTs and sectorial CERTs. These organizations will play a vital role for

contribution to the security posture of cyber security. The IoT policy documents and the cyber security strategies do not mention how the existing gap can be bridged. For suggestions on how policies can improve national cyber security, respondent 5 suggested that *"IT and Telecommunications are getting merged, and you have IP protocol network, and India is adopting IoT, not yet fully blown up but just entering, there I think more security awareness is needed and of course skills for implementation."*

The problem of skills shortage problem should be solved by investing in Institutional skill development adopted through PPP models. A long-term cybersecurity capacity building plan to develop talent, bring awareness in organizations to become 100% compliant and self-regulating on security aspects will go a long way to equipping the country. Sufficient funding by the government to the PPP skill development institutions is necessary to build skilled manpower.

4.2.4.2 Closing IoT Standards and Infrastructure Gap

The IoT ecosystem constitutes a wide range of products, services and architectures. Therefore, the process of IoT adoption by existing CIs is a gradual system integration process. The security integration of both IT and OT domains are to be treated as separate requirements with different approaches and skill sets and not stacked everything over IT, due to the different operational and security requirements.

Industrial IoT requires real-time and low latency link for which 5G can play a role in security aspects. Presently it is yet to be commercialized for which standardization by Indian government is to be accelerated. Some of the key performance indicators for IIoT ecosystem which are important for real time data flow are integrity, latency, availability and connectivity. Network transmission delays that are being caused by the attack on IoT devices are difficult to defend when the attacker manipulates the system and smartly mirrors the expected process flow to a large extent. This is further elaborated by a scenario quoted by respondent 5 *"Taking an example of when CIs are sending a big message divided into small packets - an attacker won't just hack one device to change the process and make it do whatever they want, but they mess up the framework, and by messing with the order of the packets. What happens then is that the device will not be able to recognize the messages in their order and initiates the step before the audit. It gets out of control or it gets into a hunt mode where it is waiting for an expected packet. Because the organizations have programmed the framework to sometimes expect a delay in transmission, they have to wait for a minute for latency purpose and then they expect to receive the frame. But the hacked system has been waiting for more 3 minutes and it is not getting the frame so the system ignores the packet and starts processing other messages. The security system in the organization think 'this is not a cyber-attack', this is a problem of a cold run so the framework is flushed and the system is rebooted. The hacker still has the access and the manipulation happens again."* Hence the latency in the connectivity is always an issue for a cyber-attack in industrial IoT. The Indian government should implement 5G and IPV6 standards at the earliest so that it will lead towards cyber resilience and successful business models in IIoT transformation. Apart from the advantage of low network cost in the industrial sector, the built-in feature with interoperability and unified security model features are not being exploited by organizations in IoT ecosystem due to non-implementation of IPV6 across all organizations. Cross communications of cyber vulnerabilities among these organizations will improve security when IPV6 is fully implemented.

Another approach to address the IoT security standards is to develop best practices and principles on sector to sector basis. Policies should be derived with extensive consultations from industry experts/stakeholders with strict code of practices for IoT product and services, for both

manufacturers and users. When enquired on the status of any such proposal, respondent 4 states that, "*That's a work in discussion. There are some thoughts developed and exchanged at different forums, I think that the policies will evolve. Required quite urgently, so we don't have to retrofit, because for large scale deployments, retrofitting to an existing infrastructure will become an issue as it could solve the short-term need but will not provide a long-term solution in an evolving IoT architecture scenario.*" The IoT code of practices for entities from infrastructure manufacturers, service providers and users of IoT products for both public and private industrial sectors can achieve global standardization across Indian IIoT ecosystem.

The aim towards standardization is to support all parties in the development of industrial IoT with guidelines towards secure by design and to make the IoT user more secure and flexible towards industrial adoption. To address the cybersecurity of IIoT, the IoT code of practices will nudge the market behavior in a non-intrusive manner towards achieving the holistic self-regulation of PPPs for critical infra protection and information assurance.

4.2.4.3 Closing Policy Implementation and Legal Framework Gaps

Sufficient budget allocation according to the IoT policies and as per the growth projections of IoT is not practically implemented which is impacting the capacity building of infrastructures. Budget allocation for the year 2018[93] of ~ $500 million against a total Indian budget of ~$350 billion cannot provide private sector and FDI confidence to promote the Indian IoT ecosystem. Addressing the issue of budget constraints for implementation of the IoT policy objectives is based on both a political will and decisions on economic stability by the government of India.

When the political leadership heading the government intends to drive the growth of IoT ecosystem, it is critical to obtain buy-in from all sectorial and regional state government ministries for alignment on emerging technologies. To achieve this, the roles and responsibilities required for the success of the digital transformation must be transparent. Such initiatives encourage the government decision makers to recognize the IoT technology as a core competency growth instrument for the nation. This lends priority in central and state government budget allocation for all sectors for industrial IoT adoption. This impetus will motivate the private sector to be encouraged and invest in improving the focus on building digital capabilities and solutions in industrial IoT by procuring niche skills and platforms.

At the same time, increasing attention is required to be paid by the Indian government to create financial inclusion with availability and access to financial services for the economic development of IoT startups and SMEs, failing which may lead to slower growth rate. An efficient outcome of this government investment would be to fund and encourage export of IoT services by these start-ups to make them self-sustain.[94]

India needs capacity building in manufacturing units and network infrastructure to achieve digital transformation. Breakthrough innovations, collaboration with international partners, corporate venturing and incubators accelerate achieving the desired IoT policy implementation. UN report's statement in the Indian context that "*business dynamism is hampered by administrative hurdles*,"[95] needs to be addressed by the government. This is also confirmed by the high lead time invested in making a partnership agreement in cyber security in a recent development for the Netherlands. Respondent 9 states that "*Yes, in Cyber Security, at the moment we are trying to position*

[93] Ministry of Finance. BUDGET AT A GLANCE 2018-2019. Government of India , 2018, BUDGET AT A GLANCE 2018-2019.
[94] Ministry of Electronics & Information Technology. IoT Policy Document. Government of India, 2015, IoT Policy Document, meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.
[95] Schwab, Klaus, ed. "The Global Competitiveness Report 2018-2019." World Economic Forum, 2018.

these Dutch companies on the Indian market. This is step 1. So hopefully this will lead to investments and returns etc. But at the moment we are quite in an early phase, working on it for about 3 to 5 years already, and now this program is signed and they can actually get to work. Now we are trying to spot the opportunities and get the businesses involved." Reforms by the Indian government will support the financial foundations and India's credibility in the ranking of starting a business, adaptation of ICT and other related financial instruments. To harness the IoT potential, India needs to reinvigorate reform efforts to keep the IoT growth rate as per the policy vision. Standards on oversight, frequency, methods to stimulate and coordinate with all stakeholders in the IoT ecosystem is necessary. Hence, a pragmatic approach by creating business opportunities for both private and international investors is to be incorporated for the industrial sector.

Confidence building measures by mandatory disclosure of cyber breaches by Indian law, with defined legal and regulatory framework to support private and international investors in the IoT security will regulate all stakeholders of IoT ecosystem to be responsible and accountable for end to end security solutions. The emerging IoT ecosystem needs a regulatory authority which can solve issues among all stakeholders to maintain standards, promote information sharing and provide a fair and transparent policy environment including GDPR compliance to remove liabilities in the IIoT ecosystem.

Though the cyber security strategy[96] defines to have sectorial and regional state CERTs in 2013, till date no much progress is visible on sectorial or state CERTs under a unified cyber central command and control, except for the defense and power sectors which have independent CERTs. In the context of proposal acceptance of the security operations center (SOC) by central government, Mr.Rudra Murthy who is the Chief Information Security Officer of the Digital India Programme stated that "*we need to come together and work together to fight and prevent cyberattacks. Lack of coordination among different agencies will make it difficult to tackle cybercrime.*"[97] Implementation of IoT policy in this aspect becomes very relevant. In regional states, large group of SMEs account for high volume of IoT infrastructure/sensor contributor's due to focus on cost optimization. However, the risk of digital threat in SME involvement is high due to their low digital resilience; thus, rendering the importance of cyber security in SMEs. Hence sectorial and regional state CERTs can play a crucial role in taking ownership for cyber-attack prevention in SMEs under the unified command of national CERT-In.

All the regional states which are taking the lead by collaborating with PPP models, should take suitable organizational measures with public and private sector and security settings of their 3rd parties, hence, they are to be in turn made accountable to CERT-In at central level. Government of India should mandate all central ministries and state governments to create processes and organization structures that help PPPs become more collaborative, transparent, flexible and lean in integrating seamlessly with cyber security policies and practices. These requirements need to be addressed by the central government by initial allocation of budgets as per the policy vision to the state governments and for all sectorial CERTs. Regional state and sectorial CERTs are to be assigned with responsibility to ensure business continuity and cyber incident management of all organizations dealing with essential services within their jurisdiction. Such delegation will increase the security baseline of all Indian industrial IoT organizations. The involvement of national CERT-In can then be limited to overall coordination and any required international support during incident response.

---

96 NCIIP: MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY. "National Cyber Security Policy, 2013." National Cyber Security Policy, 2013, 2013.

97 Xplorenew. "Cyber Security Operations Center to Be Set up in Telangana State:" Xplorenew, 16 Dec. 2017, www.xplorenew.com/.

On the present status of policy implementation and additional policies required in the Indian context, respondent 5 states that "*Right now the answer to policy changes is yes and no. Because the technology is fast changing, the IT security policies must change to keep pace with the technologies hence they have to be revisited frequently. We cannot have a security policy for 2018 and treat this is my bible which will be implemented. Maybe it will have to be revised next year only. Now there is lot of focus on digitization and mobile technology, even for day to day transactions. I think the security policy must be tuned to the technologies and in turn all employees should be aware of today's security requirements.*" Similarly, in a workshop by Institution of Engineering and Technology, London, UK it was concluded that "*Policymaking at the pace of change of emerging technologies like the IoT is difficult in a domestic context and coordination at the international level will be much more so.*"[98]

Cyber security policy changes can be well embedded through awareness campaigns to staff and general public to understand a user's perspective. This should be done across all Indian industrial sectors and organizations for prevention of possible cyber attacks for effective incident response management in both the IT and OT environments. This will lead towards critical infrastructure protection and their essential services to all citizens.

4.2.4.4 Closing the Gaps of Trust and Collaboration in PPP

In Indian IoT policy, PPP models are mandated in building capacities, innovations and incident management in IoT ecosystem. Even these PPP models are being implemented by nudging both the Indian private sector and their international partners by state and central governments to contribute to the IoT ecosystem. Due to non-existent self-regulating networks of IoT stakeholders in PPP models, the trust deficits appear and becomes a disjunctive element. Collaboration in PPP through mutual trust and obligation is elaborated by respondent 9 stating "*You need these different parties because government on the one hand comes up with rules and regulations, businesses and knowledge institutions come up with innovation, they are the ones to drive innovation, although sometimes you need government policy to facilitate that innovation. In the Netherlands, we have lobbies that comes to privacy and cybersecurity law, so cyber security is a field where different parties have a role to play. And cyber security is very broad, it could be applicable to with the IoT and so many industries and data security or issues even in for example in harbors, it is so important that the data is secure because it has consequences for the business if it is not but also for the country*." Though the PPP models have disjunctive elements, the government should address these elements to change this state of affairs and needs to communicate frequently with all stakeholders and adopt a network centric approach to instill trust among partners.

The trust gaps were also found between the private parties due to network security issues where standardization of 5G and IPV6 are yet to be completed across the Indian telecommunications network. Implementing universal standards in cyber incident information sharing for all stakeholders in the Indian IIoT ecosystem will instill trust in PPP models.

To enhance cyber security through PPP, the government of India should promote cyber security information sharing partnerships as part of institutional frameworks aimed at engaging all stakeholders of IIoT ecosystem to participate. Government should create a network forum and community of public private organizations to setup cyber threat information sharing in real time in

[98] Carr, Madeline, et al. "STANDARDS, GOVERNANCE, AND POLICY STREAM." Governance and Policy Cooperation on the Cyber Security of the Internet of Things, 27 Mar. 2018.

a secure, trustable and dynamic environment. This improves situational behavioral awareness and reduces the industrial IoT ecosystem liability and impact on Indian critical infrastructures.

To achieve the objective of government of India, private sector and FDI investment requirements are expected to contribute to the cyber secure growth of IoT ecosystem with shared goals and incentives. A network with participants from both public and private sectors of IIoT ecosystem including the representatives of state and central governments with facilitating roles can be a possible solution. Transparency to all the IIoT stakeholders on the present and proposed policies on financial regulations and IoT policy initiatives along with commitments of milestones and defining explicitly without ambiguity on their mutual obligations of all stakeholders will improve trust and investment in IoT ecosystem.

Concerns due to government regime change is viewed by international partners at lower trust levels that can hinder investments for the exponential growth of IIoT. Improvement in trust levels in the case of regime change was expressed by respondent 9, bringing a viewpoint especially from international partners perspective to participate through the FDI route for investment in India stating "*It probably depends on who bears the responsibility for that project because in some countries when there is a new regime and a new political party comes to power, you see that in many levels of government, people are being changed. And that can have an effect, can slow things down.*" The apprehension of international investors need to be considered, hence, the Indian government regime change should not impact the growth policies and implementation guidelines and timelines. Government of India should achieve trust in FDI investment by maintaining stimulus to the business environment irrespective of any ruling coalition governments of the day at both central and state levels.

The government should adopt a no-blame culture and drive initiatives to instill trust in PPP models by stimulating them into PPP networks incorporating frequent information sharing of best practices and incidents. This brings responsibility and accountability to the industrial IoT ecosystem stakeholders. Confidence building measures initiated by Indian government can be extended to simultaneously add new networks and ensure International standardization of IIoT ecosystem. In the nebulous arrangements in PPP models, trust with mutual obligations becomes the 'corner stone' for success of the cyber security in industrial IoT ecosystem. These initiatives can also address the GDPR compliance by all Indian organizations using international 3rd parties for their expertise and avoid any possible liabilities for them.

Creating SOPs with periodical auditing in all CIs to proactively enhance organizational security policies will achieve the standards improving mutual trust and information sharing among all stakeholders. Respondent 3 states that "*Both private or government bodies observe basic confidentiality which instils trust in the auditing process thus providing good results. Which actually builds up security in a better way because different people look into IoT application in different ways, resulting in identifying possible vulnerabilities. With the non-disclosure agreement (NDA) there is trust built that particular information including the vulnerabilities identified will not be disclosed to anybody else now we are enforcing to some extent*". This response shows that information sharing with IoT stakeholders and auditing bodies is a feedback mechanism. This can be considered as a tool to enhance trust which in turn builds security in the cyberspace. Presently the partnerships are to be enforced from an audit regulatory authority.

Due to the lack of information sharing practices by trust, the transparency from the private sector is limited to the necessity of their business needs. They are comfortable not to report all incidents to CERT-In, and respond to their queries only. Though the IoT policy envisages a trusted and transparent PPP model, the observed reality is a neo-liberal steering of the IoT stakeholders by government. This approach is also creating a hindrance to information sharing during the cyber-

attacks and increases the incident response time which can be addressed by encouraging self-regulating networks in Indian IIoT.

Indian government should stimulate PPPs on shared goals and mutual benefits. The role clarity for all stake holders should be given considering the power relations within PPPs to build trust in the PPP networks. Beyond the mandated regulatory controls, the trust element is successful only without steering by the government in the information sharing process.

4.2.5 Bridging the Gaps-A Summary

The gap analysis in the previous sections has identified four striking areas of gaps that have to be addressed to make good progress in the efficient realization of Industrial IoT goals in the Indian context. Listed below are elaborations of the steps necessary to bridge the gaps in the same categories as identified in the gap analysis section as our design requirements. These are the areas of talent, IoT standards and infrastructure, policy implementation and legal frameworks, and the trust and collaboration in PPP networks.

Common to all gap areas, a due diligence per sector at state level rolling up to the national level is necessary for the government to start remediation and bridging measures per sector. This due diligence in addition to periodic oversight and measurement helps to identify and prioritize activities to result in an effective and timely progress in India's journey in IIoT. India should exploit the PPPs to perform this due diligence and execute bridging measures in an efficient manner.

Build Talent

1. Ministry of HRD, with the help of academia and autonomous bodies should encourage PPP models to train and build the scale of security professionals as necessary
2. IoT technologies and cyber security should be recognized as core competencies rather than as a good to have skill
3. Nurture and grow in-house talent and build skilled manpower for the long term through institutional skill development at national standards
4. Employee retention programs in order to build maturity on existing talent

Establish IoT Standards and Infrastructure

1. Accelerate 5G and IPV6 implementation across all sectors, regional states and organizations to build security by design; Government should fund and drive implementation at a faster pace to realize timelines from department of Telecom.
2. Build IoT code of practices and corresponding audit mechanisms for CIs in each sector and domain to be followed by respective industries for users, IoT device manufacturers and service providers; IoT best practices per sector in consultations from PPPs and industry experts to be leveraged
3. Set up national telecom standards cell to closely monitor international trends and national progress on vital performance indicators like network integrity, latency, availability and connectivity for real-time needs of IIoT; Involve industry and PPPs to explore standardization in India
4. Policy on Integration of IT and OT security architecture should be formulated by government of India through consultation process with all stake holders of IioT ecosystem

Policy Implementation and Legal framework

1. Government should get the buy-in from and jointly collaborate with sectorial and regional state ministries and set up security processes and organization structures to help PPP become more collaborative, flexible and lean for success of IIoT.
2. Government should encourage entrepreneurship for IoT startups with additional incentives and take appropriate measures/policy changes for fostering this in the talent pool; government funding to support export of IoT services to help them self- sustain
3. Address budget allocation issues/policies for cyber security as per IoT growth mandates to all central ministries, state governments to establish sectorial CERTs and state CERTs; reinvigorate reforms to maintain the IoT growth rate as per policy vision and define standard approach in investments
4. Implement policies to bring SMEs and third-party service providers into acceptable levels of digital resilience to improve nations cyber security posture;
5. Set standards on oversight, frequency, methods, areas of coverage and essential/desirable actions to stimulate and coordinate with all stakeholders in the IoT ecosystem
6. In order to attract FDI and promote IoT investments in India, Government should be transparent in information sharing with private sector enabling trust and ensuring national economic stability with improved indices of global competitive index rankings
7. Establish legal framework catering to judicial solutions on international compliance such as EU GDPR for all PPP models to demonstrate business dynamism; administration requirements for ease of business to be ensured
8. Bring awareness to all IoT organizations across sectors on compliance/confidentiality needs on international and national regulations to develop suitable policies with PPP to avoid liabilities
9. Set up policies to avoid delay in implementation of signed-off IIoT projects due to regime changes at national or state level

Generate Trust and Enhance Collaboration

1. Build collaboration between central and state government/non-government institutions through network approach and transparency to achieve security by efficient incident management by CERT-In
2. Unified approach in cyber incident management among multi stakeholders with responsibility and accountability should be implemented by all regional state governments in line with central government to achieve cybersecurity needs
3. No-blame culture, shared goals and role clarity with mutual obligation among public, private parties to be adopted in this greenfield area of IIoT to instill trust and improve collaboration among all stakeholders
4. SOPs should mandate networking with sectorial organizations within IIoT ecosystem.
5. Mutual feedback between auditing bodies and public-private organizations to be encouraged to instill trust. In turn trust brings security in the IIoT ecosystem
6. Government to mandate CERT-In to actively promote and prioritize information sharing on incidents from sectorial and state CERTs (occurrence, response and reporting) so that synergies can be leveraged across the nation building cyber resilience across industries in the IIoT ecosystem
7. Public awareness on security to be created to instill trust rather than terror across businesses and organizations to effectively deal with incident prevention and possibilities of cyberattack

As concluded above, the PPP meta-governance framework as designed in figure 3 has resulted in identifying four major gap areas which are the requirements for the enhanced policy design: (i) Talent gaps, (ii) Standards and infrastructure gaps, (iii) Policy implementation and legal framework gaps, and (iv) Gaps in trust and collaboration. This chapter further elaborated the closure of the gaps which are consolidated as design output to yield policy recommendations in improvement of PPPs to enhance the cyber security in Indian IIoT.

5. Conclusion

The main objective of this thesis is to enhance the degree of cyber security in Indian IIoT by formulating suitable PPP policies that can secure the adoption of IoT across all sectors. The Indian Government is aggressive in terms of seeking to elevate its economic growth as it can lessen the disparity between the digital facilities of its urban and rural community. To extend the health and financial services among other services, IoT facilitates smart cities for the metropolitan community and e-governance for remote villages. The IoT adoption rate is dependent on private sector initiatives and confidence levels. This research has established the study of networking methods of existing private and public-sector organizations to elevate cyber security in IIoT. To do this efficiently, a design-science approach has been used to formulate government policies.

Using CORAS risk modeling, we have designed a new model in the telecom case study. The results are extrapolated to other Indian CIs. The case study identified the attention points to arrive at requirements for the design of PPP policy improvements for enhanced cyber security posture in Indian industrial IoT adoption.

Based on the current implementation of the IoT policy instruments, research findings show that for Indian policy makers, the government can achieve its policy objectives through a transition from practicing neo-liberal PPP governance to a networking governance. In the process, new policies are to be enacted with shared goals, priorities, risks and incentives. Accordingly, it can be concluded that the identified governance gaps can be filled by means of self-regulatory networks of PPP models as part of the cyber security policy agenda.

Although technology advancements give complexity; they also aid in policy making and moving forward to adoption of IoT in industrial usage. The effective way to make progress in an evolving field is to measure the investment and progress, versus the vision to derive new policy requirements to achieve Indian IIoT adoption.

5.1 Policy Recommendations

Though the findings express the ground reality of a huge gap between the documented policy and its implementation, the following areas need to be improved. Policy making requires a continuous governance in a dynamic and responsive manner to the rapid technology advancements in the cyber domain to emerge with a successful and secure cyber space. A more pragmatic approach to continuous assessment of tangible policy progress along with the additional policies will be able to achieve the desired goals of exponential growth in IIoT with enhanced cyber security. The below recommendations are enhancements to the existing policies for PPP models. Implementation of the recommendations through the PPP meta-governance model by the Indian government will improve incident management and cyber security compliance in IIoT. The policy recommendations on PPP are derived to accelerate cyber security implementation in the Indian IIoT ecosystem.

1) **Build talent to address shortage of skilled manpower as part of cyber security strategy across IIoT ecosystem**

In the cyber security domain, there is a definite talent gap at both operational and governance levels. A shortage of skilled security professionals proves to be an issue for timely incident identification, notification and response. Security professionals cannot be outsourced due to national security concerns.

To address this issue, new policies should be created with the purpose of nurturing in-house talent and building skilled manpower with a long-term outlook. This can be done with the help of academia, autonomous bodies through PPP models and with institutional skills developments at international standards.

Possible initiatives that can be taken by the Government of India are to build employee retention programs and encourage new IIoT research projects in the cyber domain at all academic universities. Employee retention programs are required to build maturity on existing talent. New research projects, on the other hand, can create opportunities towards trainings for employees in Industrial IoT environment.

2) **Implement "code of practice" standards in the supply chain of industrial IoT products.**

The current IoT products, market and services are immature in terms of quality. Policies on "Code of practice" in IIoT should come up with good practices for IoT security including default settings by manufacturers for Industrial usage. These need not be too prescriptive but necessarily incorporated as baseline security requirements for IoT manufacturers, application developers and users. Such standards of code of practice will address the cyber security of the industrial connected devices by adding certification agencies with PPP models. These can start with formulating suitable directives which later on can be converted to regulations. The practices will merge safety and security of industrial IoT ecosystem and also lead to testing, certification and monitoring of whole system and not just on individual components of organizations.

3) **Regulate integrated information technology (IT) and operational technology (OT) security architecture**

Cyber incident management in IIoT ecosystem needs a holistic approach. Hence maintaining the IT's and OT's security stacks independently will not deter the cyber vulnerabilities and incidents. The growth of IIoT makes OT more critical as it involves shut down of critical infrastructure for protection in case of a cyber attack. Policies on integrating IT and OT security architecture in design process to ensure holistic view to defend from cyber attacks in IIoT ecosystem are to be derived. These will ensure to prevent hardware malfunction and avoid emergency and life-threatening situations in IIoT ecosystem.

4) **Deliberate "duty to care" with all stakeholders of IoT policy implementation**

The present draft IoT policy gives a vision on what the government is expecting to achieve in the coming period. The observed IoT policy implementation in India did not yield the anticipated encouragement but instead rested obligations of IIoT growth with responsibility and accountability to the private sector. The current policy undermines the duty to care of other stakeholders who are contributing to the IoT policy agenda.

Defining roles, non-ambiguous responsibility and accountability, accurate and consistent mutual obligations and shared goals including financial provisions and revenues are areas to explore new policies by Indian government. Incorporating frequent communication and progress review with all stakeholders of IoT policy implementation will also enhance cyber posture in IIoT.

5) **Formulate policies to expand existing CERT-In functions by establishing sectorial and state CERTs under framework for cyber incident management**

The existing cyber incident management framework is insufficient. Non-availability of state and sectoral CERT (except power and defence) are impediments to Indian cyber vulnerabilities and risk assessments. Information sharing practices in the Indian context can make significant impact to the larger whole in cyber security enhancement in IIoT. Capacity and capability building with cyber awareness for operators and citizens for unified incident management is needed to enhance the cyber security posture of India.

The policy for expanding the existing CERT-in functions by establishing individual institutions such as national SOC, CSIRT, ISAC, 29 regional state CERTs and all sectorial CERTs under unified framework for cyber incident management will be a leap forward to India reaching towards a cyber resilient nation. Financial means through assured budget provisions and timelines will boost the IIoT adoption and its cyber incident management.

6) **Establish a central criminal justice system for trust and confidence building in IIoT adoption.**

Currently in majority of the states, legal framework on cybercrimes/ non-compliance of cyber incident notification is not framed as a defined law. Due to the jurisdiction of law enforcement agencies under the state government, the cyberspace domain consequences are different and spread across all regional states. This deters national security. All cybercrimes and cyber incident management legal issues demand a central criminal justice system for the IoT ecosystem. The implementation of this will build confidence in FDI and private investment in IIoT ecosystem and trust among all stakeholders to participate actively in adoption of IIoT with support of their international third parties irrespective of any regime change.

Additionally, legal framework will also enable public and private sector to cater to mandatory international regulations e.g. GDPR compliance to reduce liabilities on Indian parties in the IIoT ecosystem.

It may be beneficial to consider creating an autonomous IoT regulatory authority to enable India in the emerging IoT space. It will also provide a fair and transparent policy environment which facilitates growth and international recognition.

7) **Promote innovation and foster IoT startups entrepreneurship**

Innovations reduce the import dependency on IoT products and applications for India. With local manufacturers providing IIoT needs, India's IIoT adoption can achieve the required growth rate. IoT startups need the test beds and incubators to accelerate, though these are incorporated in present policy, large policy implementation gap is observed. Hence, no infrastructure support by government of India to IoT startups is observed.

Therefore, IoT startups require a policy change on financial and non-financial benefits for their innovation and contribution to Indian IIoT market. As fostering IoT start-ups in cyber security can contribute to 10-15 million jobs in the long term, policies created by the Indian government will reap positive payoff as economic incentives for start-ups and SMEs will encourage

them to align faster to the IoT policy vision. This will also help India achieve international standards, IoT innovations for long term economic benefits and improvement in productivity and competitiveness. Financial policies for funding IoT based startups focused on export of IoT services will make the startups self-sustainable.

8) **Promote cyber security information sharing partnerships in IIoT**

The present PPP models in IoT deployment are observed as contractual agreements. These include standard operating procedures (SOPs) but exclude any form of cyber incident information sharing. The organizations' security policy also restricts such information sharing practices. These restrictions cause cyber vulnerabilities to the IIoT ecosystem. With the policies on cyber awareness, organizations tend to achieve cyber security in IIoT ecosystem.

An institutional framework policy to bind cyber security information sharing partnerships in public-private parties of the IIoT ecosystem to further enhance cyber security is required. Cyber threat information sharing in real time will improve situational behaviour awareness, best practices sharing, timely addressing of cyber vulnerabilities and prevent liabilities to all stakeholders.

9) **Stimulate network governance as part of cyber security agenda to create self-regulating PPP models.**

The current IoT policy incorporates PPP models. There are limitations in the PPP model as it is observed that the approach taken to implement the policy is a neo-liberal approach of governance. All the stakeholders in the IoT ecosystem are working in silos under organizational SOPs. This limits the scope of information sharing and causes trust deficit. In the IoT domain, all the systems are dependent on the secure connectivity, information sharing and trust elements to enhance cyber security in industrial usage. Hence, a holistic approach of governance of cyber security in IIoT is required.

Cybersecurity governance includes support from social-technical layer of cyber space. This contributes to securing the IIoT ecosystem and Indian cyber space. Network approach of governance gives both public, private and other stakeholders in the IIoT ecosystem emphasis on collaboration to achieve shared goals with self-regulation. The government of India should act as a stimulator in a collaborative role to achieve the shared goals by arranging platforms and policies of information sharing. This ensures honesty, cooperativeness and community interest demonstrating values and trust among all the stakeholders for successful IIoT adoption across all sectors to achieve India's goal of enhanced cybersecurity in IIoT processes.

Cyber security agenda with network governance as a policy, stimulates individual PPPs into a network of institutions to form strategic domestic and international coalitions with interoperable harmonious standards from a state of cyber awareness ecosystem to cyber capability ecosystem.

5.2 Reflection and Future Research

Although this research provides significant policy corrections, a few limitations can be identified. We have done research based on a case study applying CORAS risk modeling which has given us the challenge areas in PPP in IIoT adoption. Research on these challenge areas as per the methodology framework gave us the disjunctive elements as requirements in PPPs while implementing the existing policies. New perspectives to bridge the gaps were arrived. With this

research, we have come up with the above set of recommendations in PPP governance to further enhance the cyber security in Indian IIoT. This is not the full story of course, we came up with recommendations but in practice they should be implemented and validated. We cannot validate these recommendations without the alignment of Government of India. This is a limitation in this research, but it might be an improvement for future research to figure out whether these policy recommendations will really work in practice. It might be that some recommendations work much better than the others when they are adopted in practice. These encountered experiences will be assessed by the PPP stakeholders and submitted as feedback on the implementation of the IoT security governance policies, whether fully or partially for further assessment by the Government of India. Perhaps the validation interview statements together with the new policy instruments, may later yield different perception of ground reality of cyber security implementation and the change in feedback could also lead to new policy artifacts.

Many publications focus that industrial IoT safety implications is paramount; hence, research on safety implications should be expanded; for that the IIoT ecosystem needs to be adequately informed and protected as the IIoT adoption grows. Safety should be part of the design technology standards for all things, businesses and citizens. The future in cyber security is towards cyber safety from reactive to proactive, from silos to collaborative approach through network governance incorporating transparency, trust and due diligence. Hence, it would be interesting to research for meta-governance for PPP policies in achieving cyber safety of the Indian IIoT ecosystem. Enhanced policies can be formulated based on these recommendations as improvement for future research for cyber resilience in the Indian IIoT environment.

BIBLIOGRAPHY

[1] Annual Report (2017)Indian Computer Emergency Response Team (CERT-In) Ministry of Electronics & Information Technology Government of India 9th April, 2018

[2] Brændeland, Gyrd, Atle Refsdal, and Ketil Stølen. "Modular analysis and modeling of risk scenarios with dependencies." Journal of Systems and Software 83.10 (2010): 1995-2013.

[3] Brahima, S."Global Cybersecurity Index 2017." International Telecommunication Union (ITU) (2017): 1-77.

[4] Carr, Madeline, et al. "STANDARDS, GOVERNANCE, AND POLICY STREAM." Governance and Policy Cooperation on the Cyber Security of the Internet of Things, 27 Mar. 2018.

[5] Carr, Madeline. "PETRAS." EPSRC IOT Research Hub, www.petrashub.org/iot-governance-policy-cooperation-cyber-security/.

[6] Carr, Madeline. "Public–private partnerships in national cyber-security strategies." International Affairs 92.1 (2016): 43-62.

[7] Case, Defense Use. "Analysis of the cyber-attack on the Ukrainian power grid." Electricity Information Sharing and Analysis Center (E-ISAC) (2016).

[8] CERT-In. "Indian - Computer Emergency Response Team." Indian - Computer Emergency Response Team, www.cert-in.org.in/.

[9] Christopher, Nilesh. "IoT Alone Will Create 15 Million Jobs: Aruna Sundararajan - Times of India." The Times of India, Business, 15 Sept. 2017, timesofindia.indiatimes.com/people/iot-alone-will- create-15-million-jobs-aruna-sundararajan/articleshow/60524382.cms.

[10] Department of International Relations and Cooperation. "10th BRICS Summit: Johannesburg Declaration." Government Programmes, Projects and Campaigns | South African Government, 27 July 2018, www.gov.za/speeches/10th-brics-summit-johannesburg-declaration-27-jul-2018-0000.

[11] Department of Telecommunications. "National Digital Communications Policy 2018." DepartmentofTelecommunications,2018,dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf.

[12] Dunn-Cavelty, Myriam, and Manuel Suter. "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." International Journal of Critical Infrastructure Protection 2.4 (2009): 179-187

[13] ET Bureau. "India Third Worst Hit Nation by Ransomware Wannacry; over 40,000 Computers Affected." The Economic Times, Times Internet, 17 May 2017, economictimes.indiatimes.com/tech/internet/india-third-worst-hit-nation-byransomware-wannacry-over-40000-computers-affected/articleshow/58707260.cms.

[14] ETCIO. "India IoT Market to Grow over 28 Pc CAGR during 2016-22: Study - ET CIO." ETCIO.com, 8 Dec. 2016, cio.economictimes.indiatimes.com/news/internet-of-things/india-iot-market-to- grow-over-28-pc-cagr-during-2016-22-study/55874529.

[15] ETTelecom. "Juniper Networks to Invest Rs 6,700 Crore in India to Back Digital Drive ETTelecom." ETTelecom,8Dec.2016, telecom.economictimes.indiatimes.com/news/juniper-networks-to-invest-rs-6700-crore-in-india-to-back-digital-drive/55882988?redirect=1.

[16] Europol. “Joint Cybercrime Action Taskforce (J-CAT).” Europol, 13 Sept. 2018, www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce.
[17] Exhibitions India Group. “3rd Internet of Things India Expo 2019.” IoT India, 2019, www.iotindiaexpo.com/iot-india-expo.aspx.
[18] Express Web Desk. “What Is New National Digital Communications Policy-2018?” The Indian Express, The Indian Express, 26 Sept. 2018, indianexpress.com/article/india/what-is-new-telecom- policy-2018-digital-connectivity-communications-5375761/.
[19] EY. Path to Cyber Resilience: Sense, Resist, React Global Information Security Survey 2016-17. 2017, Path to Cyber Resilience: Sense, Resist, React Global Information Security Survey 2016- 17, www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2016-17-india-report/$FILE/EY-global-information-security-survey-2016-17.pdf.
[20] Gregory-Brown, Bengt. "Securing Industrial Control Systems-2017." A SANS Survey. SANS Institute (2017).
[21] Gupta, Atul. “Information Security in Telecom Sector.” KMPG, 2011, www.kpmg.de/docs/Information-Security-in-Telecom-Sector.pdf
[22] Gupta, Monika. “Indian Telecom Industry Getting Ready for M2M/IoT.” Indian Telecom Industry Getting Ready for M2M/IoT, Aug. 2017
[23] Hevner, Alan R., et al. “DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH.”MISQuaterly,Mar.2004,wise.vub.ac.be/sites/default/files/thesis_info/design_science.pdf.
[24] Indian Government, Vigyan Bhavan, and V.S. Saraswat. “NITI .” NITI , NITI Aayog, 2018.niti.gov.in/writereaddata/files/document_publication/CyberSecurityConclaveAtVigyanBhava nDelhi_1.pdf.
[25] Jan van den Berg, Jacqueline van Zoggel, Mireille Snels, Mark van Leeuwen, Sergei Boeke, Leo van de Koppen, Jan van der Lubbe, Bibi van den Berg and Tony de Bos, On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education, NATO STO/IST-122 symposium in Tallin, (c) pages 1-10, 2014.
[26] Karnouskos, Stamatis. "Stuxnet worm impact on industrial cyber-physical system security." IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society. IEEE, 2011.
[27] Kharbanda, Vipul. “Incident Response Requirements in Indian Law.” The Centre for Internet and Society, 28 Dec. 2016, cis-india.org/internet-governance/blog/incident-response-requirements-in-indian-law.
[28] Kumar, Chethan. “One Cybercrime in India Every 10 Minutes - Times of India ►.” The Times of India, Business, 22 July 2017, timesofindia.indiatimes.com/india/one-cybercrime-in-india-every- 10-minutes/articleshow/59707605.cms.
[29] Lin, S. W., et al. "The Industrial Internet of Things, Volume G1: Reference Architecture." Industrial Internet Consortium (2017).
[30] Luiijf, Eric. Personal Interview. 24 November 2018. Unpublished.
[31] Ministry of Electronics & Information Technology. IoT Policy Document. Government of India, 2015, IoT Policy Document, meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.
[32] Ministry of Electronics & Information Technology. Personal Data Protection Bill. GovernmentofIndia,2018,PersonalDataProtectionBill,meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.
[33] Ministry of Electronics and Information Technology. 12th Plan Report on Cyber Security. Government of India, 12th Plan Report on Cyber Security, meity.gov.in/writereaddata/files/downloads/Plan_Report_on_Cyber_Security.pdf.
[34] Ministry of Finance. BUDGET AT A GLANCE 2018-2019. Government of India , 2018, BUDGET AT A GLANCE 2018-2019.

[35] Miniwatts Marketing Group. “Internet Top 20 Countries - Internet Users 2018.” Senegal Internet Usage and Telecommunications Reports, 15 Dec. 2018, www.internetworldstats.com/top20.htm.
[36] NCIIP: MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY. “National Cyber Security Policy, 2013.” National Cyber Security Policy, 2013, 2013.
[37] Peña-López, Ismael. "ITU Internet report 2005: the internet of things." (2005)
[38] Press Trust of India. “Bluru Prime Destination for IoT Startups in India, Study .” India Today, India Today, 24 May 2017, www.indiatoday.in/pti-feed/story/bluru-prime-destination-for-iot- startups-in-india-study-931731-2017-05-24.
[39] PWC. “Turnaround and Transformation in Cybersecurity: Key Findings from The Global State of Information Security® Survey 2016.” PWC, 2016, www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf.
[40] Rai, Saritha. “This Indian Judge Is Making Google and Amazon Nervous.” Bloomberg.com, Bloomberg,10June2018, www.bloomberg.com/news/articles/2018-06-10/tech-giants-nervous-as-judge-drafts-first-data-rules-in-india.
[41] Raut, Sandeep. “What Is The Difference Between Consumer IoT And Industrial IoT (IIoT)? | Articles | Internet of Things.” Articles | Finance | Innovation Enterprise, 20 Feb. 2017, channels.theinnovationenterprise.com/articles/what-is-the-difference-between-consumer-iot-and-industrial-iot-iiot/
[42] RVO Netherlands. Cyber Security in India Opportunities for Dutch Companies . Rijksdienst Voor Ondernemend Nederland, 2018, Cyber Security in India Opportunities for Dutch Companies .
[43] Sadeghi, Ahmad-Reza, Christian Wachsmann, and Michael Waidner. "Security and privacy challenges in industrial internet of things." Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015.
[44] Saiphani, Kv, and G. Venugopal. "RANSOMWARE AND ITS IMPACT IN INDIA-A LITERATUER STUDY."
[45] Schwab, Klaus, ed. "The Global Competitiveness Report 2018-2019." World Economic Forum, 2018.
[46] Sharma, Pranjal. “What the Fourth Industrial Revolution Means for India.” World Economic Forum, 3 Oct. 2017, www.weforum.org/agenda/2017/10/kranti-nation-india-and-the-fourth- industrial-revolution/.
[47] SRIA 2014. “Internet of Things.” IERC-European Research Cluster on the Internet of Things, www.internet-of-things-research.eu/about_iot.htm.
[48] Stoelen, Ketil, and Gencer Erdogan. “The CORAS Method.” The CORAS Method, 16 Nov. 2015, coras.sourceforge.net/.
[49] Talja, S. (1999). Analyzing qualitative interview data: The discourse analytic method. Library & information science research, 21(4), 459-477.
[50] Thuan, Nguyen Hoang, Pedro Antunes, and David Johnstone. "A Design Science Method for Emerging Decision Support Environments." arXiv preprint arXiv:1605.04725 (2016).
[51] UNCTAD. “Investment and New Industrial Policies: The Way Forward.” World Investment Report 2018 United Nations Conference on Trade and Development (UNCTAD) World Investment Report (WIR), 2018, pp. 165–178., doi:10.18356/9c309851-en.
[52] Xplorenew. “Cyber Security Operations Center to Be Set up in Telangana State:” Xplorenew, 16 Dec. 2017, www.xplorenew.com/.

Appendix I – Interview Guidelines and Questions

Discourse analysis was conducted with open-ended questions in a semi-structured manner. All respondents were not posed the standard questionnaire, instead the nature of interview was lively to tap their experience and obtaining expert comments to guide my thesis within the identified topics. The exhaustive questionnaire is provided below for reference.

Topic: General on PPPs

- What are your concrete experiences with public-private partnerships, or partnerships with the Indian Central/State Government and Private partner?
- With what type of organization are you engaged presently in partnerships as part of IoT ecosystem?
- What is your general perception of the use of the past and current PPPs within your organization to comply with regulatory goals and priorities?
- What would you say about the use of PPPs in the field of cyber security in General and maintaining privacy?
- Do you have any measurements of success?
- What is your perspective on advancement of digitization in India through PPP in IoT ecosystem?

Topic: The PPP, Incident management, Trust, Governance

- What are the most important factors in a PPP according to you?
- How have you experienced the PPP?
- What is the greatest added value of a PPP for you?
- What are the biggest opportunities for future PPPs?
- And what are the biggest challenges?
- What kinds of partnerships are useful to achieve your organization cyber secure?
- What does the future for PPPs look like in your opinion?
- Do you consider that the PPP was based on equality?
- Can PPP harness the opportunity of industry 4.0 revolution ensuring Indian cyber space security?
- What are your organisation's expectations if you are part of cyber-security information sharing partnership?
- How is information sharing practiced with the public/private parties and reciprocity during a possible cyber incident?
- How to do things differently in cyber incident management policy implementation?
- Do you think your organization is trending towards Critical Infrastructure Protection (CIP) or Critical Infrastructure Resilience (CIR)?

- What additional policies, policy constraints, do you envisage for Indian industry to be CIR compliant?
- Have you observed central/state governments stimulating and coordinating PPPs to secure Indian cyber space in general and telecom industry in specific?
- Do you think regulatory goals and practices will have a positive economic impact? Can you please elaborate?
- What impact meant to your organization in the present cyber incident management procedures by CERT-In policies?
- Are you comfortable with present cyber incident reporting structure? Is this structure helping your organization to be cyber secure? If not, what suggestions do you give for further improvement?
- How is risk assessment being done to protect your organizations crown jewels from aging devices/legacy systems in IoT environment that have not been patched or updated?
- If it were up to you, would you continue to engage in self-regulating governance of PPPs in the future to ensure cyber security in your organization?
- How important it is for your organization business model to self-regulate on personal data protection as part of trust management and confidence building measures?
- Do you see the cyber security policy guidelines implemented in line with national cyber security strategy?

Topic Responsibility and Accountability

- When engaging in such PPPs, how was responsibility divided/shared between the organizations?
- And how was accountability divided between the organizations?
- Do you feel this division was appropriate for the project/partnership?
- Were there any uncertainties between partners that may have caused problems according to you?
- Can you suggest the responsibility and accountability in PPP expected by you to improve cyber security in implementing IoT initiatives in your industry?
- What it looks like to be responsible and accountable to advance cyber security as stakeholder in IoT ecosystem?

Topic: Experience with partners

- How have you experienced the partnership with the Indian/State Government and Private partner?
- Do you think the cooperation on project execution at Indian/State Government is similar to that for a Private party?
- And what change would yield better results?
- Do you also notice that the cooperation changed after an election? Are there any noticeable differences?
- What do you see as the indicators (both internal and external) of success in PPP to secure Indian telecom sector?

The interviews have been anonymized to guarantee that the confidentiality of identity is maintained. Schematic overview below displays the interviewees and their respective functions in random order.

Schematic Overview of Interviewees and their Functions

Interviewee	Reference	Function
Anonymized	Respondent 1	Professor, Indian Institute of Technology
Anonymized	Respondent 2	Senior official at Government Telecom Security
Anonymized	Respondent 3	Manager at Ministry of IT
Anonymized	Respondent 4	Senior official at Ministry of Telecommunications
Anonymized	Respondent 5	Senior official at Indian Public TSP
Anonymized	Respondent 6	Network security manager, Private TSP one
Anonymized	Respondent 7	Regulatory head, Private TSP two
Anonymized	Respondent 8	Risk manager, Private TSP three
Anonymized	Respondent 9	Policy advisor, Department of International Enterprise, Government of Netherlands