IDSA Monograph Series
No. 60 April 2017

SECURING CRITICAL INFORMATION INFRASTRUCTURE

Global Perspectives and Practices

MUNISH SHARMA

IDSA Monograph Series
No. 60 April 2017

Securing Critical Information Infrastructure

Global Perspectives and Practices

Munish Sharma

INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

ISBN: 978-93-82169-74-1

Disclaimer: The views expressed in this Monograph are those of the author and do not necessarily reflect those of the Institute or the Government of India.

First Published: April 2017

Price: Rs. 180/-

Published by: Institute for Defence Studies and Analyses
No.1, Development Enclave, Rao Tula Ram Marg, Delhi Cantt., New Delhi - 110 010
Tel. (91-11) 2671-7983
Fax.(91-11) 2615 4191
E-mail: contactus@idsa.in
Website: http://www.idsa.in

Layout & Cover by: Vaijayanti Patankar

Printed at: M/S Manipal Technologies Ltd.

Contents

Abbreviations

APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
CCA	Centre for Cyber Assessment
CERT	Computer Emergency Response Team
CERT-In	Indian Computer Emergency Response Team
CESG	Communications-Electronics Security Group
CIAC	Critical Infrastructure Advisory Council
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CIR	Critical Infrastructure Resilience
CISO	Chief Information Security Officer
CIWIN	Critical Infrastructure Warning Information Network
COTS	Commercial off-the-Shelf
CPNI	Centre for the Protection of National Infrastructure
CSOC	Cyber Security Operations Centre
CTSA	Counter Terrorism Security Advisor
DNS	Domain Name System
DoS/DDoS	Denial of Service/Distributed Denial of Service
ECI	European Critical Infrastructures
ENISA	European Union Agency for Network and Information Security
EP3R	European Public-Private Partnership for Resilience
EPCIP	European Programme for Critical Infrastructure Protection
EU	European Union
GCHQ	Government Communications Headquarters
GII	Global Information Infrastructure

GoI	Government of India
HSIN-CI	Homeland Security Information Network-Critical Infrastructure
ICONS	Industry Consultation on National Security
ICT	Information and Communications Technology
ISIS	Islamic State of Iraq and Syria
IT	Information Technology
NATO	North Atlantic Treaty Organization
NCIIPC	National Critical Information Infrastructure Protection Centre
NCSC	National Cyber Security Centre
NIC	National Informatics Centre
NII	National Information Infrastructure
NIPP	National Infrastructure Protection Plan
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
OCSIA	Office of Cyber Security and Information Assurance
OECD	Organisation for Economic Co-operation and Development
PSTN	Public Switched Telephone Network
SCADA	Supervisory Control and Data Acquisition
SCO	Shanghai Cooperation Organization
SSA	Sector-Specific Agency
TCP/IP	Transmission Control Protocol/Internet Protocol
TISN	Trusted Information Sharing Network
UIDAI	Unique Identification Authority of India
UNGA	United Nations General Assembly
UN GGE	United Nations Group of Governmental Experts
VPN	Virtual Private Network

List of Tables and Figures

Tables

Figures

Chapter 1

Introduction

The advances made in the field of information and communications technology (ICT) have transformed the functioning, operations and security practices of the governments, business enterprises, research institutions and defence and security establishments. Over the last two decades, these interconnected computer networks have engulfed every aspect and process of production, communication and decision making. Often termed as information systems, they play a pivotal role in dissemination of key governance services, business development, communication among people, organizations and nation states, defence management and executing societal functions. In practice, information systems enable modern governments to deliver services such as healthcare and education; business enterprises to manage their global operations and supply chains; and armed forces to control their logistics across wide geography and varying physical conditions. Therefore, in this era, information is an asset and the availability, confidentiality and integrity of information is vital to the decision-making process.

The modern society is built upon a number of physical infrastructures, such as generation, transmission and distribution of energy, air and maritime transport, railways, water supply pipelines and storage, telecommunication networks, banks and financial services, healthcare, taxation, manufacturing industries and so on. The seamless functioning of these infrastructures is essential for the social and economic development or well-being of a nation state. In the contemporary environment, national security calculus encompasses both economic and military dimensions. Robust, resilient and efficacious infrastructure in the form of electricity, transportation and secure communication channels is vital to economic and social advancement.

Over a period of time, these infrastructures have grown, expanded and interconnected; in fact, they have evolved in such a manner that many of the systems are intertwined. For instance, a thermal power

plant is dependent upon railways for timely delivery of coal and, in turn, the same railway system is dependent upon the electricity generated by the thermal power plants. Therefore, the convolution of these infrastructures is so complex and capricious that a small malfunction can spread across different segments, having a wide-ranging impact, which may or may not have been assessed. Generally, the cascading effect of disruptions, either minor or major, is practically unfeasible to assess and simulate. In essence, the infrastructures are immensely interdependent; and fostered with the operational complexity, they are extremely vulnerable to a plethora of threats, ranging from natural hazards to crime and terrorism and from human-induced errors to scrupulous technical or operational problems.[1] In some form or the other, these infrastructures have been the prime target of terrorist attacks. For example, the World Trade Centre in New York and the urban transit systems in Mumbai, Madrid or London were targeted as epicentre of economic activity and transportation system used by masses, which crippled other infrastructures and had a devastating impact on the psychology of the victims as well as the onlookers. The alleged Russian denial of service (DoS) attacks in 2007 were precisely targeted at the Estonian Parliament, major banks, governmental ministries, newspapers and broadcasters, creating havoc for one of the most networked countries in the world. As threats and vectors have grown manifold, so have the responses and countermeasures.

The United Nations General Assembly (UNGA), in its Resolution 58/199, has recognized the importance of information technology (IT) for the promotion of socio-economic development, the provision of essential goods and services, the conduct of business and the exchange of information for governments, businesses, other organizations and individual users.[2] The resolution discerns the complexity of the network of critical information infrastructure components that exposes them to a growing number and wider variety of threats and vulnerabilities,

---

1 Eugene Nickolov, "Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations", *Information and Security*, Vol. 17, 2005, p. 107.

2 UNGA, "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures", Resolution 58/199, 30 January 2004.

thereby raising new security concerns. The resolution calls upon the member states to examine infrastructures and identify interdependencies among them, engage in international cooperation and develop strategies to reduce risks to critical information infrastructures, in accordance with national laws and regulations.[3]

As recognized and realized in reality, these infrastructures are dependent upon information systems for their day-to-day functioning, maintenance and operations. The IT infrastructure, as a backbone of information systems, enables efficient storage, processing and seamless transmission of information for complex interactions among networks and systems, spread across organizational boundaries or physical and political borders. The relationships among various components of critical infrastructure can therefore be characterized by a web of multiple connections such as feedback, feed-forward paths and intricate, branching topologies. A minor disruption at a point could have a rippling effect across multiple critical infrastructures.[4] For instance, a failure at an electricity grid can immediately bring dependent railway or mass transit services to a complete standstill, and a prolonged outage of this sort would impact telephone, healthcare and banking services.

The evolving nature of information infrastructures is complex and poses challenges to security measures due to decentralized operations, diverse technologies and multiple actors and varying interests of the stakeholders. To address these emerging security challenges, it is imperative to define the parameters of criticality from management, technological and security perspectives. Moreover, the various degrees of interdependency among the critical infrastructure needs to be identified and quantified to assess the impact in case of a crisis. Due to various technical, practical and financial constraints, comprehensive protection is a daunting task for policymakers and information security

---

3 Ibid.

4 Steven M. Rinaldi, James P. Peerenboom and Terrence K. Kelly, "Identifying, Understanding and Analyzing Critical Infrastructure Dependency", *IEEE Control Systems Magazine*, Vol. 21, No. 6, 2001, p. 14, available at http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf, accessed on 04 July 2016.

practitioners. According to Myriam Dunn, critical infrastructure protection is inclusive of four different perspectives: a system-level technical perspective; a business perspective; a law enforcement perspective; and a national security perspective.[5]

Critical infrastructure is facing new and technologically sophisticated threats. The growing offensive capabilities of nation states and non-state actors to exploit the vulnerabilities underlying the prevalent information infrastructure for political, economic and military predominance have lately added a geopolitical dimension as well. Cyber warfare and cyber terrorism have evolved as matters of serious concern and are being discussed in many of the bilateral, multilateral and international forums, such as the United Nations,[6] North Atlantic Treaty Organization (NATO),[7] European Union (EU),[8] Shanghai Cooperation Organization (SCO),[9] Organisation for Economic Co-operation and Development (OECD) and Association of Southeast Asian Nations (ASEAN).[10] The United Nations Group of

---

5 M. Dunn, "Understanding Critical Information Infrastructures: An Elusive Quest", in M. Dunn and V. Mauer (eds), *International CIIP Handbook 2006, Vol. II*, Switzerland: Center for Security Studies, ETH Zurich, 2006, pp. 27–53.

6 United Nations, Department of Economic and Social Affairs, "Cybersecurity: A Global Issue Demanding a Global Approach", 12 December 2011, available at http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html, accessed on 04 September 2016.

7 "NATO: Changing Gear on Cyber Defence", *NATO Review*, available at http://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/, accessed on 04 September 2016.

8 European Union Agency for Network and Information Security, available at https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme, accessed on 04 September 2016.

9 NATO Cooperative Cyber Defence Centre of Excellence, "SCO Fighting Cyber Terrorism", available at https://ccdcoe.org/sco-fighting-cyber-terrorism.html, accessed on 04 September 2016.

10 "ASEAN Steps up Fight against Cybercrime and Terrorism", *ASEAN Affairs*, 30 May 2014, available at http://www.aseanaffairs.com/asean_news/security/asean_steps_up_fight_against_cybercrime_and_terrorism, accessed on 04 September 2016.

Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, in its report of 2015, has laid "special emphasis on the dangers stemming from attacks against critical infrastructure systems".[11]

The vulnerabilities of critical infrastructures and their dependence on information infrastructure make them a soft and obvious target for states, as well as for terrorists, to disrupt critical services or functions disbursed by them. These types of attacks, which are increasing across the globe, have considerably altered the views of the policymaking apparatus of all the members of the international community on how to secure and protect their population, information systems, critical infrastructure and the cyberspace as global commons, from any unforeseen attack manifesting in cyber or physical realm. Successful attacks on critical infrastructure can directly or indirectly inflict mass casualties or have grave economic implications, attracting significant public attention or discontent. As a result, threats to critical infrastructure are becoming more probable and potent, with far-reaching impacts and consequences.[12] Steadily, the primary functions of industries, i.e., commercial or public sector undertaking entities which collectively form the critical infrastructure, have been built over an unfathomable asset, known as information infrastructure.

---

[11] NATO Cooperative Cyber Defence Centre of Excellence, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law", available at https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html, accessed on 04 September 2016.

[12] Thales Security Systems, *Airport Infrastructure Security towards Global Security: A Holistic Security Risk Management Approach*, Vélizy Cedex: Thales Security Solutions and Services Division, 2008, p. 3, available at http://www.thalesgroup.com/Markets/Security/Documents/Airport_Infrastrucure_Security_Towards_Global_Security/, accessed on 23 July 2016.

Chapter 2

Information Infrastructure
The Building Block

Even as physically and geographically dispersed applications are getting integrated for information exchange purposes, the dependency amongst systems is growing and therefore information in itself has become an asset. On the other side, the computer hardware, software and their digital networks which support collection, storage, processing and dissemination of information are the underlying physical infrastructure. Information infrastructure is the term used to describe, in totality, the interconnected computers and networks and the essential information flowing through them.[1] In other words, information infrastructure is "a shared, evolving, heterogeneous installed base of IT capabilities among a set of user communities based on open and/or standardized interfaces".[2] In practice, information infrastructure includes the transmission media; telephone lines, cable television lines and satellites and antennas, and also the routers, aggregators, repeaters and other devices that control transmission paths. Infrastructure also includes the software used to send, receive and manage the signals that are transmitted.[3]

Historically, most of the infrastructures of national importance were physically and geographically segregated. However, with rapid changes

---

1 Peter Westrin, "Critical Information Infrastructure Protection", *Information and Security*, Vol. 7, 2001, p. 69.

2 Ole Hanseth and Kalle Lyytinen, "Theorizing about the Design of Information Infrastructures: Design Kernel Theories and Principles", *Sprouts: Working Papers on Information Systems*, Vol. 4, No. 12, 2004, p. 207, available at http://sprouts.aisnet.org/4-12, accessed on 14 July 2016.

3 "Infrastructure", available at http://searchdatacenter.techtarget.com/definition/infrastructure, accessed on 14 July 2016.

since the 1970s in technology, international market conditions and operational needs, information infrastructure has progressively converged[4] and, at the same time, expanded to the global level. Over the years, automation in the operations and control systems of large industrial and manufacturing facilities has become cost effective as a result of technological developments and penetration of computers. In the twenty-first century, or at the onset of the information age, information infrastructure itself has emerged as one of the most important infrastructures as it forms the very foundation for integration and efficacious management of all other infrastructures as well as new forms of communication, information exchange and commerce.[5]

Tracing the origins of this progression, IT was first introduced to automate the machines, industrial processes and some of the auxiliary business functions such as payrolls. In broader terms, it was considered and perceived to be an agent of automation, quite similar to the function of machines installed by large manufacturing firms during the industrial revolution. The control systems in industries, specifically in large manufacturing units such as chemical or petroleum plants, electrical generation or transmission, began utilizing programmable logical controllers and computers for smooth, reliable and continuous operations.

As the research and development in semiconductor materials and software as an engineering discipline progressed, the size of integrated circuits began to shrink, its computing power increased exponentially and consequently, the market for industry-specific software programmes widened and expanded. Gradually, other management operations, such as sales, marketing and human resources, became geographically spread as industrial operations began expanding across the borders, extending to different time zones. This further enhanced the need of communication systems to coordinate the management of operations, which included exchange of information in real time.

---

4 Peter S. Anderson, "Critical Infrastructure Protection in the Information Age", in Robin Mansell, Rohan Samarajiva and Amy Mahan (eds), *Networking Knowledge for Information Societies: Institutions & Intervention*, The Netherlands: Delft University Press, 2002, p. 188.

5 Ibid.

This transformation led to generation of huge data which, in turn, required IT for management, storage, processing and dissemination of data or information to different stakeholders, partners and vendors. Initially, the applications and programmes were developed for standalone functions, but as the reliance on IT grew, the industrial and business processes began to get integrated. Hence, an information system was initially understood to be just an application of computers developed to help large organizations to process the vast amount of data in order to improve their management of information. Evolving from mainframe computing to the client/server networks and enterprise computing or the cloud computing of today, information systems do not just perform auxiliary functions such as payroll processing but also underpin almost every vital function, be it human resource management, production, project management or business analytics. As the computer technologies have developed and matured over time, their potential applications areas also have increased manifold, and accordingly the role of an information system and the scope of the discipline has widened both horizontally and vertically.

2.1 Information Infrastructure: Characteristics

At an organizational level, the physical elements of the information infrastructure include the location and disposition of network equipment (such as servers, routers and storage media), documents and physical storage devices associated with the organization's own data elements. The logical elements of the information infrastructure are inclusive of electronic information assets, such as the data and information stored across the systems, the operating systems and the various applications an organization has developed and deployed.[6]

Information infrastructure has certain characteristics such as it is "shared" by a community spread across a wide cross-section of users. These users could either be colossal systems like governments or business

---

[6] John P. Pironti, "Key Elements of a Threat and Vulnerability Management Program", *ISACA Journal*, Vol. 3, 2006, p. 2, available at http://www.isaca.org/Journal/Past-Issues/2006/Volume-3/Documents/jpdf0603-Key-Elements.pdf, accessed on 12 October 2016.

houses spread across the globe or an individual user. Information infrastructures evolve over time and the process of their "evolution" continues as more applications are developed and integrated or merged with the existing network. Furthermore, information infrastructure is "open" for participation and development, though it requires "standards" for the ease of integration and interoperability or compatibility of systems. It is also "heterogeneous" because of different kinds or versions of technological and non-technological components, as well as different platforms such as Windows, Linux and Unix. Due to the above-mentioned characteristics, information infrastructure, like other infrastructures, exists in 'layers' or 'strata' which are built upon each other. For instance, the Transmission Control Protocol/Internet Protocol (TCP/IP) service of the Internet is built upon a wide range of basic telecom infrastructures, like ordinary telephone service, mobile phone services and satellite communication; and correspondingly, the email or the Web infrastructures are built upon the TCP/IP-based infrastructure; or likewise, e-commerce infrastructures are further built on top of the email and Web infrastructures.[7]

There are many stakeholders involved in the design, development and maintenance of information infrastructure. No single body, or organization or government can perform all these tasks individually or muster the resources to develop such a massive infrastructure. Therefore, keeping the information infrastructure up and running is a collective effort of multiple actors. Small to large segments of independent infrastructure, when woven into a web of network, manifest in the form of national information infrastructure (NII) and global information infrastructure (GII).

---

[7] Ole Hanseth, "From Systems and Tools to Networks and Infrastructures—From Design to Cultivation: Towards a Design Theory of Information Infrastructures", in Jonny Holmström, Mikael Wiberg and Andreas Lund (eds), *Industrial Informatics Design, Use and Innovation: Perspectives and Services*, Pennsylvania: IGI Global, 2010, p. 122, available at http://heim.ifi.uio.no/~oleha/Publications/ib_ISR_3rd_resubm2.html, accessed on 12 October 2016.

2.2 Defining National and Global Information Infrastructure

Infrastructure can be a subjective term as far as an organization, a segment or department of a government, a nation state or an international organization is concerned. Moving from the micro level to the macro level, the infrastructures keep collating and become an all-encompassing immense system, identified as national and thereupon global information infrastructure.

As per the Australian defence doctrine, the NII is defined as:

> compris[ing] the nation-wide telecommunications networks, computers, databases and electronic systems; it includes the Internet, the public switched networks, public and private networks, cable and wireless, and satellite telecommunications. The NII includes the information resident in networks and systems, the applications and software that allows users to manipulate, organise and digest the information; the value added services; network standards and protocols; encryption processes; and importantly the people who create information, develop applications and services, conduct facilities, and train others to utilise its potential.[8]

Another definition for national infrastructure from the EU refers to NII as:

> physical infrastructure and often also intangible assets and/or to production or communications networks. These definitions are very broad, certainly broader than the notion of infrastructure commonly used in other fields of policy (e.g. the 'essential facility' notion in competition law) and end up including not only the tangible assets, but also the intangibles that run with them (e.g. software, services, etc.).[9]

---

[8] Gary Waters, Desmond Ball and Ian Dudgeon, *Australia and Cyber-warfare*, Canberra: ANU Press, 2008, p. 61, available at http://epress.anu.edu.au/wp-content/uploads/2011/08/ch0420.pdf, accessed on 12 October 2016.

[9] "Critical Infrastructure Protection: Basic Facts and Existing Policies", *Protecting Critical Infrastructure in the EU*, Brussels: Centre For European Policy Studies, 2010, p. 22.

Drawing similar definitions towards the next stratum, the United States (US) Department of Defense defines the concept of GII at the macro level to be:

> the worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact discs, video and audio tape, cable, wire, satellites, fibre optic–optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure.[10]

The following five are the distinct interdependent components in NII and GII:[11]

1. *Hardware* : The computers; physical transmission components such as cable/optical fibre; radio/wireless; satellites; and transmission towers.
2. *Software* : Applications; for example, processes, protocols, encryption and firewalls.
3. *Information* : The databases and information in transit, including voice, facsimile, text messages, imagery or information in other forms.
4. *People* : Human resources who build, operate and maintain the infrastructure.
5. *Power supply* : Hardware and software cannot function and information cannot be transmitted or accessed in the absence of

---

[10] The US Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication No. 1-02, 17 October 2007, available at http://www.dtic.mil/doctrine/ jel/doddict/data/g/02329.html, accessed on 12 October 2016.

[11] n. 8, p. 63.

continuous power supply and it is critical to the functioning of the systems. Specifically, the localized power backup or uninterrupted power systems are part of the components of infrastructure.

The ownership of development and maintenance of the information infrastructure of a nation state is shared by the government and private sector, depending upon the component of the infrastructure and the country-specific policies, market conditions and availability of resources. As an observation, majority of the telecommunications and Internet service providers today are privately owned; and this is common across most of the countries.

In the era of globalization, these services and infrastructure may be largely owned or partly owned by foreign-based multinational corporations. Moreover, majority of the procured software systems, especially operating systems and standard applications or tools and specialized hardware components like microprocessors or integrated circuits, are sourced from foreign corporations.

Furthermore, the skilled human resources who design, develop, maintain and administer the components of networks, or the networks themselves, usually belong to the private sector. The process of globalization has facilitated the access to global markets where the best of the hardware, software, services and people vital to the operations and maintenance of NII and GII are sourced from across the globe.

From the definitions given earlier, it can be derived that the common denominators for both NII and GII are same, which primarily are telecommunications or computer networks, computers, databases and the resident information, software applications, encryption process, standards and protocols and the human resources. However, NII and GII have both the physical aspect, which is generally tangible, as well as the intangible assets in the form of information itself and the policies or practices or guiding principles and the people. The availability, integrity and seamless functioning of infrastructure—not just information infrastructure but the physical infrastructure—is taken for granted. This very assumption and confidence on which the daily human activity, the social interactions, physical movement and operational skeletons of organizations is built brings in the concept of critical infrastructure, which will be discussed in the forthcoming chapters.

Chapter 3

Defining Critical Infrastructure

An infrastructure, as a system, is built up of numerous facilities and enables a specific set of activity for the society. Just as water, oil or gas pipelines enable flow and supply of water or oil from the source to the consumption end and roads, bridges, railway networks and aviation enable movement of people, goods and freight, telecommunication networks built over optical fibres, switches and microwave antennas enable voice and data communication. Interconnected banking operations, network of automated teller machines and other financial or banking services over Internet enable delivery of these services round the clock in every corner of the world. In general, these infrastructures are dependent on other infrastructure to dispense their core functions: for instance, banking system uses telecommunication network to deliver mobile banking or security functions such as one-time password. Similarly, payment systems of railways or civil aviation are dependent on the bank gateways for payments processing. The day-to-day societal functions and requisites, such as water and electricity, banking and financial services, transportation, fuel and food supplies and communications and Internet services, are completely dependent on these multi-layered physical or virtual infrastructures.

An infrastructure performs its defined set of functions as it is conceived to do. However, this assumption might not always hold true and therefore, an infrastructure is deemed to be critical when it is perceived that any disruption in its functioning or core business processes would induce a major socio-economic crisis, with the potential to undermine the stability of the society with dire political or security consequences. The disruption could be a natural hazard, such as a flood or an earthquake, or man-made as a result of an error, miscalculation or a physical or cyber-attack.

As mentioned earlier, society depends on a cross-section of infrastructures for its day-to-day functions, lying within the control and management of both governmental and private entities. The

Department of the Prime Minister and Cabinet of the Australian government defines critical infrastructure as follows:

> physical facilities, supply chains, information technologies and communication networks are deemed critical for the functioning of a nation state, because, if destroyed or degraded, they would impact social and economic well-being or affect the ability to ensure national security.[1]

The Department of Homeland Security of the US government has defined it as:

> physical and cyber-based systems essential to the minimum operations of the economy and government, whose incapacitation or destruction would have debilitating impact on the national security and the economic and social welfare of a state.[2]

The council directive of EU has also defined critical infrastructure as:

> an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.[3]

The term "critical" refers to infrastructure that provides an essential support for economic and social well-being, for public safety and for

---

1 Department of the Prime Minister and Cabinet, Australian Government, *Protecting Australia against Terrorism: Australia's National Counter-terrorism Policy and Arrangements*, Canberra: The Department of the Prime Minister and Cabinet, 2006, p. 45, available at http://www.australianislamistmonitor.org/uploads/docs/paat_2006.pdf, accessed on 15 October 2016.

2 Presidential Decision Directive on Critical Infrastructure Protection, United States, 22 May 1998, available at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm, accessed on 15 October 2016.

3 The Council of the EU, "Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection", *Official Journal of the European Union*, p. 77, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= OJ:L:2008:345:0075:0082:EN:PDF, accessed on 12 October 2016.

the functioning of key government responsibilities, such that disruption or destruction of the infrastructure would result in catastrophic and far-reaching damage.[4] Therefore, critical infrastructure is composed of the basic services on which nation states have developed dependency, and they are necessary to support the society, economy and to ensure national stability. The loss, damage, unavailability, though for a short duration, can have significant consequences and cascading effects far beyond the targeted sector and physical location of the incident.

The critical national infrastructure has been defined by the Government of United Kingdom (UK) as:[5]

> those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) major detrimental impact on the availability, integrity or delivery of essential services—including those services, whose integrity, if compromised, could result in significant loss of life or casualties—taking into account significant economic or social impacts; and/or b) significant impact on national security, national defence, or the functioning of the state.

The definition of critical infrastructure varies from country to country and is fluid, as the definition and list of infrastructures deemed to be critical have changed or matured over the time.[6] The executive order

---

4 "Critical Infrastructure Protection: Basic Facts and Existing Policies", *Protecting Critical Infrastructure in the EU*, Brussels: Centre For European Policy Studies, 2010, p. 22.

5 Centre for the Protection of National Infrastructure (CPNI), "Critical National Infrastructure", available at http://www.cpni.gov.uk/about/cni/, accessed on 12 October 2016.

6 The approach to identify critical infrastructures is pragmatic when attributes are enlisted or characteristics are enlisted with change in time. For instance, the general definition of what constitutes a critical infrastructure has expanded from those vital to the nation's defence and economic security and continuity of government to include those vital to public health and safety. Without a rigorous process for identifying critical infrastructure, the list may keep changing or growing.

of the President of the US which established the Commission on Critical Infrastructure Protection in 1996 included the following as critical infrastructure:[7] telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire and rescue); and continuity of governance.

Table 3.1: Summary of Critical Infrastructure Sectors

Sector	US	Australia	UK	EU	China	India
Power/Energy	✓	✓	✓	✓	✓	✓
ICT/ Communications	✓	✓	✓	✓	✓	✓
Finance/Banking	✓	✓	✓	✓	✓	✓
Public Health	✓	✓	✓	✓	✓	
Food/Agriculture	✓	✓	✓	✓		
Water	✓	✓	✓	✓	✓	
Transport	✓	✓	✓	✓	✓	✓
e-governance	✓		✓	✓	✓	✓
Defence Industries	✓					
Emergency Services	✓		✓			
Other Sectors	National Monuments and Icons, Critical Manufacturing	National Icons			Industrial Manufacturing, Education and Scientific Research.	

***Source*:** Format taken from *Protecting Critical Infrastructure in the EU*, Brussels: Centre for European Policy Studies, 2010. Information is derived from various primary sources.

---

[7] John Moteff, Claudia Copeland and John Fischer, "Critical Infrastructures: What Makes an Infrastructure Critical", Congressional Research Service Report for Congress, No. RL31556, 2003, p. 8, available at http://www.fas.org/irp/crs/RL31556.pdf, accessed on 12 October 2016.

The current list of the Department of Homeland Security has been extended to 18 sectors now, adding critical manufacturing, IT, public health and defence industrial base.[8]

Table 3.1 summarises the sectors part of the critical infrastructure as identified by the US, UK, Australia, EU, China and India.

Since the definitions and scope of critical infrastructure vary from country to country, so does the degree of dependency of different sectors on information infrastructure. For instance, food and agriculture, as an independent sector, does not find a mention in the case of India, but the US, Australia, the UK and the EU find this sector to be critical. For the UK and the US, national monuments and icons are part of critical infrastructure. Similarly, defence industrial base, or emergency services or chemical industries form a part of critical infrastructure for some of the countries, but not for all of them. China considers education and scientific research to be part of its critical infrastructure. It is quite evident that there are differing perceptions and therefore, different scope of the term critical infrastructure.

Going forward, even if the scope widens, there might not be a universally accepted definition or a well-defined scope. However, maintaining social and economic well-being and ensuring national security and public safety will remain the underlying principles or core of the concept of critical infrastructure. As discussed earlier, critical infrastructures, in their respective country and capacity, have certain degree of dependency on the information infrastructure. The critical infrastructures rely on a spectrum of software-based control systems or information systems for seamless and reliable operations. Therefore, ICT has not just become omnipresent but it also connects infrastructure systems, subsystems and constituents in such a manner that they have subsequently become highly interrelated and interdependent.

---

[8] US Department of Homeland Security, "Critical Infrastructure Sectors", available at http://www.dhs.gov/files/programs/gc_1189168948944.shtm, accessed on 18 July 2016.

Chapter 4

Critical Information Infrastructure (CII)

Information technology, itself as an infrastructure, has become an integral part of the critical infrastructure of a nation state. Therefore, critical infrastructure is dependent on telecommunications—the public telephone network, or the Internet or satellite wireless networks—and the associated computing assets—computers, networks and networking equipment, servers, storage, etc.—for a host of functions pertaining to information management, processing, dissemination and the wider communications objectives. Notably, this dependence has a national security component as well, since information infrastructure undergirds and enables both economic vitality and military and civilian government operations. Hence, the part of the information infrastructure that is essential for the continuity of critical infrastructure services is known as critical information infrastructure (CII). Principally, CII is part of critical infrastructure of a nation state and includes components such as computers, software, the Internet, satellites and fibre optics.[1]

Critical information infrastructure generally refers to:

> Information and Communication Technology systems that are essential to the operations of national and international Critical Infrastructures. Some of the examples include i) telecommunication networks; ii) transportation: air traffic control, railway routing and control, highway or city traffic

---

[1] Myriam Dunn Cavelty, "Critical Information Infrastructure: Vulnerabilities, Threats and Responses", *ICTs and International Security* No. 3, 2007, p. 16, available at http://www.unidir.ch/pdf/articles/pdf-art2643.pdf, accessed on 13 July 2016.

> management; iii) financial services: credit card transactions, online payment systems or gateways, electronic stock trading; and iv) Industrial Control Systems/SCADA (Supervisory, Control and Data Acquisition) used to manage energy production and distribution, chemical manufacturing and refining processes.[2]

Similar to critical infrastructure, CII also has a plethora of definitions, appearing in governmental policy documents, legislations or strategy documents and reports from private enterprises in the information/cyber security domain. Symantec Corporation, in its Critical Infrastructure Protection Study in 2010, had characterized CII as "businesses and industries whose importance is such that if their cyber networks were successfully breached and disabled, it could result in a threat to national security."[3]

Critical information infrastructure is communications or information service whose availability, reliability and resilience are essential to the functioning of a modern economy, security and other essential social values. The CIIs are needed to support the functioning of other critical infrastructures, ranging from power distribution to transportation and finance to governance.

In India, Section 70 of the IT (Amendment) Act, 2008 (Ministry of Information Technology, Government of India [GoI]) describes CII as "the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."[4] The IT Act was amended in 2008 to expand the scope of

---

2 "Critical Infrastructure Protection: Basic Facts and Existing Policies", *Protecting Critical Infrastructure in the EU*, Brussels: Centre For European Policy Studies, 2010, p. 24.

3 "Symantec 2010 Critical Infrastructure Protection Study", 5 October 2010, available at http://www.slideshare.net/symantec/symantec-2010-critical-infrastructure-protection-study, accessed on 13 July 2016.

4 Ministry of Law and Justice, GoI, "The Information Technology (Amendment) Act, 2008", 05 February 2009, pp. 13–14, available at http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf, accessed on 13 July 2016.

the existing legal framework, and the broadened scope included defining CII and designating a nodal agency and its roles and responsibilities for the protection of CII. The act designated any computer resource which directly or indirectly affects the facility of CII to be a protected system. The scope of CII is very wide and it becomes extremely challenging to identify the computer resources supporting the functioning of CII. Moreover, tools, techniques and frameworks for quantitative assessment of the impact of CII disruptions and degradation on national security, economy, public health or safety are inadequate.

In the beginning of the discourse on critical infrastructure in India, the Department of Electronics and Information Technology (GoI) had identified defence, finance, energy, transportation and telecommunications as the critical sectors.[5] With the inception of a designated nodal agency—the National Critical Information Infrastructure Protection Centre (NCIIPC)—to protect the CII of India, the sectors that were put under the auspices of the agency are power and energy (oil and gas, power, industrial control systems, etc.), banking, financial services and insurance, ICT, transportation (air, surface [rail and road] and water) and e-governance and strategic public enterprises.[6] These sectors can be further subdivided into independent business or industrial functions: for example, in the case of transportation; aviation, shipping, road and rail are the primary constituents. Similarly, the subdivision of services, such as telecommunications has landline voice services, mobile voice services and broadband cable services. The CII sectors in perspective and their sector-wise break up is given in Table 4.1.

---

5 Department of Electronics and Information Technology, GoI, "Strategic Approach for Cyber Security", available at http://deity.gov.in/content/strategic-approach, accessed on 22 July 2016.

6 NCIIPC, "Sectors in NCIIPC", available at https://nciipc.gov.in/?p=sector, accessed on 22 November 2016.

Table 4.1: Critical Infrastructure Sectors in India

1. Civil Aviation 2. Railways 3. Shipping	1. Thermal Power 2. Hydroelectric Power 3. Nuclear Power 4. Petroleum/ Natural Gas 5. Power Grid 6. Refineries	1. PSTN Network 2. Satellite Communication 3. Network Backbone 4. Mobile Telephony 5. Broadcasting	1. Reserve Bank of India 2. Stock Exchanges 3. Banking 4. Clearing Houses 5. Payment Gateways	1. NIC 2. e-Governance Infrastructure
Transpo-rtation	Power and Energy	Information and Communications Technology	Banking, Financial Services and Insurance	e-Governance and Strategic Public Enterprises

Source: Compiled by the author.

In essence, there are certain common criteria which reflect across the different definitions or varying perspectives on the constituents of critical infrastructure. First, there exists a computer resource, upon which other physical systems or processes are dependent, and this computer resource, if compromised or incapacitated, would cause widespread damage, which might have severe consequences. For instance, a malfunctioning automated meter or valve in the critical control system of a chemical processing plant may display incorrect parameters, or quite possibly trigger a release or contraction of the valve, taking the shape of an accident bearing physical consequences. This control system, which takes care of a critical process in the plant, has a computer resource which monitors the gauged physical parameters and executes a predefined or programmed industrial function.

Second, the operational stability and security of CII is vital for national and economic security of the nation state. The IT infrastructure provides the processing, transmission and storage of vital information, and also enables government agencies to rapidly interact with each other as well

as with industry, citizens, state and local governments and the governments of other nations.[7] Many of the critical services that are essential to the well-being of the economy are increasingly becoming dependent on IT.

Governmental institutions across the globe have been making efforts to identify the core services that need to be protected. In this regard, they have been consistently working with organizations responsible for operationalizing, maintaining and operating critical infrastructure. The primary focus of these efforts has been to secure the information resources belonging to the government as well as those key organizations which are an integral part of the nation states' critical sectors.[8] The unprecedented dependence of modern societies and nation states on CIIs, their interconnectedness and interdependencies with other infrastructure, sometimes across the physical or political borders, as well as the underlying vulnerabilities and the threats of exploitation they face elevates the requisites to strengthen the security of CII and inculcate resilience.

In both conceptual and operational terms, CI and CII are engrained to each other. Figure 4.1 pictorially represents the scope of Critical Infrastructure and Critical Information Infrastructure Protection. However, operationally there may not be such distinctions, and the figure is just indicative to explain the concepts governing the identification of CI and CII.

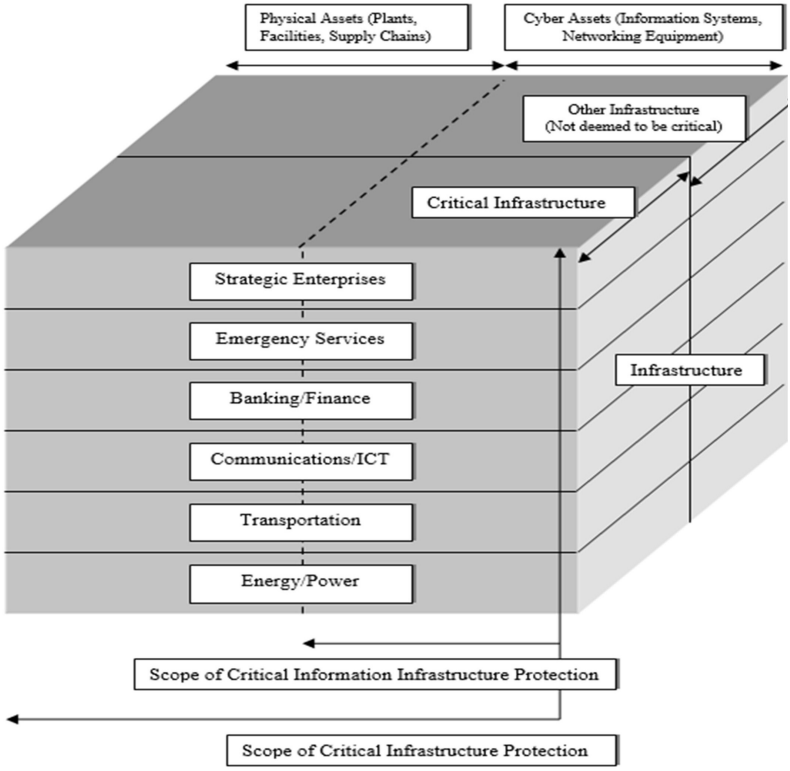
As the critical infrastructures of a nation state are becoming integrated and gaining strategic advantage, there is a growing insecurity among the nation states on the issues pertaining to the protection and defence of these infrastructures. There has been a significant increase in the number of cyber-attacks, and this has been established from reports published by security agencies and private security firms.

---

7 Department of Electronics and Information Technology, GoI, "Overview on Cyber Security Strategy", available at http://deity.gov.in/content/overview, accessed on 15 July 2016.

8 Ibid.

Figure 4.1: Pictorial Representation of the Scope of Critical Infrastructure Protection and Critical Information Infrastructure Protection



***Source*:** Prepared by the author.

The cyber threats, particularly categorized as cyber-crime, cyber terrorism, cyber espionage and cyber warfare, exploit numerous vulnerabilities in the software and hardware design, human resources and physical systems. This concern has gained significant traction among governmental agencies, computer/network security firms and the scientific and strategic community. There is a dire need to evolve a comprehensive security policy to address the physical, legal, cyber and human dimensions of security. Nation states across the globe have realized the growing challenges in preventing and containing the attacks on critical infrastructure, while ingraining resiliency in the critical infrastructure and the corresponding information infrastructure.

4.1 The Element of Criticality in CII

Critical infrastructure, by virtue of its structural evolution, is a highly complex, heterogeneous and interdependent infusion of facilities, systems and functions that are extremely vulnerable to a wide variety of threats. Given the immense size and scope of this vast potential target set, it is absolutely infeasible to completely protect all the assets at all times, against all conceivable threats, through all probable threat vectors.[9] It is essential to demarcate between critical assets and non-critical assets in order to gain a clear picture of the impact of failures, disruptions and analysis of risk with respect to the business functions, depending on the importance of the asset to the core mission of the enterprise. In other words, if called as criticality assessment, the purpose of the exercise is to compute the relative importance of the assets, as a derivative of various factors such as their function, risk exposure and significance in terms of enterprise security, economic security, public safety or any other criterion laid out. Ted G. Lewis is credited with a significant study in this regard, on critical infrastructure using critical node analysis utilizing the principles of network theory.[10] Due to the complexity of interactions among the components of infrastructure as well as within the infrastructure sectors, computer-based modelling of each sector and interdependencies among sectors could help solve many of the practical constraints. Such an exercise based on quantitative methods is essential as it assists the policymakers in allocating or prioritizing their limited resources to the security of the most important assets.

By definition, criticality assessment of an asset is:

> the estimation of its relative importance as compared to other assets, and in concept, it is based upon a wide variety of factors, such as the mission or function it performs; the extent to which

---

[9] John Sullivant, *Strategies for Protecting National Critical Infrastructure Assets: A Focus on Problem-solving*, New Jersey: John Wiley and Sons, 2007, p. 111.

[10] Ted G. Lewis, *Critical Information Infrastructure Protection in Homeland Security: Defending a Networked Nation*, New Jersey: John Wiley and Sons, 2006, pp. 60–61.

> systems, functions, facilities, and resources are at risk if the asset does not meet its desired functionality; and significance in terms of enterprise security, economic security, or public safety at large.[11]

Criticality assessment is important because it aids the practitioners, based on the factors, in prioritizing the security of those assets that require elevated protection, given the finite resources and budgetary constraints.[12]

John Sullivant describes the process of determining the criticality of an asset as four-dimensional,[13] where the first dimension reflects the "enterprise perspective", which underscores the importance of the asset to the enterprise itself and its customer base. The basic questions in this exercise pertain to the dependency of core mission or key business processes on the asset and the difficulty in restoring the services in the case of damage or disablement. The second dimension envelopes "vulnerability of the asset" and deliberates on redundancy built up with the asset and its access. Criticality assessment further covers the third dimension, the "attractiveness to the adversary", given the importance and vulnerability of the asset, based on questions regarding the perceived value of the asset to the adversary. The fourth dimension, and the most difficult to assess, is the "public reaction" when public safety is endangered and the adverse effect on society, either in the form of deteriorating public confidence, the behaviour of stock markets or financial sector and the open issues of liability.

In principle, criticality assessment is generally carried out in every department or unit of an organization in some way or the other, though it may or may not be in detail. However, when the organization is part of the critical infrastructure of a nation state, either perceived or designated as, its critical assets need to be assessed in a conscientious manner. While figuring out the answers to the process of determining the criticality, the analysts have to assess under a defined framework or

---

[11] n. 9, p. 63.

[12] Ibid.

[13] n. 9, pp. 113–14.

a set of parameters. Defining and drawing on these parameters could be the jurisdiction of the organization or the sector it belongs to, or there could be nationally agreed upon parameters to conduct the criticality assessment as part of a regulatory framework.

4.1.1 Parameters of Criticality

The criticality of an asset or an industrial function is dependent upon a range of factors, such as the duration of loss of service or equipment, availability of alternatives to execute the same function or the time taken to bring back the service into functioning. Therefore, the resilience of an industrial function, or a business process or an asset, to the instances of disruption and degradation increases when the substitutes which can promptly restore the services to normalcy are readily available. Service disruptions or equipment degradation can culminate into cascades of failure if other business functions are highly dependent on the outputs of the given system.[14] This is the characteristic which brings in the element of criticality. Industrial functions, at the micro level, have certain degrees of dependence on other functions, whether they are upstream or downstream in the chain. Owing to certain characteristics, and to the specific functions they perform, their degree or magnitude of criticality varies. The parameters given in Table 4.2 contribute towards the criticality of an asset, an industrial function or probably for an infrastructure. However, this list is indicative, and there may be additional parameters subjective to the specific case under consideration.

There are additional parameters which could contribute towards the criticality, such as the moment of failure, because the criticality of an infrastructure could also vary with time as at a specific time of the day or under specific circumstances, its criticality is higher. This specific aspect has not been addressed in the research and the time factor has been kept out of scope of the study.

---

[14] US Department of Homeland Security, "Information Technology: Critical Infrastructure and Key Resources Sector-specific Plan as Input to the National Infrastructure Protection Plan", May 2007, available at http://www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf, accessed on 20 July 2016.

Table 4.2: Criticality Parameters

Criticality	Redundancy/Alternative
	Threshold Mean Time to Restore (MTTR)
	Impact Severity/Degree
	Probability
	Impact Type
	Interdependency
	ICT Dependency

***Source*:** Compiled by the author.

The key principle to ensure availability of a function or asset is to build in "redundancy". A redundant function or asset, even if disrupted, is less likely to impact the mission-critical processes, while a function without redundancy becomes critical and, at the same time, vulnerable. Redundancy, as part of the design has become the key principle to ensure availability of the services under all circumstances. Moving forward, the assets or services with high "duration of failure" or higher "mean time to restore" are undoubtedly critical as they require more time for restoration to normalcy. Their higher downtime between service restoration, or time required for reinstating business continuity, make them a point of vulnerability. The assets or services which have high degree of "impact or severity" also contribute more towards criticality. An asset whose disruption, loss or unavailability could significantly disrupt, or for that matter even cease, the operations of the entire facility/industry/infrastructure gains higher on criticality as the consequences could be catastrophic. While assessing the criticality of infrastructure, this parameter could also be quantified in terms of percentage of population affected or percentage of services impacted, or the number of causalities or the number of users impacted. As a parameter, impact could be further segregated into factors based upon the definitions of CII laid down by various governments, where emphasis is on the impact over societal functions, public health and safety, national security and economic or social well-being of the people.

"Probability" or the "likelihood" of disruption is also a determining factor, but the assessment would require several experts to assess the

impact and probability of failure of core business functions. The approach is quite similar to risk assessment where probability/likelihood for an accident or failure is combined with the estimation of negative consequences. The "dependence" of various business functions on ICT increases their vulnerability and exposure to the threats hovering in cyberspace. The disruption of information infrastructure and related services can have catastrophic consequences on the very execution of core business functions of critical infrastructure, and the higher dependence on such services and assets adds to the criticality.

The complex interactions among various industrial functions of critical infrastructure and the exchange of information leads to "interdependencies", which is the most significant and yet the most complicated parameter of criticality. These interdependencies vary from geographical to physical and cyber to logical. A minor disruption at one point could have a rippling effect across multiple infrastructures.

In addition to these parameters, while comprehending the parameters of criticality for infrastructure at large, there are certain observations from definitions which need attention. It is evident from the definitions that critical infrastructures, as entities, have clear implications for national, economic and environmental security. These dimensions must be understood and reflected upon when the assessments for designating critical infrastructure are made.

In principle, national security could encompass economic security, energy security, food security, political security, military security, environmental security and so on. A workable definition could be "the ability of a nation state or its institutions to prevent adversaries from undermining the national interest or the confidence in the capability of the nation state, maintenance of territorial and political integrity while preserving the fundamental rights of the citizens". In the information age, along with foreign and domestic components of national security, information security has also become an important dimension of national security.[15] On similar lines, the term economic security for a

---

[15] Sam C. Sarkesian, John Allen Williams and Stephen J. Cimbala, *US National Security: Policymakers, Processes & Politics*, Boulder: Lynne Rienner Publishers, 2008, pp. 2–5, available at https://www.rienner.com/uploads/47e148fd47a65.pdf, accessed on 22 September 2016.

nation state could be anything related to the aspects of production, distribution and consumption of goods and services and can be possibly defined as "the state's ability to meet, on a sustained basis, the material aspirations of its citizens" and protect the citizens from domestic and global threats which could undermine these aspects.[16]

Since the delivery of governance is reliant on ICT, e-governance policies and programmes are implemented across the globe for efficiency, reach and cost effectiveness. A disruption may impact or impair the ability of a government to deliver these vital services such as passport, consular and visa services, water and electricity management or income tax filings. Moreover, a data breach may compromise personal information of the citizens.

The growing concerns over environmental change and degradation, and its interactions with geography and geopolitics, have elevated its imperatives for the safety and security of human life. The prevalence of control systems for waste management and treatment and industrial plants for chemical processing (some of them are toxic with known hazards) are also a risk to the environmental security. This aspect has further implications for public health and safety.

It must be noted that the parameters defined here are indicative and not definitive. Moreover, it is not necessary that all of them are applicable to the case under consideration. There may be more parameters which are relevant for certain organizations. The basic aim of defining the criticality parameters is to facilitate or present the broader principles which have utility in undertaking an organization-wide exercise to identify the assets vital to the critical business or industrial processes or nation-wide exercises for critical infrastructure/CII assessment. However, at the organizational level, the exercise begins with identification of cyber assets before computing their relative importance in terms of criticality.

---

[16] Jayanta Roy, "India's Economic Security", *The Financial Express* (New Delhi), 26 November 2007, available at http://www.financialexpress.com/news/indias-economic-security/243291, accessed on 22 September 2016.

4.1.2 Cyber Asset Identification

In general, cyber assets could be part of either the control systems, data acquisition systems or the networking equipment used by any of the control or data acquisition system. Control systems primarily comprise of the devices or sets of devices that manage, command or regulate the behaviour/parameters of processes, devices or other systems. Data acquisition systems are a collation of sensing/reading/monitoring devices and communication links that sample, collect or provide data from the designated system to a centralized database/location or a human–machine interface for display, archiving or further processing. The networking equipment includes myriad of devices such as routers, hubs, switches and modems.

In order to identify cyber assets within the perimeters, their respective roles and functions undergo review and assessment is made to gauge the impact on the essential business or industrial functions, which could be one or a combination of the following:[17]

1. The asset may provide operational information in the real time.
2. The asset controls parameters of industrial processes, which could either be manual intervention or through an automated function.
3. It performs some critical functions such as it prompts errors, raises alarms, flags or alerts for further action or human intervention.
4. The asset may provide data connectivity between cyber assets within the electronic security perimeter.
5. The asset supports the operations or the business continuity plans.[18]

Once the exercise of identifying cyber assets is complete, the next step is to identify those cyber assets which underpin or support the critical assets/business processes/industrial functions, known as critical cyber

---

[17] North American Electric Reliability Corporation, "Critical Cyber Asset Identification - NERC Standard CIP-002 R3", p. 6.

[18] Ibid.

assets. Again, the criteria could be subjective, but in broader terms, they could be:

1. The cyber asset is involved in or capable of or executes supervisory or autonomous control that enables an essential function of a critical asset.
2. The cyber asset displays, transfers, processes or contains/stores information, which is used to make operational decisions in real time, regarding an essential function of a critical asset.
3. The cyber asset, if lost/compromised/unavailable, would severely degrade/disable/incapacitate the critical asset to deliver its essential functions.[19]

The critical asset elements which may further help in identifying critical assets are given in Table 4.3.[20]

Every organization or its independent departments or business units conduct similar exercises as part of their risk assessment activities. However, it becomes vital for organizations that are part of the national critical infrastructure to proactively and periodically conduct this exercise. Nevertheless, few organizations have understood the myriad or web of interdependencies, which inadvertently shape their risk exposure. The disruptions in one of the sectors might have unforeseen impact on other sectors, and therefore it is essential to detangle the web of interdependencies for better preparedness.

---

19 n. 17, pp. 7-8.

20 Critical Infrastructure Assurance Office of the US Department of Commerce, "Practices for Securing Critical Information Assets", p. 19, available at http://www.infragard.net/library/pdfs/securing_critical_assets.pdf, accessed on 22 September 2016.

Table 4.3. Critical Asset Elements and Description

Critical Asset Elements	Description
Human Resources	Includes staff, management and executives who are deemed to be necessary to plan, organize, acquire, deliver, support and monitor mission-critical/core services, information systems and facilities. This may also include the groups or individuals external to the organization but involved in the executing mission-critical/core services.
Automated Information and Control Systems	This category encompasses entire electronic and telecommunications equipment, hardware, and software (including operating systems, communications and applications), security countermeasures and engrained safeguards that are part of critical assets, or in some way or the other support critical assets/mission-critical services.
Data	Entire data belonging to the organization (both in electronic and print form) and information that is part of or which supports critical assets and mission-critical services. The inclusions are disparate electronic or printed records, collected/stored data, images, as well as other means of storing information (assessments by human resources or the inputs into a computer either for storage or/and processing) and digital transmission.
Facilities and Equipment	All facilities and equipment that form part of or support critical assets/mission-critical services, especially those that house and support IT assets.

***Source*:** Critical Infrastructure Assurance Office, Practices for Securing Critical Information Assets, p. 19, available at http://www.infragard.net/library/pdfs/securing_critical_assets.pdf.

4.2 Understanding Interdependencies

The potential vulnerabilities of an integrated infrastructure system are compounded by the interdependence of various constituents. As the complexity of networks increases, and the number of attacks on these networks surge, an impact even due to a small disruption could be severe. The defence and protection strategy warrants the governments to have credible and sufficient knowledge or awareness of their critical infrastructure, and the information infrastructure which is vital to the healthy functioning of these infrastructures and their interdependencies. This poses significant challenges before governmental agencies in terms of identifying, understanding and analyzing such interdependencies, which are spread across the globe (within or outside national boundaries) and interlinked through complex topologies.

In the present scenario, information infrastructure is increasingly interlinked with nearly all other infrastructures, which includes both critical and non-critical infrastructure, where isolating or segregating critical segments from non-critical infrastructure in the dynamic ecosystem still remains a daunting task. As the interactions amongst critical infrastructure increase, the interdependency[21] between various elements is an important factor in criticality analysis. Complexity of infrastructures and their interdependency leads to elevated risk exposure. Critical infrastructures depend on inputs/outputs of each other for physical commodities, data, information, energy and so on. Disruption or degradation of cyber elements can also have physical consequences. In the context of critical infrastructure, interdependency could be defined as "a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other."[22] In other words, two infrastructures are interdependent when each is dependent on the other. For instance,

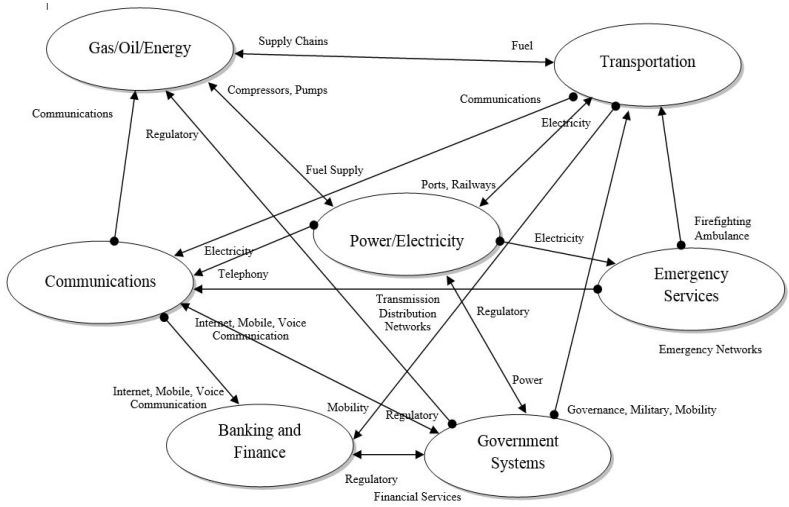
---

[21] Infrastructure *i* depends on *j* through some links, and when its bidirectional, *j* likewise depends on *i* through other links. This is termed as interdependency.

[22] Steven M. Rinaldi, James P. Peerenboom and Terrence K. Kelly, "Identifying, Understanding and Analyzing Critical Infrastructure Dependency", *IEEE Control Systems Magazine*, Vol. 21, No. 6, 2001, p. 14, available at http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf, accessed on 04 July 2016.

thermal power plants depend upon the railway systems for their coal supply, which is a vital input to the power plants. On the other hand, the produced power is critical to the functioning of railways, so these two infrastructures are interdependent. Similarly, the petroleum supply chain (both crude and refined) is dependent upon road, rail and sea ways. Entire road transportation systems and parts of railway systems are fuelled by petroleum products, adding up to interdependency between both.

Figure 4.2: Representing Interdependency among Critical Sectors



***Source*:** Prepared by the author with inputs from http://www.rbtxllc.com/energy-industry.html.

Interdependency among critical infrastructure sectors is depicted in Figure 4.2. All the critical sectors, such as transportation, communications and government services, depend upon the power/electricity sector for their basic requirement of electricity supply, which powers the railways, airports and communication systems such as switching centres or telephone exchanges. In an interdependent function, the power/electricity sector itself depends on transportation for fuel supplies and communications for its data transmission or to maintain health of the transmission/distribution networks. Similarly, governments depend on the banking and financial services for all monetary needs. The banking sector is technology driven, and communications sector plays a pivotal role in seamless banking operations.

The depiction in the figure is just indicative and does not represent the complexity of the relationship. It does represent the direct relationship between two sectors, such as transportation and the power/electricity sector, but it is inadequate to define the characteristics of the relationship. For analysis, interdependency could only be expressed in the form of mathematical models, which can identify all the linkages, as well as assign a degree or measure of dependency to assess the characteristics of the interdependent business function.

4.3 Detangling Interdependencies

The challenge of complexity in the study of critical infrastructure, as a result of the underlying interdependencies, is fundamentally derived from both organizational and technical complexities. According to Ted Lewis, there is dearth of specialized tools and techniques to model these complex infrastructures, comprehend their interdependencies, analyze their vulnerabilities and find the optimal means of their protection.[23] He stresses on the need of quantitative methods to scientifically compute the optimal allocation of limited resources to the most important assets of each sector of critical infrastructures. Such tools must operate at the local, state, regional and national levels.[24]

Given the complexity involved in interdependencies, there are only a few research efforts in the quest of investigating infrastructure interdependencies; simulate the cascading effects due to disruptions in a segment of the critical infrastructure; and mathematically assess their impact. The understanding of the potential damage and socio-economic impacts of such disruptions is limited. Due to the intricacies of interdependence, so far this field has been studied from an organizational perspective, analyzing critical infrastructures as physical assets[25] and not

---

[23] n. 10, pp. 60–61.

[24] Ibid.

[25] Fabio Bisogni and Simona Cavallini, "Assessing the Economic Loss and Social Impact of Information System Breakdowns", in Tyler Moore and Sujeet Shenoi (eds), *Critical Infrastructure Protection IV, Fourth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, Washington, DC: Springer, 2010, pp. 186–187.

as a stratified web or network of interdependent and closely knit system of systems. The studies are generally carried out at the organizational level for risk assessment, which provides credible inputs to the decision makers, but is futile for the policymakers whose task is to enhance preparedness and infrastructure resilience at national level.

The efforts are primarily concentrated in the area of dependency analysis to understand the intricate web of dependencies between cyber assets and physical infrastructures. The interdependence between the infrastructures is fundamental to the propagation of threats among them.[26] Some of the analysts have focused upon the coupling between different sectors of critical infrastructure, such as physical coupling, logical and information coupling, inter-regional economic coupling and inter-sector economic coupling, which broadly explains the interdependence of infrastructure when they behave as a network.[27]

For the purpose of simplification, the interdependencies can be divided into four principle classes:[28]

1. *Geographical* : When two or more infrastructure facilities exist in same geographic location and disruption/destruction of one has impact on other, it is understood to have a geographical interdependency. In other terms, a geographic interdependency occurs when elements of multiple infrastructures are in close spatial proximity, which could lead to disturbances in other infrastructure as a result of disruption in one. For instance, a case of fire in one infrastructure can have negative consequences for geographically interdependent infrastructures.

---

[26] Jason Kopylec, Anita D'Amico and John Goodall, "Visualizing Cascading Failures in Critical Cyber Infrastructures", in Eric Goetz and Sujeet Shenoi (eds), *Critical Infrastructure Protection*, New York: Springer, 2008, pp. 351–362.

[27] Yacov Haimes, Joost Santos, Kenneth Crowther, Matthew Henry, Chenyang Lian and Zhenyu Yan, "Risk Analysis in Interdependent Infrastructures", in Eric Goetz and Sujeet Shenoi (eds), *Critical Infrastructure Protection*, n. 26, pp. 297–310.

[28] Ibid.

2. *Physical* : In case of physical interdependency, the state of each is dependent on the material or output(s) of the other. A physical entity or object is passed on from one infrastructure to the other. For instance, thermal power plants are dependent on railways for coal supplies and disruption in services of railways can block the supply chain which would have severe consequences for the operations. On the other hand, shortage of power as a result of supply chain blockage could lead to unavailability of electricity for railways operations or other infrastructure, such as banking, industries and telecommunications.

   To elaborate, physical interdependency arises from a physical linkage between the inputs and outputs of two entities where a commodity produced or modified by one infrastructure (an output) is required by another infrastructure for it to operate (an input). Physical interdependencies could include transmission of electricity through transmission and distribution networks to the consumption end; supplies of water/natural gas/petroleum through a network of distribution channels to the points of consumption; materials or physical entities from one process to another or from one facility to another over pipeline or other modes of transport.[29] However, a disruption in the supply or availability of entities in the case of physical couplings can render multiple systems inoperable if the hubs of the network are disrupted.

3. *Information* : If the state of a function depends on information transmitted through information infrastructure, the relationship can be classified as information dependency. In this case, the commodity passed on is information. These interdependencies occur due to the connection between infrastructures via electronic/digital or informational links. Going forward, nation states will be more dependent upon their NII and it will become too difficult to assess the risk associated due to the breadth and complexity of the networks.

---

[29] Ibid., p. 299.

4. *Logical* : When the state of an infrastructure depends upon the other, though it is none of the dependency relationships mentioned earlier (geographical, physical or cyber); and yet, there is a relationship, it could be termed as logical dependency. For instance, impact of failure or poor performance of stock market-enlisted corporations on their respective stock prices (which in turn guides the stock market indices) is a kind of logical interdependency.

Given the interplay of dependencies and interdependencies, the infrastructures are bound to interact with each other, and these interactions may take the shape of linearity or complexity. In a mesh or network of infrastructures, a set of two infrastructures could either be directly connected or there could be an indirect coupling between the two through single or multiple intervening infrastructures. Linear interactions are quite visible, expected and known or apparent, and subsequently their sequences or linkages are familiar. Complex interactions, on the other hand, are outcomes of unexpected sequences, unfamiliar therefore invisible and unplanned, and at the worst, they may not be visible or immediately comprehensible.[30]

4.4 Failure Impact: Interplay of Interdependencies

The understanding of CII interlinkages and interdependencies should be based upon the analysis of failure in an interactive system (not just in isolation). The failure is to be analyzed not only with a single element but also its consequences on the wider system and impacts on other identified critical infrastructures. The entire ecosystem of critical infrastructure is decentralized, interconnected and interdependent; controlled by multiple actors (both government and private sector); and inducts diverse types of technologies. Furthermore, the infrastructures and their operational characteristics are strongly influenced by the degree of linkage, which is either flexible or stern. If it is stern, there is little or no flexibility for the system to respond to the changing conditions or sudden failures that can exacerbate problems or cascade from one infrastructure to another. Infrastructures are frequently connected at multiple points through a wide variety of

---

[30] n. 22, p. 19.

mechanisms, such that a bidirectional relationship exists between the states of any given pair of infrastructures. Failures in critical infrastructure can be classified into four major categories.[31]

A failure takes the shape of a cascade, also known as a "cascading failure", when a disruption at one infrastructure leads to the failure of a component in a second infrastructure and consequently, this failure causes a disruption in the third infrastructure. This chain of events, taking the shape of cascades, one after another, happens due to the interlinked infrastructures, and the impact of disruptions in the upstream system is carried forward to the systems or infrastructures at the downstream or further ahead connected in the network. Slightly different, but more perilous is the case of an "escalating failure", where disruption in one infrastructure aggravates an independent disruption of another infrastructure, which increases the severity or the time for recovery or restoration of the services as the failure traverses ahead. Since this kind of failure compounds the impact of failure, downstream systems face more severe consequences as compared to upstream systems. A "dampening failure impact" can be defined as the one when disruption in one infrastructure does not cascade or escalate to other sectors and the impact is reduced in intensity. A "common cause or distributed failure impact" occurs when two or more infrastructure networks are disrupted at the same time: components within each network fail because of some common cause, due to same root cause or physical proximity of infrastructure.

It is noteworthy that the components or the constituent sectors/industries/facilities of critical infrastructure are essential primarily due to their position within the colossal network comprising of the critical infrastructure themselves as the nodes and their relationships or dependencies as the links. In practice, none of the functions of these infrastructure components is in isolation. Their activities, outputs, products, processes are not just dependent on others, but they tend to play a vital role in ensuring the functioning of other components dependent on them. This phenomenon—of a networked relation of dependencies and interdependencies—gives rise to a vast collation of

---

[31] n. 22, pp. 22–23.

direct and indirect relationships, which, if expressed in terms of computer science, behaves as a network of networks. The next section contemplates on this property of critical infrastructure and their information infrastructure.

4.5 Critical Infrastructure Systems as Networks

The behavioural characteristics of critical infrastructure have paradoxical evidences, an architectural or structural challenge from a technical perspective. Such as, a robust system is often not resilient to failures or disruptions. A technically dependable or hardened system may not have optimal operational efficiency. Optimization has its own trade-off; either the system could be designed optimally for security or performance.[32]

A hierarchical network is fundamentally most efficient, but it lacks redundancy, and a single-point failure at the top can break the network down and therefore, it is most vulnerable.[33] Larger networks, such as social networks, Internet or electricity grids, are not hierarchical; rather they behave as random networks, which are more resilient to random failures.

The network of critical infrastructure in cohesion displays the characteristics of a complex system. Behind every complex system, there is a network which defines the interactions between and among the components. In order to understand the complex systems, understanding or detangling of network behind the complex systems is very important. Certainly, critical infrastructures are networked systems, leading to complex relationships due to varying degrees of interdependence and interconnectedness. The critical infrastructure network can be analyzed using the tenets of graph/network theory. This approach can help establish the relationships between objects which, in normal assessment, appear to be discreet. A complex system is represented by components which are the nodes or vertices of the

---

[32] Kenneth Neil Cukier, Viktor Mayer-Schönberger and Lewis M. Branscomb, "Ensuring Critical Information Infrastructure Protection", Faculty Research Working Paper Series RWP05-055, John F. Kennedy School of Government, October 2005, p. 7.

[33] Ibid.

network; the interaction signified by the links and edges; and the system which is denoted by the network or graph.

The real-world networks are continuously evolving. The networks can expand and evolve very quickly, and this phenomenon is based upon the mathematical concept of power functions, an amplification mechanism where small ranges accelerate changes logarithmically. The networks grow organically as well as the growth owes to the migration of nodes to the network. As nodes increase in size, they eventually become hubs, which link numerous nodes. For instance, the transportation network is evolving continuously with the construction of new highways between the cities, the railways networks are also expanding and so is the case of aviation. Some of the airports are hubs of activity. Therefore, networks continue to emerge as their size and scope expands. The network of critical infrastructure is continuously expanding with the inclusion of new industries and services and the growing linkages among the sectors and industries.

4.5.1 Scale-free Networks

In simple terms, scale-free network is a network whose nodes are not randomly or evenly connected, but includes many "very-connected" nodes known as the hubs of connectivity that are responsible for shaping the way the network operates. A scale-free network evolves and grows with time.[34] The term scale free finds its origin in a branch of statistical physics called theory of phase transition. Since the discovery of scale-free nature of the World Wide Web (WWW), real networks have been found to display the characteristics of scale-free networks in the diverse domains of biology, social networks, electricity grids and computer networks.

Complex systems are architecturally resilient against accidental failures. Scale-free networks too display robustness against accidental failure, as

---

[34] Ahmed Tolba, "Scale Free Networks: A Literature Review", International Conference on Complex Systems, New England Complex Systems Institute, 2007, p. 2, available at http://www.necsi.edu/events/iccs7/papers/97f3f392a6d3603c0e6dbbdf5797.pdf, accessed on 29 August 2016.

elimination of nodes with less number of links does not disrupt the network topology. A scale-free network is dependent on its hubs, which are vulnerable to attacks and in particular, to coordinated attacks. If hubs of a scale-free network are eliminated in a coordinated manner, the network faces significant disruptions and ceases to function. So, in the case of scale-free networks, protection of the hubs is critical from the security perspective.[35] The impact of a targeted attack, primarily directed at the hubs of a scale-free network, by taking out the most connected nodes, could result in catastrophe and cease the whole network. In the case of cyber-attacks on CII, whether the nodes (critical infrastructure) on the network are randomly distributed or are scale-free makes a big difference.[36] The reason is that scale-free networks break down in a way different from that of random networks.

When nodes are eliminated from a random network, the random network experiences steady and slow decay with time until it reaches a point where it breaks into smaller separate domains that are unable to communicate with each other. On the contrary, scale-free networks are resistant to random failures. The reason lies in the architecture of scale-free networks, where densely connected nodes are statistically less likely to fail under random conditions. Moreover, a scale-free network completely fails only when the hubs are wiped out, which could be resultant of random failure of many hubs in the network. Hence, they are resistant to random failures. But, on the other hand, under the scenario of targeted attacks, scale-free networks can experience catastrophic failure. A targeted attack is often directed at hubs and once the hubs are eliminated, the network stops functioning immediately. Therefore, scale-free networks are prone to failure under targeted attacks. The defence of scale-free network lies in the protection of hubs and not the many thousands nodes that form the network.

---

[35] Albert Barabasi and Eric Bonabeau, "Scale-free Networks", *Scientific American*, May 2003, p. 59, available at http://barabasi.com/f/124.pdf, accessed on 29 August 2016.

[36] Jan Matlis, "Scale-free Networks", *Computerworld*, 04 November 2002, available at http://www.computerworld.com/article/2579374/networking/scale-free-networks.html, accessed on 29 August 2016.

As the interactions among critical infrastructure are increasing, the interdependency between various elements becomes an important factor. Critical infrastructures depend on input/output of each other for physical commodities, data, information, energy, etc. In fact, the interdependencies on electricity grids can trigger a domino effect—a cascading series of failures that could bring a nation's banking, communications, traffic and security systems, among others, to a complete standstill.[37]

A disruption or failure in electricity supply could bring the functioning of the critical business processes to a grinding halt, and this was experienced when the northern and north-eastern sections of the Indian power grid failed on 31 July/1 August 2012. The failure impacted the basic services such as railways, metro, road signals and emergency and medical services. In December 2015, a severe power outage at three regional Ukrainian electricity distribution companies impacted 225,000 consumers. BlackEnergy3 malware was used to manipulate the industrial control systems of the utilities through remote access.[38]

There are multiple segments/services embedded within every CII, such as the Supervisory Control and Data Acquisition (SCADA) systems, Virtual Private Network (VPN) services, email, Web services, network services and databases. As evident from the case of Ukranian power grid attack, every segment or service is vulnerable to exploitation, and the threat actors might adopt any of the vectors to exploit the underlying vulnerabilities. The next section discusses the threats, their characteristics, motivational factors and the probable vectors they might employ to target critical infrastructure.

---

[37] US Department of Energy, "The Smart Grid: An Introduction", p. 9, available at http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf, accessed on 28 June 2016.

[38] FireEye "Cyber Attacks on the Ukranian Grid: What You should Know", 2016, available at https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf; accessed on 28 June 2016 and Kelly Jackson Higgins, "Lessons from the Ukraine Electric Grid Hack", *DarkReading*, 18 March 2016, available at http://www.darkreading.com/vulnerabilities—threats/lessons-from-the-ukraine-electric-grid-hack/d/d-id/132474, accessed on 28 June 2016.

4.6 Critical Infrastructure: Threat Assessment

The threat actors exploit the underlying vulnerabilities within the application software, control systems software, hardware or even the people to get access to the desired location in the network. Once the network—enterprise or control system network—is breached, they can execute commands, steal sensitive information such as design or configuration or corrupt the information flowing to the interfaces. Threat actors have their own set of motivational factors, varying from political to security or monetary gains to rivalry or competition. There are myriad malicious actors, varying from insiders (in the form of disgruntled employees or compromised/socially engineered employees), economic, military or adversary nation states, criminal syndicates to terrorist outfits with their growing prowess in technology and transnational presence. All of them have different capacities and capabilities. A nation state has the technological means and the requisite wherewithal to conduct and sustain long-term operations, which include espionage, data or credentials theft and execution and monitoring of attacks. Recently, terrorist organizations are also alleged to be capable of perpetrating attacks on CII, with the ease of access to the professional skills available in the market.

Critical infrastructure protection is basically a two-step approach. The first step is to identify the plausible threats and the next step is to identify and reduce the vulnerabilities of individual systems to any sort of damage or attack and reduce their recovery time.[39] As part of the vulnerability–threat–risk identification exercise, understanding the threats, their motivations and their means, which could also be termed as threat vectors, can reduce the organizational attack surface. Threats to critical infrastructure can be broadly classified into three categories: natural,

---

[39] "G8 Principles for Protecting Critical Information Infrastructures", Adopted by the G8 Justice & Interior Ministers, May 2003, p. 1, available at http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf, accessed on 28 June 2016.

human induced and accidental.[40] Natural threats encompass floods, earthquake, tsunami, volcanic activities, etc., while accidental threats arise from failures, errors and miscalculations. Human threats include all the attempts made by malicious actors to gain access to the system with the intent of causing a harm or damage. Human threat can be any one or a combination of the following three broad classifications:[41]

1. *Insider*: An insider could be a person (employee, partner, contractor or vendor) within the organization, having authorization or legitimate access to the asset where the attack has been executed. Generally, insiders possess the requisite information, credentials or security clearances pivotal to perpetrate an attack. There are different motivational factors, varying from monetary gain to disgruntlement and jealously to vengeance.

2. *Outsider*: An outsider, as an adversary, is external to the organization, and therefore does not have the authorization or legitimate access to targeted asset. The list of motivational factors is quite wide, as it could vary from acts of terrorism to crime and hacktivism to professional services.

3. *In Collusion* : Collusion happens when an outsider partners with an insider to perpetrate an attack. In order to gain an easy and definite access, adversaries are generally in quest of vulnerable insiders, and they exploit these insiders to their own advantage. However, the insider might sometimes unconsciously pass on certain information to the adversary.

The attacks on infrastructure vary in terms of nature, capability and the targeted system. The attacks have different impacts on the targeted

---

40 Rosslin John Robles, Min-kyu Choi, Eun-suk Cho, Seok-soo Kim, Gil-cheol Park and J. Lee, "Common Threats and Vulnerabilities of Critical Infrastructures", *International Journal of Control and Automation*, Vol. 1, No. 1, 2008, pp. 18–19, available at http://sersc.org/journals/IJCA/vol1_no1/papers/03.pdf, accessed on 28 June 2016.

41 Brian T. Bennett, "Types of Terrorist Attacks", *Understanding, Assessing and Responding to Terrorism: Protecting Critical Infrastructure and Personnel*, New Jersey: John Wiley and Sons, 2007, pp. 124–25.

system; it might lead to a small or major disruption in the operations or it might compromise sensitive information. In the extreme case, an attack may completely incapacitate an industry, organization, production plant or a service. The origin, motivational factors of the perpetrators and the technological capabilities at their disposal are the key determinants of the magnitude of impact. Some of the common forms of modes of such attacks are:

1. Targeted scanning, probing and exploration of networks and IT infrastructure;

2. Using malicious code/malware such as viruses, worms and trojans;

3. Identity/personal information theft or large-scale spamming;

4. Defacement of websites and semantic attacks on the websites;

5. DoS/DDoS attacks for disruption; and

6. Application-level attacks.

Every attack has a different anatomy because it targets specific assets, and in the case of critical infrastructure, the possible targets are identified as:

1. Sensitive and critical information infrastructure.

2. Infrastructure of data centres and network operation infrastructure, such as:

    a) Routers, switches, database and domain name system (DNS) servers;

    b) Web portals; and

    c) Satellite network communication systems.

3. SCADA, centralized and distributed control systems of facilities.

4. Database administrators, individual users, including senior executives and officials.

The important variable in the protection calculus is the origin or the threat actor. Given the vast impact of disruptions of critical infrastructure, they are the prime targets for adversarial nation states. With the use of proxies, even terror outfits, with the support of a nation state, are a potent and probable threat. There is no clear distinction between the actors, but they can be broadly classified as follows.

4.6.1 Terrorists and Non-state Actors

As evident from the terrorist attacks on the urban transit systems in London and Mumbai, or the hubs of economic activity at the World Trade Center in New York, critical infrastructure has been the prime target for terrorist groups. A single terrorist attack on the World Trade Center directly affected banking and finance, telecommunications, emergency services, air and rail transportation and energy and water supply.[42] Terror groups can be domestic or acting with the support/sponsorship of other adversary nations. With the growing radicalization among the educated youth, these terror outfits have access to the human resources possessing good working knowledge of computers, networks and programming. As a matter of fact, some of the groups such as the Islamic State of Iraq and Syria (ISIS) and Lashkar-e-Taiba are known to have developed their own secure communication applications for smartphones.[43] Given the growing prowess and access to technology as well as technological skills, terrorist outfits are a probable and potent threat actor.

In addition, criminal activities in the cyber realm have witnessed an exponential increase,[44] taking the shape of organized crime. Termed as

---

[42] Ronald L. Dick (Director, National Infrastructure Protection Center, Federal Bureau of Investigation), "Testimony before the House Committee on Governmental Reform, Government Efficiency, Financial Management and Intergovernmental Relations Subcommittee", Washington, DC, 24 June 2002, available at https://archives.fbi.gov/archives/news/testimony/cyber-terrorism-and-critical-infrastructure-protection, accessed on 04 September 2016.

[43] Munish Sharma, "Lashkar-e-Cyber of Hafiz Saeed", IDSA Comment, 21 March 2016, available at http://www.idsa.in/idsacomments/lashkar-e-cyber-of-hafiz-saeed_msharma_310316, accessed on 04 September 2016.

[44] Federal Bureau of Investigation, "Cyber Crime", available at https://www.fbi.gov/investigate/cyber, accessed on 04 September 2016.

cyber-crime or cyber-enabled crime,[45] such activities may not have a direct bearing on the CII as the activities under this umbrella have more association with monetary gains. However, cyber criminals indulge in the trade of data, tools and the desired technical know-how/skills through underground or black markets. Their activities are targeted at trade secrets, sensitive corporate data and identity theft in general, but the same tactics might compromise the secured designs, process flow diagrams, blueprints or security architecture. Perhaps, readily available data, tools or toolkits and the technical knowledge can be exploited by other state or non-state actors to perpetrate an attack targeted at CII. The nexus between non-state actors and terrorist organizations, their transnational characteristics and their use as proxies by nation states makes it strenuous to identify these actors and analyze their modus operandi or underlying motivations.

Motivational Factors : Terrorist outfits strive for attention of masses and their respective governments to meet their political objectives. Spreading terror is their primary means to do so, and major acts of terror get extensive media attention. Critical information infrastructure is vital to the nation states because the masses and the society as a whole depend on them. The crippling effects of an act of terror, either physical or cyber, targeting the vulnerabilities of CII would have far-reaching impact on the victims and the psychology of the witnesses. This is exactly the primary objective of a terror outfit—to instigate terror in the minds of the victims as well as the onlookers. With the support of the adversarial states, terror groups become a more credible threat as they are equipped with financial resources.

Monetary gains, the prime driver for cyber criminals, can easily be leveraged by any adversary in lieu of technology, tools and skills. Their motivational factors are quite clear and in collusion with the nefarious motives of an adversary, make them a direct threat to the security of CII.

---

[45] Interpol, "Cyber Crime", available at https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime, accessed on 04 September 2016.

4.6.2 Insiders

Employees, contractors, partners or vendors, termed as insiders in an organization, have varied degree of access to information, trade secrets, processes and other sorts of business or operations information. Even technology or management consultants, legal advisers/lawyers, auditors or vendors/contractors such as suppliers or outsourcing firms for technology integration or infrastructure management have access to classified information about different aspects, such as technology, human resources, marketing, finance, mergers/acquisition and operations.

Insiders are a potent and credible threat as they tend to have roots deep inside the organization. Financial gain, revenge or ideological motivation may persuade an insider to divulge classified information[46] or in the extreme, to perpetrate an attack. There are numerous ways and means to do so: information can be exchanged through written or printed documents, photographs, verbally, sharing of log-in credentials, access cards or even through portable media such as USB drives or mobile phones. Surveys and studies based on the incidents of data theft or cyber-attacks have designated insiders as a serious security threat.[47]

Insider threat encompasses malicious insiders, compromised victims and ignorant or careless users who inadvertently share sensitive data or information.[48] Phishing or social engineering attacks are generally

---

[46] Center for Responsible Enterprise and Trade and PricewaterhouseCoopers, "Economic Impact of Trade Secret Theft", February 2014, available at https://www.pwc.com/us/en/forensic-services/publications/assets/economic-impact.pdf, accessed on 14 September 2016.

[47] Tara Seals, "Insider Threats Responsible for 43 percent of Data Breaches", *Info Security*, 25 September 2015, available at http://www.infosecurity-magazine.com/news/insider-threats-reponsible-for-43/, accessed on 14 September 2016 and "The Threat of Attack from Insiders is Real and Substantial", *IS Decisions*, available at http://www.isdecisions.com/insider-threat/statistics.htm, accessed on 14 September 2016.

[48] Nir Polak, "Looking at Insider Threats from the Outside", *Help Net Security*, 30 July 2014, available at https://www.helpnetsecurity.com/2014/07/30/looking-at-insider-threats-from-the-outside/, accessed on 18 September 2016.

targeted at those individuals who, by mistake or negligence, are likely to click on a malicious link/attachment or divulge information unconsciously. Unintentional divulgence of information, sharing of log-in/access credentials out of ignorance or identification of phishing attacks can be tackled through awareness and training programmes. However, malicious insiders, as a threat actor, are difficult to detect and deter, making them a serious threat residing within the security perimeters of the organization.

Motivational Factors : It is arduous to identify or screen insider(s) and decipher their underlying motivational factors. The factors could be as diverse as dissatisfaction with the management, poor appraisals, monetary advantage or vengeance. Dismally, malicious insiders are well versed with the vulnerabilities of the organization—those pertaining to the industrial or IT systems, services, products or facilities. They may even implant vulnerabilities intentionally to be exploited later.[49] This set of threat actors have considerable insider knowledge, and a broad scope varying from present and former employees to business partners, such as contractors, consultants, service providers, vendors, IT integrators and so on.

4.6.3 Nation States

If gauged in terms of resources at disposal and the extent of technological capabilities, nation states feature as the most potent threat to the CII. The governments, their intelligence agencies or the armed forces have the desired expertise at their disposal and there is no dearth of financial and computing resources required to execute persistent and sophisticated operations in the cyber realm targeting CII. Economic and technological competition and geopolitical confrontations, such as territorial or maritime disputes, further fuel the desire to develop such capabilities and the intent to put them to use if the need to do so arises.

---

[49] US Department of Homeland Security, "National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat", December 2013, available at https://info.publicintelligence.net/DHS-NRE-InsiderThreats.pdf, accessed on 14 September 2016.

In the absence of globally agreed upon norms or legal measures to dissuade nation states from targeting each other's CII in the face of any eventuality, the CII remains a lucrative target. Under such circumstances, cyber-based attacks have the potential to amount to an act of warfare[50] as they might be utilized to destabilize a nation state. Such attacks may be used to augment an existing political conflict, as evident from the Estonian case of 2007. As one of the most densely connected countries, Estonia has pioneered facilities such as e-government, Internet voting and online banking transactions (98 per cent). Estonia witnessed massive Internet traffic, which brought down the networks of its banks, broadcasters, police, parliament and ministries.[51] The scale and timing of this attack targeted at the core of the CII, which practically brought Estonia to a standstill, affirms that CII is susceptible to the arm-twisting of a nation state, even if the conflict does not escalate to the scale of war.

With reference to targeted attacks against CII, state-sponsored campaigns, known as advanced persistent threats (APTs), have transformed the threat landscape. The APTs are sophisticated, targeted and prolonged attempts of intrusion and information theft using a wide variety of techniques, including SQL injection, malware, spyware, phishing and spam. They also use customized tools such as zero-day vulnerability exploits, viruses, worms and rootkits.[52] Attacks led by the APTs infiltrate into sensitive systems, such as email servers, and they are designed to remain undetected or hidden from the administrators—sometimes for years. Since APTs are highly advanced, planned and

---

50 NATO Cooperative Cyber Defence Centre of Excellence, "Defining Critical Information Infrastructure in the Context of Cyber Threats: The Privacy Perspective", available at https://ccdcoe.org/multimedia/defining-critical-information-infrastructure-context-cyber-threats-privacy-perspective.html, accessed on 14 September 2016.

51 Patrick Howell O'Neill, "The Cyberattack that Changed the World", *The Daily Dot*, 20 May 2016, available at http://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/, accessed on 14 September 2016.

52 Symantec Corporation, "Advanced Persistent Threats: A Symantec Perspective", White Paper, 2011, p. 1, available at https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf.

executed meticulously, they hardly leave any trace, and therefore render traditional means of security and forensics incapacitated. The APTs can be used to serve a cross-section of objectives, including military, political or economic intelligence gathering, confidential data or trade secret theft, disruption of industrial operations or even destruction of industrial equipment.[53] Organizations charged with the responsibility of maintaining or operating critical infrastructures are also at a higher risk from APTs.

Motivational Factors : Cyber domain has enabled asymmetric means of warfare for nation states, coupled with the high degree of deniability. For nation states, considering their strategic interests, cyber is a lucrative option driven by political/military or economic imperatives. For nation states to engage in industrial or corporate espionage, the military and strategic technologies are the key areas of interest. The APT campaigns or malware-based attacks such as Stuxnet or Duqu, carried out by the military establishments or intelligence agencies at the behest of the state, are a credible, apparent and direct threat to the CII. Economic competition, technological disparity, military confrontation or political conflict are few of the factors which trigger the intent to incapacitate, or at the worst cripple down, the information infrastructure underpinning the critical infrastructure of the adversary state.

Table 4.4 summarises the motivations and the characteristics of attacks with their prevalent objectives and the likely impact on CII. Data/ Information Theft and Network Attacks or Espionage Attempts have higher impact on CIIs. The attacker is quite likely to target the critical components of the system, also known as mission-critical systems, which, according to the attacker, would have significant effect on the functionality or may require extended time to repair or restore to normalcy. The preferred targets, therefore, are the critical components in the form of applications, information, hardware or the human resources, or a combination of these.

---

[53] Joel Brenner, "The Calm before the Storm", *Foreign Policy*, 06 September 2011, available at http://foreignpolicy.com/2011/09/06/the-calm-before-the-storm-2/, accessed on 14 September 2016.

Table 4.4. Objectives, Motivations and Characteristics of Cyber-attacks

Objective	Motivation	Characteristics	Example	Impact on CII
Nuisance/ Disturbance	Access or Control/ Revenge/ Political Animosity	Automated/ Scripted/Short Time Span	Botnet/Spam/ DoS/DDoS	Moderate
Data/ Information Theft	Economic/ Industrial or Political Advantage	Persistent/ Clandestine/ Long Time Span	IP Theft/Identity Theft/Sensitive Information Theft	High
Crime/ Fraud	Monetary Gain	Opportunistic/ Discreet/Wide Scale	Banking Frauds/ Phishing/ Ransomware	Low
Hacktivism	Defamation/ Political Rivalry/ Political Animosity	Conspicuous	Website Defacements	Low
Network Attack/ Espionage	Escalation/ Disruption/ Destruction	Clandestine/ Conflict-driven Military/ Economic or Political Interests	Disrupt/Destroy/ De-capacitate Critical Infrastructure Networks or their Key/Auxiliary Industrial Functions	High

Source: Compiled by the author.

4.7 Attack Surface and Threat Vectoring

An attack is fundamentally the convergence of vulnerability, accessibility of the system and capability of the adversary. In other words, an attack culminates when an adversary equipped with the desired skill set is able to access the targeted system to exploit a known vulnerability (either a zero-day exploit or an un-patched vulnerability) to disrupt/degrade or compromise the integrity of the targeted system. In this case, vulnerability is an identified weaknesses arising out of inadequate security

procedure or a weakness due to failure in following proper security processes designed to prevent unauthorized access.

An attack surface is an aggregate of all the points of entry for a potential attacker, and these points are spread across the network, the software or the applications, through physical means of entry and it also includes the human beings.[54] These points of entry let the attacker send data to the target or extract data from the target. In-depth security architecture encapsulates these interrelated considerations for protection from an external attack.

Network attack surface originates from the exposed constituents of networking technology, such as the protocols, the ports and communication channels; the devices in form of routers, firewalls or mobile phones; and the network applications such as cloud-based services and firmware interfaces with external systems.

Software attack surface is calculated across the programmed code an organization executes in totality and these include the applications, different email services, configurations, databases, executables, Web applications, mobile applications and operating systems, covering the interfaces, services, protocols and practices available to all users, particularly the components accessible to unauthenticated users.

Human attack surface considers the wide spectrum of vulnerabilities within the human beings, which could compromise sensitive information leading to an easy way into the secured systems. These considerations are as diverse as social engineering attacks, inadvertent errors, malicious insiders, death, disease or disability of human resources.

A thorough attack surface analysis is a vital input to the process of setting up defensive mechanisms of firewall, intrusion prevention systems, intrusion detection systems, data policy and other security

---

[54] Stephen Northcutt, "The Attack Surface Problem", SANS Technology Institute Security Laboratory, 7 January 2011, available at http://www.sans.edu/research/security-laboratory/article/did-attack-surface, accessed on 23 October 2016.

measures. Despite defences, attacks do take place; and for an attack to succeed, attacker adopts a path or means to gain access to the target and deliver the malicious code, known as attack vector.

Common attack vectors are Web application attacks, client side attacks, network attacks, attacks using malware and APTs, DoS/DDoS attacks, social engineering or spear phishing attacks, brute force attacks on encrypted data, man-in-the-middle attack or interception of communication channel, routing attacks, supply chain contamination, DNS attacks, targeted attacks by evading/bypassing perimeter protection devices, etc.[55]

The most common techniques or best practices to reduce attack surface are: to reduce the amount of running code; reduce access to entry points by unauthenticated users; reducing privilege to limit damage potential; anonymous code paths; reduce attack surface; and periodical measuring of attack surface.[56] There are five primary architectural approaches to achieving defence-in-depth: uniform protection, protected enclaves, threat vector analysis, information-centric protection and role-based access control.[57] The process of defending the networks and assets of critical infrastructure should, in the first place, start with the identification of assets to be protected and prioritizing the security of critical assets from business continuity perspective. The further process of defining, analyzing and calculating attack surface, reducing the attack surface and management of vulnerabilities is an organization-wide exercise with active participation/consultations of all the sections and departments.

The entire focus of a security strategy is to figure out all the available options/ways to place necessary controls on the applications, networks

---

[55] NCIIPC, *Guidelines for Protection of Critical Information Infrastructure*, Version 2.0, 16 January 2015, available at http://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf, accessed on 22 March 2017.

[56] Ibid.

[57] Stephen Northcutt, "The Uniform Method of Protection to Achieve Defence-in-Depth", SANS Technology Institute Security Laboratory, 26 February 2007, available at http://www.sans.edu/research/security-laboratory/article/367, accessed on 23 October 2016.

and human resources, so as to prevent the threat actors from exploiting vulnerability through any of the vectors. The strategy could also discern the probable threat actors (governments, terrorists, hacktivists, industrial espionage, organized crime, errors or natural disasters) and their respective motives. A good case study in this context is the good practices guide developed by the European Union Agency for Network and Information Security (ENISA).

The guide has adopted an all-hazards approach to address the prime issue of resilience. The wide scope encompasses the threats in the form of natural hazards (floods, hurricanes, etc.) or system failures (both hardware and software failure) to the likes of cyber-crime (malicious acts arising from internal and external agents through fraud, cyber theft and DoS attacks), and extends up to the overarching issues of terrorism or the involvement of nation states (large-scale disruption of computer networks to create panic or espionage).[58]

The increased dependency, aggravated by the complexity of operations, has made critical infrastructures vulnerable to a wide variety of threats, which includes natural hazards, human error, technical problems and the sophisticated acts of cyber terrorism and warfare, capable of services degradation or infrastructure failure.[59] The identification and qualitative as well as quantitative assessment of the risk is key focus area of the research in the discipline of critical infrastructure protection. The approach is based upon identification of critical functions; assessment of threats, vulnerabilities and consequences; and prioritization of risk.

---

[58] ENISA, "Cooperative Models for Effective Public Private Partnerships Good Practice Guide", 2011, p. 21, available at https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps, accessed on 14 March 2017.

[59] Peter S. Anderson, "Critical Infrastructure Protection in the Information Age", in Robin Mansell, Rohan Samarajiva and Amy Mahan (eds), *Networking Knowledge for Information Societies: Institutions & Intervention*, The Netherlands: Delft University Press, 2002, pp. 188–194.

Chapter 5

Critical Infrastructure Protection

Critical information infrastructure protection (CIIP) is gradually being acknowledged as a vital component of national security policy, as nation states are detangling the complexities and gaining understanding of their implications. Perhaps, developed nations have greater dependencies on their information infrastructure and realizing that, they have adopted policy measures and established new organizations mandated to specifically devise and execute comprehensive critical infrastructure protection (CIP) strategies. These organizations involve governmental agencies, departments, ministries and private sector, basically encapsulating all the stakeholders.[1]

In order to effectively protect critical infrastructures, countries must protect their respective CIIs from any sort of intentional or accidental damage and secure them against both physical and cyber-attacks. Effective communication, coordination and cooperation at both national and international levels, among the stakeholders—industry, academia, private sector and government entities, including infrastructure protection and law enforcement agencies—is a prerequisite to CIIP.[2]

---

1 Manuel Suter, "A Generic National Framework for Critical Information Infrastructure Protection", Center for Security Studies, ETH Zurich, August 2007, p. 1.

2 The Council of the EU, "Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection", *Official Journal of the European Union*, p. 29, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF, accessed on 12 October 2016.

However, the process of protecting critical infrastructure has many challenges; some of them are discussed next.

1. *Private and Public Perspectives* : The list of actors involved in developing or maintaining critical infrastructure installations is endless, but they broadly fall under government or public enterprises and private entities. Private sector is a key player and government, by itself, has limited control on the functioning or policymaking apparatus of private entities. This induces issues related to sharing of responsibilities, implementation of regulations and division of powers among the public and private sectors.

   The industry owns and operates majority of the infrastructure, while government is more often reliant on the services and products of these infrastructure. Government also owns and operates some of the infrastructure, but generally regulates the markets, supervises compliance and due to national security imperatives, is more concerned with the protection of critical infrastructure.[3] Private sector, on the other hand, views the government in regulatory roles, whose control sometimes is an impediment in their organizational objectives, which primarily revolve around creation of wealth for the shareholders. Therefore, it is essential for both the private and public sectors to foster the trust and confidence which is vital to information sharing and success of any policy measure adopted to protect the critical infrastructure.

2. *Multiple Stakeholders* : This gives rise to the collective action problem, given the large number of entities; they have diverse and sometimes divergent interests.[4] The private sector has business growth as its top-most priority, while the government has national security and delivery of essential services as the primary concern. Within the governmental structure, multiple agencies and departments are charged with the responsibilities. Too much regulatory control might

---

[3] Kenneth Neil Cukier, Viktor Mayer-Schönberger and Lewis M. Branscomb, "Ensuring Critical Information Infrastructure Protection", *Faculty Research Working Paper Series RWP05-055*, John F. Kennedy School of Government, October 2005, p. 5.

[4] Ibid, pp. 9–10.

be detrimental for free market systems, while absence of requisite controls or legislations discourages investments. Accommodating the interests of all the stakeholders, including the civil society, demands multiple consultations, platforms and strenuous effort.

3. *Scale and Unlimited Boundaries* : Critical infrastructures are geographically spread, across the length and breadth of the nation state. It is impossible to set any physical boundaries, which makes it a daunting task to affix the areas of responsibility. The overall network or structure of critical infrastructure in the national perspective is so vast, large and spread that it is impractical for the practitioners to protect each and every component of every sector with equal measures of priority and resources.[5] Information networks are spread beyond physical and political boundaries of a nation state, and protecting such a globally spread infrastructure is again an international responsibility.

4. *An Expanding Network* : Critical infrastructures are growing day by day, as new facilities, industries, technologies, equipments and processes are continuously being added to the already existing massive network. Infrastructures are evolving; also, the size and interconnections of this vast network are dynamically growing due to the rising demands or requirements of the populace. Formulating policies and protection strategies need periodic calibration to ingest the changes and risks brought in by the expanding network of CIIs.

5. *Complexity and Interdependencies* : Critical infrastructures are complex and difficult to understand in terms of their behaviour under conditions of disruption, also known as cascading failures, which have unpredictable consequences. It arises out of the interdependencies between and among the sectors, as materials, products, information, etc., are passed on to the downstream sectors. Critical infrastructure protection strategies are inadequate if understanding of these interdependencies, failure analysis and

---

[5] Ted G. Lewis, *Critical Information Infrastructure Protection in Homeland Security: Defending a Networked Nation*, New Jersey: John Wiley and Sons, 2006, pp. 49–50.

behaviours remains limited. Moreover, since these networks cut across political boundaries, the absence of legal mechanisms and fragmented national policies governing CIP exacerbate the existing challenges.

6. *Human Element* : This is most critical in CIP policymaking and its implementation. All the key decisions regarding the design, development and operations of the systems, applications and networks behind critical infrastructure installations are human dependent. Every business or industrial process has a definite human element or interface, and entire policy, management or technical expertise lies with the human resources. Also, human resources have different levels of access rights, for both physical and IT/ industrial control system/SCADA systems. There is always a possibility of human-induced error or a deliberate attempt on part of the employee(s), leading to compromise in either the system itself or sensitive information pertaining to any aspect of the critical infrastructure operations.

7. *Endless Vulnerabilities and Limited Knowledge* : The technologies that underpin critical infrastructure sectors/industries, such as process or assembly chain automation, robotics, remote process controls, IT, database systems, industrial control system and SCADA, are built over a period of time, and probably by different vendors under varying demands of the clients. Gradually, the industrial control system networks have been integrated with IT networks, which has thrown open a wide space for the attackers to exploit the control systems for potential malfunction or disruption. The list of installed proprietary software and hardware, which have its own set of vulnerabilities, across critical infrastructure verticals is endless. With the growing use of commercial off-the-shelf (COTS), vulnerabilities have been introduced in every industry, and have perhaps spread across the globe.

   Human resources, the actual brains behind the operations, are one of the weakest links, and they are always vulnerable to unintentional or intentional disclosure of information, sabotage or social engineering.

   The knowledge and understanding of the technologies underpinning critical infrastructure, and their respective vulnerabilities, is therefore

limited and the research in this field is at a nascent stage. The methodologies for analysis, assessment and mitigation of risk are yet to mature in the discipline of CIP.

8. *Information Sharing/Analysis* : In the absence of clearly defined roles and responsibilities, duties and a definite command structure, information sharing among the entities is not seamless. Information is hoarded and not shared with the right department or agency; and there are only a few information-sharing platforms and therefore, collecting and using the information to aid decision making remains a key challenge. The gathering and analysis of threat information is a network-intensive effort and intelligence agencies tend to have the desired expertise in this regard. Their experience is valuable to the agencies tasked with CIP, and both should partner, rather than compete, on this turf. There are few states who have established a specialized CIP agency; however, most of them have functional computer emergency response teams (CERTs). Although CERTs have their own set of responsibilities in the form of information disbursement and issuing warning and advisories, they are supposed to work in tandem with the CIP agency, irrespective of the department or ministries they both function under. The CIP agency would also need to leverage the technical expertise or competence residing with the CERTs and their contacts with CERTs in the region and other parts of the world.

9. *Fragmentation* : In the wake of sudden rise in cyber threats, various departments and ministries of the government and private sector associations have set up cyber security agencies, which are more aligned to serve their own mandates and interests. This fragmented approach is a substantial challenge, as most of these agencies work in silos and devise policies according to the small set of stakeholders.

10. *Asymmetric Angle* : The threat spectrum has widened as threats originate from nation states as well as malicious non-state actors. The present-day threats are ambiguous, uncertain and indistinct in terms of their identity and goals.[6] While nation states have broader

---

[6] Elgin M. Brunner and Manuel Suter, "International CIIP Handbook 2008 / 2009", Center for Security Studies, ETH Zurich, July 2008, p. 34.

political or security motivations, they have more resources and technical prowess. But the motivations of malicious non-state actors are hard to comprehend, and could be anything from monetary gain to terrorism or even a narrow political agenda. Of late, these threats are being characterized as "risks", and risks by definition are indirect, unintended and uncertain.[7] The critical infrastructures, with their widely spread vulnerabilities and interdependencies, are a soft and obvious target. A small failure might aggravate to become a catastrophe, and addressing this particular aspect of asymmetry in the geopolitical frame is the prime challenge as well as the target of a CIP strategy.

Protection of critical infrastructure involves different perspectives from system-level technicalities, business perspective, law enforcement perspective and above all, a national security perspective. The protection is further made complicated by the attributes of critical infrastructures: they are decentralized, interconnected and interdependent. They are controlled by multiple actors spread across government or privately owned enterprises, having diverse types of technologies in place. The central challenge in designing a policy to protect critical infrastructures from threats is not technical or operational, rather a challenge of a comprehensive national strategic vision.[8] There is no definitive approach to CII protection. It is an amalgamation of national priorities or commitments and several other recursive initiatives encompassing the dynamics of business objectives, operational processes, technological advances and arising threats.

5.1 Approach to CIIP

The CIIP is bound with varying perspectives over threat perception and risk appetite. It is unfeasible to eliminate the threat actors and the vulnerabilities; therefore, protection is essentially about securing assets, information and people. Protection, as a mechanism, is a blend of

---

7 Ibid.

8 Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats", in Gabi Siboni (ed), *Cyberspace and National Security*, Tel Aviv: Institute for National Security Studies, 2013, p. 36.

policy initiatives: adoption of best practices, implementation of controls, compliance/regulation in the form of audits and most importantly, comprehensive risk assessment and management.

Table 5.1: Best Practices Summary

Best Practices	Description
Redundancy	Operation centres Communication systems/channels Applications Data centres
Standards/ Compliance	Application development Equipment installation Network design Information/data security standards/compliance
Degradation Modes	Alternative processes to sustain mission-critical processes Separation of control areas for containment
Collaboration	Collaboration with public authorities/governmental agencies Collaboration within sector (e.g., mutual assistance, facilities)
Tightened Access Control	Restrictive user access management Application of special technologies (e.g., IRIS-scan)/two-factor authentication Least privilege User behaviour monitoring
Early Warning	CERT level/sector specific National, regional, international institutions for information sharing/dissemination Network-specific security messages (e.g., validation of principles, alerts, warnings)
Training, Exercises	Communication, coordination and awareness among employees Information security trainings/sensitization Sector-specific trainings Security exercises/drills Frequent exercises (planned, periodic)

***Source*:** Compiled by the author.

5.1.1 Best Practices

Some research estimates suggest that if IT network management follows good practices, 85 per cent of cyber-attacks could be prevented.[9] As a beginning step, adopting and implementing good practices can thwart majority of the targeted attacks against networks, applications and human resources, and also reduce the attack surface considerably. The best practices can be moulded into seven wide categories (see Table 5.1).

There is a plethora of information available regarding best practices. In summary, these fall under the above-mentioned seven categories pertaining to building redundancies, tightening the access controls, implementing standards and adhering to compliances, forming a network of collaboration and early warning and training the human resources for efficacious implementation of all these measures, including sensitization to the basics of information security.

Redundancy in the operating/data centres or communication lines ensures the sustainability of operations in the case of attacks or disasters. Redundancy itself is a parameter of criticality, and in order to reduce the degree of dependence on a single system, or channel or source, building redundancies in the critical processes is a key best practice. If the systems or assets are designed in such a way that they remain operative even if degraded, such as the segregation of control areas, it contains the propagation of failure or disruption. A vigilant and tightened access control for information systems, applications, assets or information itself can keep a number of threat actors at bay. Restricting the access to the facility or production area and assigning stringent role-based access controls are some of the practices which help strengthen the security baselines. Establishing early warning systems and a network of collaboration with industry peers or regional/international institutions ensures that malware or vulnerability information is shared among the critical infrastructure at the earliest, to be acted upon in a timely manner.

---

[9] Kim Zetter, "Senate Panel: 80 Percent of Cyber Attacks Preventable", *Wired.com*, 17 November 2009, available at http://www.wired.com/threatlevel/2009/11/cyber-attacks-preventable/, accessed on 26 July 2016.

The need and imperatives of emergency response teams for sector specific requirements, or at national, regional, international levels have been put forth by the resolutions adopted by the UNGA and recommendations or principles adopted by the G8 countries and the OECD. The human element is the vital link in the security chain and therefore, the trainings, awareness and exercises, as a practice, elevate the efficacy of protective mechanisms through communication/ coordination at the departmental, sectoral, national and international levels. Adopting best practices is not the end of security process; it is just the beginning. Best practices evolve and improve over time and therefore, the security practitioners need to be abreast with the changes in this dynamic environment. The trends suggest that the process of mitigating the impacts of attacks or incidents is basically a risk management exercise, as practised by every organization in their own limited capacity.

5.1.2 Risk Management in CIP

Risk assessment and management for CIP is a relatively new and emerging discipline, and it is gradually maturing as research in this field is picking up pace. Computer-based modelling techniques or simulations to detangle the intricacies of dependencies are part of the evolving landscape. Several approaches have now been proposed by researchers to analyze critical infrastructure systems. These approaches, in general, focus on linking structural and functional aspects with security goals, and associating vulnerabilities with known attack vectors.[10]

The primary objective of security management is to protect the assets or resources of the organizations. These assets could be physical, such as facilities, industrial plants, generation units, buildings, offices, machinery and investments, or they could be intellectual property in form of trade secrets or copyrights. Even the components of IT network, the routers, switches, computers, servers, databases, etc., fall under the category of assets. These need to be secured because: (a) their destruction, unavailability or incapacity to perform their intended/

---

[10] Jason Kopylec, Anita D'Amico and John Goodall, "Visualizing Cascading Failures in Critical Cyber Infrastructures", in Eric Goetz and Sujeet Shenoi (eds), *Critical Infrastructure Protection*, New York: Springer, 2008, p. 353.

desired functions, or disclosure to unauthorized agents, might cause a detrimental effect; (b) they are the prime target for malicious threats actors; and (c) they are at continuous risk from malicious activities, either intentional by exploiting vulnerabilities, errors on the part of system operators or an unforeseen natural disaster.[11]

Going by the definitions, a "threat" is a "potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm";[12] a "vulnerability" is a "weakness in the architectural design or implementation of an application or a service"; and an "attack" is the "entire process implemented by a threat agent to exploit a system by taking advantage of one or more vulnerabilities".[13] The consequences of a successful attack can be assessed in the form of monetary loss, opportunity loss or loss of life and diminished trust.

Risk is the probability or likelihood of occurrence of a damaging incident or a threat actor exploiting vulnerability, leading to negative consequences. Risk assessment involves the integration of information with respect to the threat, vulnerability and the associated consequences. The process of risk management involves decision making to adopt protective measures based on an agreed-upon risk reduction strategy.[14] The cumulative effects of probability of uncertain occurrences that may affect the objectives or operations of an organization are termed as risk. Security strategies for IT systems are moving towards risk management as a key methodology to develop a trusted computing base and optimize resource allocation. The existing research in this area pursues the challenges pertaining to the events which can disrupt business

---

[11] Marcelo Masera and Igor Nai Fovino, "A Service-oriented Approach for Assessing Infrastructure Security", in Eric Goetz and Sujeet Shenoi (eds), *Critical Infrastructure Protection*, n. 10, pp. 370–371.

[12] Ibid, p. 370.

[13] Ibid.

[14] John Moteff, "Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences", Congressional Research Service Report RL32561, 04 February 2005, p. 2, available at https://www.fas.org/sgp/crs/homesec/RL32561.pdf, accessed on 12 August 2016.

substantially, their likelihood and consequences, both using qualitative and quantitative methods.

The National Infrastructure Protection Plan (NIPP) of the US Department of Homeland Security highlights the absence of a national-level understanding of the risks faced by the IT sector, although individual entities manage a wide range of risks to deliver the products and services. It specifies that the risk assessment methodologies should include human, cyber and physical elements of infrastructure.[15] The practices guiding resilience of critical infrastructure are leaning towards an "all-hazards" approach to address the wider spectrum of natural and man-made/human-induced risks. The US Department of Homeland Security utilizes a wider threat profiling approach in the analysis, addressing natural threats, cyber threats, terrorist threats, workforce threats, etc., by identifying vulnerabilities in people, processes and technologies.

In the perspective of information security, risk assessments are used to identify, estimate and prioritize risks to organizational operations, missions, functions, image, brand equity, credibility and reputation, its assets, individuals, resulting from the operation and use of information systems.[16] The National Institute of Standards and Technology (NIST) has published guidelines for conducting risk assessment in information security. As per the document, the purpose of risk assessments is to inform decision makers and support risk responses by identifying:[17]

1. Relevant threats to organizations or threats directed through organizations against other organizations;

2. Vulnerabilities, both internal and external to organizations;

---

[15] US Department of Homeland Security. "Critical Infrastructure and Key Resources Sector-specific Plan as Input to the National Infrastructure Protection Plan", May 2007.

[16] National Institute of Standards and Technology, US Department of Commerce, "Information Security: Guide for Conducting Risk Assessment", September 2012, available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, accessed on 12 August 2016.

[17] Ibid.

3. Impact (that is, harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and

4. The likelihood that harm will occur.

The process of risk assessment begins with a thorough examination of the negative effects of the degradation or loss of a key asset to the core business processes of the enterprise or organization. The likelihood of occurrence of such an event is an input to risk assessment. The level of risk is based on the value of the key assets, profile of the threats to the key assets and vulnerabilities and likelihood of exploitation of the vulnerability by the probable threats.[18] This has essentially become a national priority as nation states have realized the importance of information systems to the very functioning of their critical infrastructures.

The primary aim of risk analysis is to identify the key resources or key assets under different jurisdictional controls, and figure out their vulnerabilities to disparate attacks, natural disasters or accidents. It begins with an examination of the implications or how does degradation or loss of key assets affect the core business processes? The analysts then determine, either quantitatively or qualitatively, the likelihood of occurrence of these negatively impacting events. Furthermore, cost computation of the agreed-upon measures is made, in terms of finance, human resources, effort or technology. The cost benefit of securing the assets/resources against the risks with respect to the consequential costs of "no action taken" influences further decision making. It makes the difference between accepting the risk or mitigating it through some action or transferring the risk. That gives the right inputs to devise appropriate security measures, specific to the requirements of the organization.

In essence, risk analysis is a detailed identification, examination and assessment exercise, undertaken to understand the nature of unwanted, negative consequences resulting from undesired events. The severity of risk is based on three key aspects:

---

[18] Brian T. Bennett, *Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel*, New Jersey: John Wiley and Sons, 2007, p. 230.

1. The value of the key assets;
2. Threats to the key assets; and
3. Their vulnerabilities and likelihood of exploitation.

Quantitative risk analysis methodology enables the analysts to measure or express the magnitude of risk in numerical terms. The calculations are based upon the numerical values associated with the consequences of the attack/failure in form of monetary losses and the probability in form of likelihood. Since risk is measured as a quantity, it makes the task of cost–benefit analysis quite easy for the policymakers. On the other hand, qualitative risk analysis is carried out based upon a matrix describing the events, likelihood and the consequences, and it uses a scalable table. The parameters on which risk is analyzed vary from human resources to assets/resources; financial implications to loss of service; or it may even consider impact on environment, public health, stock markets or reputation.[19] The process has been summarized in Figure 5.1.[20]

The fundamental objective of any risk management practice is to minimize the impacts and if possible, eliminate the risk. There is a cost associated with the protection mechanism required to mitigate the risk, either in form of changes in processes, acquisition of technology or hiring of human resources. The decision to either accept or not to accept a risk is based upon the evaluation of the threat, related risk, the cost of countermeasures and the cost-to-benefit ratio.

It is noteworthy that there is no return on investment for CIP and the investments made to mitigate risks may bear intangible benefits. The threat of legal liability somehow does not exist—either there are no legal frameworks or it is facile to cover up acts of negligence or minor failures. Given these two factors, there is neither a business need nor a deterrent in place if CII providers fail to secure themselves. Additionally, CII providers, and even the policymaking apparatus, have dearth of information and tools regarding the risks to critical infrastructure and

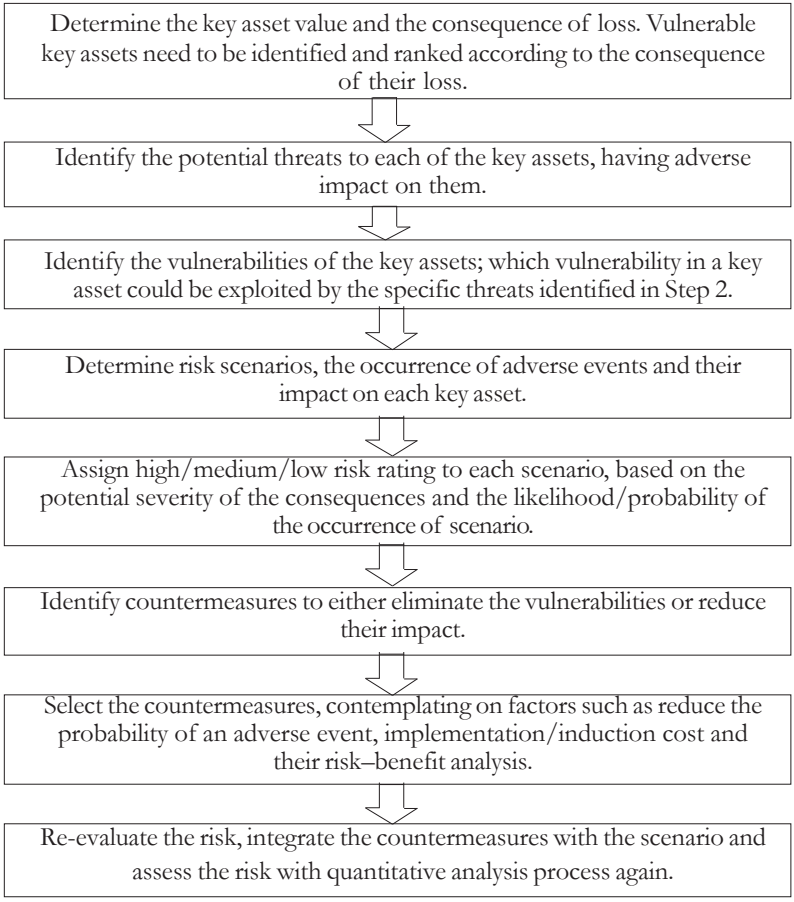
---

[19] Ibid, p. 232.

[20] Ibid, p. 231.

the costs of failure.[21] The extent or intensity of the risks and consequences or costs is unknown. The asymmetry between risks and their consequences is substantial.[22]

Figure 5.1: Summary of Risk Management



***Source*:** Prepared by the author with inputs from Bennett, *Understanding, Assessing, and Responding to Terrorism*, p. 231.

---

[21] n. 3, p. 10.

[22] n. 3, p. 11.

It has been discussed earlier that critical infrastructure sectors are organized as networks: some of them are hubs with high density, while some have a few connections. As found in a research led by the principles of network science, the hubs are the critical nodes, so the effort must be directed at protecting the hubs. Given the limitation in terms of availability of resources and the vast spread/scope of the critical infrastructure sectors, protection of everything is practically unfeasible.[23] Therefore, identifying hubs in the networks—also known as critical node analysis[24]—and protecting these critical nodes can, on one end, optimize investments and at the same time, prevent the distressing impacts arising out of disasters.

5.2 Mitigating Risks: Planning Business Continuity and Crisis Management

In business terms, risk is a functional analysis of the level of threat, degree of vulnerability and the impact of an adversarial event. Impact and threat are constant and therefore beyond control, while vulnerability can be reduced. The means of risk reduction can be integrated in: (a) the network architecture, such as firewall and network segregation; (b) management controls, ranging from planning to risk assessment; (c) operational controls, for instance, personnel security, contingency planning and configuration management; and (d) technical controls, such as authentication, access control and systems and communication protection.

In the case of technical security risks, assessment and communication are the two closely aligned activities. Technical risk assessment involves all the hardware and software associated with the monitoring and control of a system, encompassing each and every component. Risk assessment takes into account the vulnerabilities of both hardware and software, threats in the form of exploits and the relative consequences stemming from vulnerabilities that are exploited. Risk communication between groups involves preparing and presenting risk information to

---

[23] n. 5, p. 16.

[24] Ibid.

the business decision makers, who may or may not possess technical knowledge. Risk communication between the teams that carry out the assessment and the officers or the board is essential. Risk assessment methods help in the translation of technical risk into business risk, to express the consequences in terms of financial loss, or loss of human life, or reputational loss and/or environmental degradation.[25] Most of the organizations already practice risk management and their business continuity planning is one of such practices.

A business continuity plan helps prevent or manage the consequences of a disruption and mitigates the impact on the core business functions of the organization. It refers to the activities required to keep the organization operating during a period of interrupted operations.[26] It could include all possible threats and catastrophic events or natural disasters such as floods/earthquakes as well as the acts of terrorism and sabotage. A comprehensive business continuity plan covers the safety of data and information in case of outages due to hardware or network failures. As the businesses are becoming heavily dependent on IT infrastructure, there is a constant risk to the continued availability, reliability and recoverability of resources. The disruptions range from mild to severe arising out of a variety of events, such as:

1. Equipment failure (such as disk crash);
2. Disruption of power supply or telecommunication services or connectivity;
3. Application failure or corruption of database;
4. Human error, sabotage or strike;

---

[25] Peter Kertzner, Deborah Bodeau, Robert Nitschke, Jim Watters, Mary Louise Young and Martin Stoddard, "Process Control System Security Technical Risk Assessment: Analysis of Problem Domain", Research Report, Institute for Information Infrastructure Protection, January 2006, p. 3.

[26] SANS Institute, "Introduction to Business Continuity Planning", 2002, p. 2, available at https://www.sans.org/reading-room/whitepapers/recovery/introduction-business-continuity-planning-559, accessed on 07 August 2016.

5. Malicious software (viruses, worms, Trojan horses) attack;
6. Social unrest or terrorist attack;
7. Fire; and
8. Natural disasters (flood, earthquake, cyclone).[27]

In business operations, such adverse events are termed as "crisis" and defined as a "significant threat to operations that can have negative consequences if not handled properly"[28]. In crisis management, the threat is the potential damage a crisis can inflict on an organization and its stakeholders. A crisis can create three related threats: (a) public safety; (b) financial loss; and (c) reputation loss.[29] In accordance with this, a crisis management plan is designed to provide guidelines for a practical communications system that is adaptable for any crisis situation. It is part of an overall safety and emergency preparedness plan and a standard part of overall strategic planning process.[30]

The crisis management plan for countering cyber-attacks outlines a framework for dealing with cyber-related incidents. The plan needs a coordinated and multi-disciplinary approach for rapid identification, information exchange, swift response and remedial actions to mitigate and recover from malicious cyber-related incidents impacting critical processes and assets. A good reference work in this regard is the *Computer Security Incident Handling Guide* published by the NIST of the US. As

---

[27] Ibid, p. 3.

[28] W. Timothy Coombs, "Crisis Management and Communications", Institute for Public Relations, 30 October 2007, available at http://www.instituteforpr.org/crisis-management-and-communications/, accessed on 12 March 2017.

[29] Gujarat Informatics Ltd, "Crisis Management Plan", *e-Governance Bulletin*, Vol. 7, No. 7, 2010, pp. 1–5, available at http://www.gujaratinformatics.com/pdf/Crisis%20Management%20Plan.pdf, accessed on 07 August 2016.

[30] "A Guide to Developing Crisis Management Plans", NTA's Market Development Council, March 2000, p. 1, available at http://www.ntaonline.com/includes/media/docs/crisis-mgm-plan-020703.pdf, accessed on 07 August 2016.

per the guide, the strategy for crisis management at organizational level is divided into four stages:[31]

1. *Pre-incident Preparation* : This phase involves establishing and training an incident response team and acquiring the necessary tools and resources for incident analysis and response.

2. *Detection and Analysis* : Detection is necessary to alert the organization whenever an incident occurs. Identifying the attack type, scope and vectors and then implementation of the appropriate controls to contain the attack and quarantine any compromised host is done during this phase.

3. *Containment and Mitigation* : Strategies and procedures for containing the incident have to be predetermined to limit continued impact.

4. *Post-incident Activity* :

    a. A follow-up for each incident, for technology upgrade, future use and to document lessons learnt.

    b. Create a formal chronology of events.

    c. Create the monetary estimate of the amount of damage caused in terms of any loss of software and files, hardware damage and staffing cost.

A cyber-related incident of national significance may take any form: a coordinated cyber-attack; an exploit (zero day), virus, worm or any malicious software code; and a national disaster or other related incidents capable of causing extensive damage to the critical infrastructure or the information infrastructure underpinning critical infrastructure and their key assets. The GoI has formulated a Crisis Management Plan for countering cyber-attacks and cyber terrorism to be implemented by all ministries/departments of central government, state governments and their organizations and critical sectors. The organizations operating CII have been advised to implement information security management

---

[31] Paul Cichonski, Tom Millar, Tim Grance and Karen Scarfone, *Computer Security Incident Handling Guide*, NIST, Special Publication 800-61, August 2012.

practices based on international standard, ISO 27001.[32] Such practices are being adopted by information security agencies and governments across the globe, while being integrated with CIIP policies. However, the domestic factors, such as laws, regulatory frameworks, public–private sector relationships and governments' commitments, shape the CIIP-related policies and perspectives.

[32] Press Information Bureau, GoI, "Crisis Management Plan for Cyber Attacks", 06 May 2010, available at http://pib.nic.in/newsite/erelease.aspx?relid=61597, accessed on 07 August 2016.

Chapter 6

National Perspectives and Multilateral Platforms

The policies governing the protection mechanisms for critical infrastructure and CII are subject to the priorities set by the respective governments under their domestic laws and circumstances. This issue is actively being discussed in multilateral platforms as well. Domestic factors such as legal and regulatory frameworks, maturity of public–private sector relationships and governments' commitment etc. shape the CIIP-related policies and perspectives to a large extent. Despite the variations, certain characteristics remain common. The following section discusses the national perspectives of various countries, namely, the US, the UK, Australia, China and India, and some of the key multilateral initiatives in this sphere.

6.1 National Perspectives

6.1.1 CIIP in the US

The Department of Homeland Security provides strategic guidance to public and private entities in the US. It promotes a national unity of effort and coordinates the overall federal effort to ensure security and resilience of the nation's critical infrastructure.[1] The National Infrastructure Protection Plan (NIPP) of 2013 outlines the framework for government and private sector participants in the critical infrastructure community to work together to manage risks and achieve security and resilience outcomes. The initial version of NIPP was released in 2006 and revised in 2009, and it has thereafter evolved in the present shape,

---

[1] US Department of Homeland Security, "National Infrastructure Protection Plan", available at https://www.dhs.gov/national-infrastructure-protection-plan, accessed on 07 November 2016.

adapting and streamlining the current risks, policy imperatives and strategic environments. It envisions: "[a] Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened."[2]

The NIPP 2013 encompasses the requirements laid down in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21), signed in February 2013. The plan has been developed through a collaborative process involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry.[3] PPD-21 assigns a federal agency, known as Sector-Specific Agency (SSA), as a lead agency to collaborate the process for critical infrastructure security within each of the 16 critical infrastructure sectors. Each SSA is responsible for developing and implementing a sector-specific plan to apply the NIPP concepts to the unique characteristics and conditions of their specific sector.[4] The SSAs for the various critical infrastructure sectors are given in Table 6.1.

The Executive Order 13636—Improving Critical Infrastructure Cybersecurity—directs the federal government to coordinate with critical infrastructure owners and operators to improve information sharing and collaboratively develop and implement risk-based approaches to cyber security.[5] The directive builds upon the extensive work done in protecting critical infrastructure. It delineates a national effort to share threat information, reduce vulnerabilities, minimize consequences and hasten response and recovery efforts related to critical infrastructure.[6]

---

2 Ibid.

3 Ibid.

4 US Department of Homeland Security, "Sector-Specific Agencies", available at https://www.dhs.gov/sector-specific-agencies, accessed on 07 November 2016.

5 US Department of Homeland Security, "National Infrastructure Protection Plan 2013", p. 1, available at https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf, accessed on 11 November 2016.

6 Ibid, p. 9.

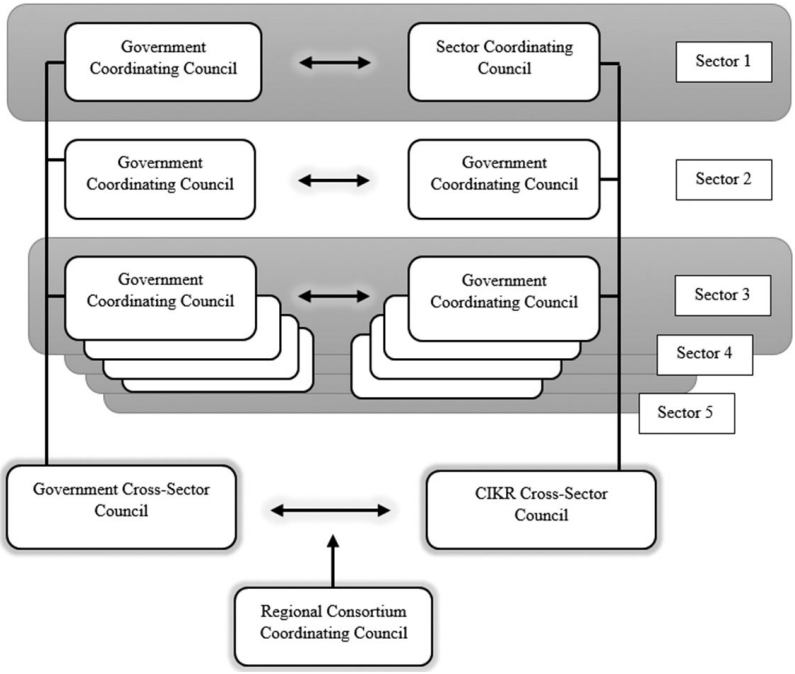
As a guiding policy document, the NIPP 2013 is a prime example for partnerships among owners and operators: federal, state, local, tribal and territorial governments; regional entities; non-profit organizations; and academia.

Table 6.1. Critical Infrastructure Sectors and Respective Sector-Specific Agency

Critical Infrastructure Sector	Sector-Specific Agency
Chemical	Department of Homeland Security
Commercial Facilities	
Communications	
Critical Manufacturing	
Dams	
Emergency Services	
Information Technology	
Nuclear Reactors, Materials and Waste	
Defense Industrial Base	Department of Defense
Energy	Department of Energy
Financial Services	Department of the Treasury
Food and Agriculture Department	Department of Agriculture and of Health and Human Services
Government Facilities	Department of Homeland Security and General Services Administration
Healthcare and Public Health Services	Department of Health and Human
Transportation Systems	Department of Homeland Security and Department of Transportation
Water and Wastewater Systems	Environmental Protection Agency

***Source*:** US Department of Homeland Security, available at https://www.dhs.gov/critical-infrastructure-sectors.

Figure 6.1: Public-Private Partnership Framework in the US



***Source*:** US Department of Homeland Security, available at https://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing.

***Note*:** CIKR: Critical Infrastructure and Key Resources.

Figure 6.1 gives a snapshot of the public-private partnership framework in the US and the interactions among and between the coordinating and cross-sector councils. The present mechanism in the US has evolved over the time, since first Presidential Decision Directive on Critical Infrastructure Protection was signed in 1998. It involves definite roles and responsibilities, representation and requirements of all the stakeholders that is, owners, operators, governance at all strata and research institutions. The NIPP is one of the mature partnership-based models in the world.

The Sector Coordinating Councils are self-organized, self-run and self-governed private sector councils, with representation from owners

and operators, facilitating discussion on wide range of sector-specific strategies, policies, activities and issues.[7] The Critical Infrastructure Cross-Sector Council consists of the chairs and vice-chairs of the Sector Coordinating Councils; this private sector council coordinates cross-sector issues, initiatives and interdependencies.[8] Government Coordinating Councils consist of representatives from various levels of government; and they enable inter-agency, intergovernmental and cross-jurisdictional coordination within and across sectors and partner with Sector Coordinating Councils on public–private efforts.[9]

Similarly, there are other councils: Federal Senior Leadership Council, consisting of senior officials from the SSAs and other federal departments and agencies; State, Local, Tribal, and Territorial Government Coordinating Council, consisting of representatives from across state, local, tribal, and territorial government entities; and Regional Consortium Coordinating Council, comprising of regional groups and coalitions, for integrating efforts, expertise, interests and representation of all the partners in national critical infrastructure security and resilience.

It is observed that the CIP policy implementation in the US has shifted from a completely private–public cooperative-led mechanism to an arrangement where the government has definite powers to exercise and guide the institutions or enterprises, in addition to supervising the implementation of CIP policies. Cross-Sector Councils are pivotal in harmonizing cross-sector issues and interpreting the complex interdependencies within the sectors. Most important, the government, from time to time, has taken strong steps in the form of executive orders, underscoring the quantum of significance CIP holds for the US.

6.1.2 CIIP in Australia

The *Critical Infrastructure Resilience Strategy* sets out the Australian government's approach to ensure the resiliency of its critical

---

7 Ibid, pp. 10–12.

8 Ibid.

9 Ibid.

infrastructure.[10] Although the government is deemed to have an active role in the protection of critical infrastructure, it is considered to be a matter of responsibility and good corporate governance, where the owners/operators of critical infrastructure address the security of their assets and continuity of their respective business functions.[11] The implementation of strategy is through a broadly non-regulatory business–government partnership model, with the objective of managing foreseeable risks to the continuity of operations through: (a) mature, risk-based approach; and (b) an organizational resilience approach.[12] The guidelines warrant the owners/operators of critical infrastructure to consider an "all-hazards" management approach to their operations, termed as critical infrastructure resilience (CIR). It includes natural disasters, pandemics, negligence, accidents, criminal activity, computer network attack and terrorism. The Australian government supports CIR through a Trusted Information Sharing Network (TISN) and the Critical Infrastructure Advisory Council (CIAC).[13]

The Government of Australia established TISN in 2003. Since then, it has been Australia's primary national engagement mechanism for business–government information-sharing and resilience-building initiatives on critical infrastructure. It provides a secure environment for critical infrastructure owners and operators across seven sector

---

[10] Australian Government, "The Trusted Information Sharing Network", *Australian National Security*, available at https://www.nationalsecurity.gov.au/Securityandyourcommunity/Pages/default.aspx, accessed on 11 November 2016.

[11] Australia–New Zealand Counter-Terrorism Committee, "National Guidelines for Protecting Critical Infrastructure from Terrorism", 2015, p. 3, available at https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf, accessed on 11 November 2016.

[12] Australian Government, "Critical Infrastructure Resilience Strategy: Plan", 2015, p. 1, available at http://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlan.PDF, accessed on 11 November 2016.

[13] n. 10, p. 3.

groups to regularly share information.[14] With the participation of governmental regulatory agencies from sectors such as aviation, communications, offshore oil and gas and banking, the TISN provides an important informal link between industry sectors and the agencies that regulate their activities.[15]

Australia's federal governance system warrants intergovernmental work among the Australian state and territory governments which own and operate some of the critical infrastructure, bearing different direct responsibilities.[16] The *Critical Infrastructure Resilience Strategy* complements the existing critical infrastructure programmes under the respective jurisdictions of state and territory governments. The state and territory governments are also key participants in the TISN.

In addition, there are specialist forums, known as Cross-Sectoral Interest Groups, which assist in exploring solutions for cross-cutting issues, and a Resilience Expert Advisory Group which is bound towards organizational resilience. The CIAC provides coordination and strategic guidance, and it consists of the chairs of each of the TISN groups, senior Australian government representatives and senior state and territory government representatives.[17] The practice is driven by owners and operators of seven sector-specific groups and is overseen by the CIAC. The Industry Consultation on National Security (ICONS), as a primary business–government engagement mechanism on national security matters, facilitates direct engagement between the business leaders and Attorney-General.[18]

Figure 6.1 gives a snapshot of the critical infrastructure protection apparatus in Australia and the placement of different departments,

---

[14] Australian Government, "Trusted Information Sharing Network for Critical Infrastructure Resilience", available at http://www.tisn.gov.au/Pages/default.aspx, accessed on 11 November 2016.

[15] n. 11, p. 4.

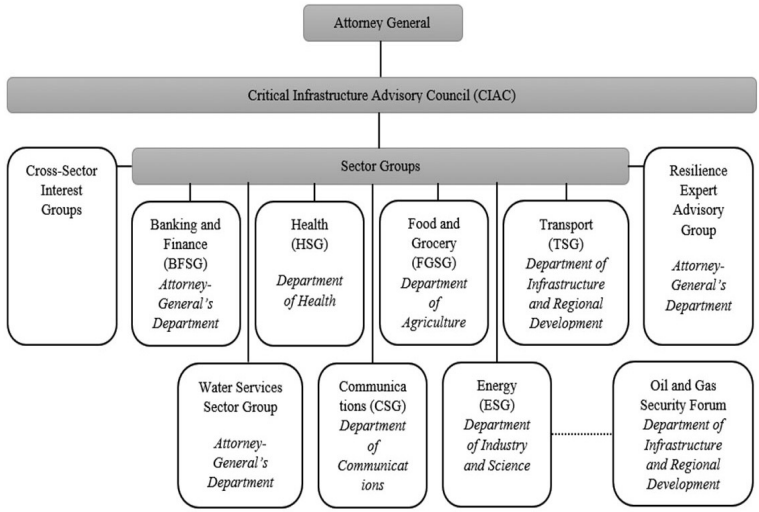
[16] Ibid.

[17] n. 11, p. 2.

[18] n. 11, p. 3.

their sector groups under the purview of CIAC and the office of Attorney-General.

Figure 6.2: Critical Infrastructure Protection Apparatus in Australia



***Source*:** Australian Government, "Trusted Information Sharing Network for Critical Infrastructure Resilience", available at http://www.tisn.gov.au/Pages/default.aspx.

Australia's Critical Infrastructure Resilience Strategy lays down four key outcomes of the strategy with definite action points, and it is due for a review in 2020. As part of the activities, identifying the key elements of Australia's critical infrastructure and dependencies is the first firm step in the implementation of the strategy. This would assist the owners and operators to prioritize measures and focus on the areas which need immediate attention, given the complexity and resource constrains of CIP, and also outline the national understanding of the systems, networks, assets and dependencies that are most critical at the organizational and sectoral levels. Australian strategy for CIP has the right blend of governmental control and guidance, augmented by a conducive partnership environment for information sharing (through both formal and informal networks/links) between the businesses/

private players and all the tiers of governments (both state and territory). The TISN and non-regulatory business–government partnership model are the prime highlights and takeaways for any national CIP strategy.

6.1.3 CIIP in the UK

The strategic framework for resilience of critical infrastructure in the UK works under the purview of Cabinet Office of the government. The infrastructure is categorized according to its value or "criticality" and the impact of its loss using a criticality scale, so that the critical elements within the infrastructure receive the utmost priority. The criticality scale includes three impact dimensions: (a) impact on delivery of the nation's essential services; (b) economic impact (arising from the loss of essential services); and (c) impact on life (arising from the loss of essential services).[19] The details are laid out in the sector resilience plan, which has evolved over five revisions since 2010. The plan is produced annually and identifies the relevant risks.

As a strategic step, the National Cyber Security Centre (NCSC) was established in October 2016 as the UK's authority on cyber security. As part of the Government Communications Headquarters (GCHQ), NCSC has absorbed and replaced the Communications–Electronics Security Group (CESG; the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), CERT UK and the cyber-related responsibilities of Centre for the Protection of National Infrastructure (CPNI).[20] The NCSC works with other government agencies and departments, law enforcement, defence, intelligence and security agencies and international partners.[21]

The CPNI is charged with the responsibility to provide protective security advice on all the three fronts, namely, physical security, personnel

---

[19] CPNI, "Critical National Infrastructure", available at http://www.cpni.gov.uk/about/cni/, accessed on 12 November 2016.

[20] NCSC, "About Us", available at https://www.ncsc.gov.uk/about-us, accessed on 15 March 2017.

[21] Ibid.

security and cyber security/information assurance (which has been absorbed into NCSC). The "protective security" methodology, more about "building into design", adopts security measures or protocols to deter, detect or minimize the consequences of an attack.[22] The CPNI's protective security advice is built on a combination of inputs from the research and development programmes and national security threat perception, leveraging the expertise and the partnership of public and private sectors. The CPNI works in close collaboration with some key partners, such as the National Counter Terrorism Security Office, the Counter Terrorism Security Advisor (CTSA) network and the recently established NSCS (previously it was the National Technical Authority for Information Assurance–CESG).[23] As a standard practice, government departments lead the responsibility of protective security within their respective sectors, and they work in consultation with CPNI and sectoral organizations. Table 6.2 enlists the Critical Sectors designated by the Government of UK and the respective departments of the government assigned with the lead responsibility for the specific sectors.[24]

In response to the emerging cyber threats, the government had set up the Office of Cyber Security and Information Assurance (OCSIA) and the Cyber Security Operations Centre (CSOC) in 2010. The CPNI also works closely with OCSIA, CSOC and NCSC to drive the cyber security programme of the Government of UK. As an operational requisite, CPNI has built relationships with organizations and businesses that own or operate the national infrastructure, and the flow of information is through various means, such as face-to-face advice, trainings, online advice and written advisory products.[25]

---

[22] CPNI, "About CPNI", available at http://www.cpni.gov.uk/about/, accessed on 12 November 2016

[23] CPNI, "Who we Work with", available at http://www.cpni.gov.uk/about/Who-we-work-with/, accessed on 12 November 2016.

[24] Ibid.

[25] Ibid.

Table 6.2: Critical Sectors and the Respective Departments with Lead Responsibility

Critical Sector	Departments with Lead Responsibility
Communications	Department for Business, Innovation and Skills
Emergency services	Department for Business, Innovation and Skills
Ambulance	Department of Health
Fire	Department for Communities and Local Government
Maritime and Coastguard Agency	Department for Transport
Police	Home Office
Energy	Department for Energy and Climate Change
Finance	HM Treasury
Food	Department for the Environment, Food & Rural Affairs and Food Standards Agency
Government	Cabinet Office
Health	Department of Health
Transport	Department for Transport
Water	Department for the Environment, Food & Rural Affairs

Source: Cabinet Office of the Government of UK, "Summary of the 2015-16 Sector Resilience Plans", p. 6.

The CIP initiative in the UK is primarily government driven, with the government departments leading every sector, which is part of the national critical infrastructure. The scientific inputs in this emerging area of national security implications, through research and development programmes, are an integral part of the innovative methodology of "protective security". Protective security interlaces the much-desired national threat perception and is based upon an "all-risks" model encompassing terrorist and espionage threats and natural hazards.

The integration of all cyber security-related efforts under the NCSC draws in the synergies of expertise and experience from all the agencies/

departments tasked with cyber security across the UK, be it the intelligence agencies, the emergency response teams or the CPNI. The sheer focus of the sector resilience plan on identifying the criticalities and interdependencies within the infrastructures using a structured scale and scientific methodology is a key differentiator. This equips the owners and operators with a clear understanding and view of the interdependencies and the assets they need to prioritize for security. Furthermore, the yearly revision of sector resilience plan encapsulates dynamic threat perception, incorporating new learning and developments periodically and keeping it relevant throughout.

6.1.4 CIIP in China

In the recent past, China has passed a law on cybersecurity and promulgated an international strategy for cooperation in the cyberspace. Given the deep interest of Chinese political leadership in cybersecruity, CIIP must be among the top priorities of the government. China's Cyber Security Law of November 2016 defines the national CII as:

> the information facilities that are related to national security, national economy and people's livelihood, which have been damaged, destroyed or lost, may seriously endanger the national security and public interests, including but not limited to the provision of public communication, radio and television transmission Information network, energy, finance, transportation, education, scientific research, water conservancy, industrial manufacturing, health care, social security, public utilities and other areas of important information systems, important Internet applications.[26]

The law accounts the information infrastructure protection as common responsibility of the government, enterprises and society as a whole, and accentuates the protection of CIIs through a combination of

---

[26] "National Cyberspace Security Strategy: Full Text", *People.com*, 27 December 2016, available at http://politics.people.com.cn/n1/2016/1227/c1001-28980829.html, accessed on 10 March 2017.

technology and management, protection and deterrence simultaneously.[27]

China has recently published an "International Strategy of Cooperation on Cyberspace" in March 2017. The strategy has a section on "Global Information Infrastructure Development and Protection", which affirms China's willingness to strengthen global information infrastructure, promote information infrastructure connectivity and raise the awareness of CIIP through a mechanism bringing governments, industries and enterprises together.[28]

There is a dearth of information regarding the policies and organizations governing or driving the protection of CII in China. Besides definitions, as part of the Cyber Security Law and the "International Strategy of Cooperation on Cyberspace" document, information regarding the developments or the steps undertaken in this regard is inadequate to form any analysis. In general, amendments in domestic laws, executive orders from the government or policy documents defining the terms and alluding the mechanisms are a precursor to the steps towards CIIP.

Therefore, it is quite likely that the Government of China has recently inferred the imperatives of CII and already moved the necessary resources in this direction. It is also noteworthy that the Chinese Government has underscored the role of industries and enterprises in this endeavour, which paves the way for a collaborative model between the government and the private sector, as is practised across the globe and essential for this colossal task.

6.1.5 CIIP in India

India has elevated its response to protect CII in the recent years. The legal framework to address the threats emanating from cyberspace to the CII, especially from cyber terrorism, was developed in the amendment made in 2008 to the IT Act, 2000. Section 66F of IT

---

[27] Ibid.

[28] "Full text: International Strategy of Cooperation on Cyberspace", *Xinhua*, 01 March 2017, available at http://news.xinhuanet.com/english/china/2017-03/01/c_136094371_5.htm, accessed on 10 March 2017.

(Amendment) Act, 2008 identifies cyber terrorism as a threat to CII as it could be used to "threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people". It notes that the computer resources might be used to conduct causes leading to death or injuries to persons, or damage to or destruction of property, or damage or disruption of supplies or services essential to the life of the community or adversely affect the CII.[29] Section 70A of the Act designates an organization of the government as the national nodal agency responsible for all measures, including research and development relating to the protection of CII. The GoI has notified NCIIPC, under the auspices of National Technical Research Organisation, as the nodal agency with respect to CIIP, vide *Gazette of India* notification of 16 January 2014.[30]

The NCIIPC aims to reduce the vulnerabilities of CII against cyber terrorism, cyber warfare and other threats. It is tasked with: identification of all CII elements; providing strategic leadership and coherence across government; and coordinating, sharing, monitoring, collecting, analyzing and forecasting national level threat to CII for policy guidance, expertise sharing and situational awareness.[31] The NCIIPC is developing and executing national and international cooperation strategies for protection of CII across India. As part of its mandate, it issues guidelines, advisories and vulnerability or audit notes to the CII operators. It holds consultations with the stakeholders and works in close coordination with Indian computer emergency response team (CERT-In) and other organizations working in the domain of CIP and cyber security.[32]

Since inception, NCIIPC has held multiple consultations with the stakeholders, generating awareness among the public and private

---

[29] Ministry of Law, Justice and Company Affairs, GoI, "The Information Technology Act, 2008", p. 25, available at http://meghpol.nic.in/acts/central/it_act_2000_2008_amendment.pdf, accessed on 04 July 2016.

[30] NCIIPC, "About Us", available at https://nciipc.gov.in, accessed on 13 November 2016.

[31] Ibid.

[32] Ibid.

enterprises, sensitizing the senior management with the imperatives of critical infrastructure and facilitating the organizations that are part of the CII across India. The NCIIPC has published control guidelines, a framework for evaluating cyber security and standard operating procedures for auditing/incident reporting,[33] which is essential to ensure that relevant security mechanisms are built into CII facilities as key design features.[34]

The NCIIPC Advisory Committee has representation from the Ministry of Home Affairs, Ministry of Law and Justice, Department of Telecommunications, Ministry of Electronics and IT (MeitY); Ministry of Defence, CERT-In, National Security Council Secretariat and the Cabinet Secretariat of the GoI. It has representation from the Intelligence Bureau and industry and state governments as well. The requirements have been set forth for critical sector organizations and ministries, such as: to appoint a Chief Information Security Officer (CISO) as the point of contact for all interactions with NCIIPC; identify critical business processes and assets; and implementation of controls. The CIIP strategy of India is moving towards a collaborative model where private sector is part of the initiatives taken by the government through continuous engagement. In such a move, joint working groups are being set up by NCIIPC with representatives of industry associations to bring out guidelines for protection of CII in India.

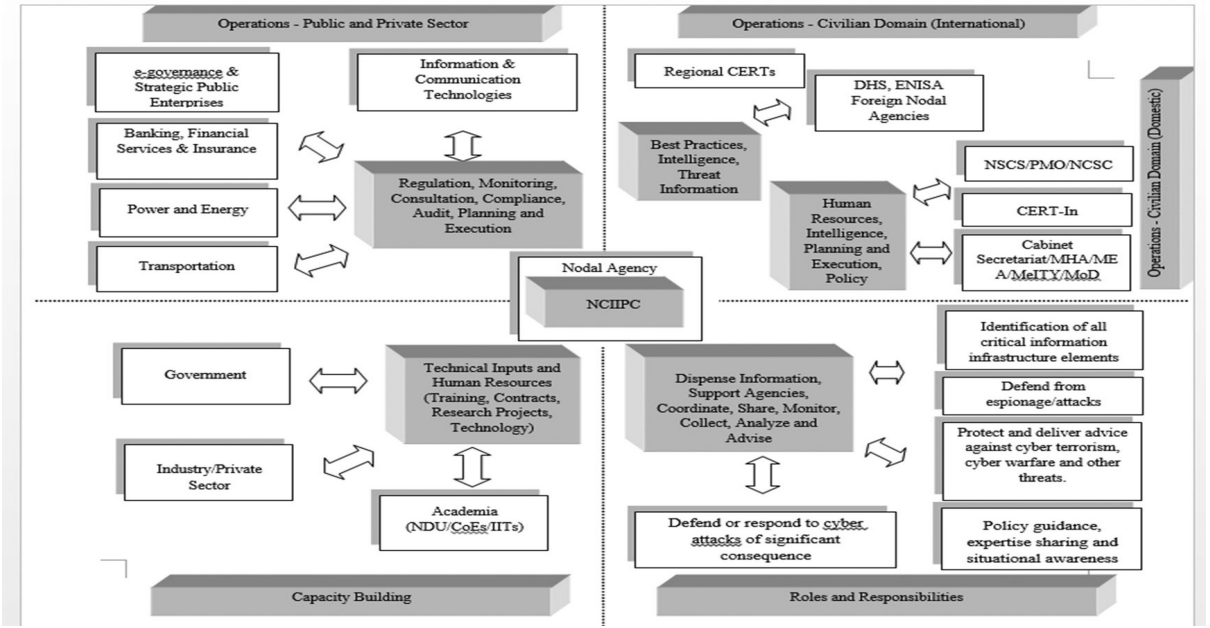
The NCIIPC has assumed a central role in CIIP, and it would be in the best interests of the agency as well as the key stakeholders that it functions as a networked agency, rather than a traditional hierarchy-oriented organization. Figure 6.3 illustrates the possible interactions between NCIIPC and other stakeholders, their roles and responsibilities and operational aspects in the civilian space.

---

[33] Ibid.

[34] NCIIPC, *Guidelines for Protection of Critical Information Infrastructure*, Version 2.0, 16 January 2015, p. 1, available at http://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf, accessed on 22 March 2017.

Figure 6.3: Critical Information Infrastructure Protection in India: Possible Interactions among the Stakeholders



***Source*:** Compiled by the author.

The NCIIPC would have a two-way relation with every player in this domain. First and foremost, it would need to exchange expertise/ intelligence with CERT-In, National Security Council Secretariat, National Cyber Security Coordinator, Ministry of Home Affairs, Ministry of External Affairs and Ministry of Defence. Then, it is required to have professional relations with CIIP agencies abroad, such as Department of Homeland Security of the US, ENISA or CPNI of the UK, for intelligence and threat information exchange.

Similarly, technical and policy inputs from academia, industry and centres of excellence in cyber security technology/policy research would be essential to its capacity building. The NCIIPC would continue to foster strong operational linkages with the public and private sector players in the identified critical infrastructure sectors.

However, there has been an inordinate delay between provisioning a nodal agency for CIIP under the legislation (IT Act) in 2008 to the gazette notification of NCIIPC in January 2014. There are certain ambiguities pertaining to the administrative aspects of NCIIPC as it functions under the auspices of NTRO, India's premiere technical intelligence agency. Agencies tasked with CIIP are required to work in close coordination with both the private and public sector enterprises as equal partners in this endeavour. The NCIIPC, under the administrative control of an intelligence agency, might lead to interference with the multi-stakeholder, consultative, collaborative and open approach, which it aspires to adopt in delivering the responsibilities.

Despite the delays and operational challenges, in a short span of time, NCIIPC has gained the much-desired momentum to start sensitizing the CII operators in India and forge a partnership-based corroborative model, rather than a mere regulatory one. It has held various workshops across India and has interacted candidly with the private sector as well as the public sector enterprises to initiate consultations and understand the concerns of the key players in this domain. The NCIIPC identifies five principle stakeholders: the CII owner/operator; service providers to the CII; NCIIPC; the CERT-In; and law enforcement agencies.

In addition to security audits conducted for some of the identified critical sectors on a priority basis, NCIIPC has also managed to lay down a draft of manual for cyber security specific to the controls and

requirements of the power sector,[35] after consultation with the respective stakeholders. Owing to the efforts of the NCIIPC, the Unique Identification Authority of India (UIDAI) has been declared STQC ISO 27001:2013 certified, and has also been identified to be declared as "Critical Infrastructure", thereby adding another layer of IT security assurance.[36] The NCIIPC is constantly working towards identifying and recognizing GoI's vital systems as "protected systems",[37] so that the security of these systems and their assets lies within the area of responsibility of the NCIIPC.

6.2 Multilateral Platforms

6.2.1 CIIP in the EU

The EU initiative on CIIP aims to strengthen the security and resilience of vital ICT infrastructures by stimulating and supporting the development of a high level of preparedness, security and resilience capabilities both at national and European level. The European Programme for Critical Infrastructure Protection (EPCIP) is the directive for identification and designation of European critical infrastructures, which identifies the ICT sector as a future priority sector. It focuses on the global dimension of the challenges and the importance of boosting cooperation among member states and the private sector at national, European and international level, in order to address global interdependencies.[38] The strategy to tackle security challenges is based

---

[35] Released at the India Smart Grid Week organized by India Smart Grid Forum in February 2016.

[36] Press Information Bureau, GoI, "Making Aadhar Card Mandatory for Digital India Programme Schemes", Ministry of Communications & Information Technology, 04 December 2015, available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=132521, accessed on 13 November 2016.

[37] Once an entity is notified as a "protected system", any form of cyber-attack on it amounts to the offence of cyber terrorism under Section 66(F) of the IT Act (Amended), 2008, with the quantum of punishment from three years imprisonment to life imprisonment.

[38] "Critical Information Infrastructure Protection", available at http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm, accessed on 05 November 2016.

upon a three-pronged approach: specific network and information security (NIS) measures; the regulatory framework for electronic communications (which includes privacy and data protection issues); and the fight against cyber-crime. The strategy includes certain activities such as improving the security and resilience of NIS, developing multi-stakeholder dialogues, building partnerships for data collection and alert system and promoting international cooperation on NIS.[39]

The EPCIP sets forth the overall framework for activities aimed at improving the protection of critical infrastructure in Europe—across all member states and in all relevant sectors of economic activity. The programme aims to respond to a cross-section of threats, such as terrorism, criminal activities, natural disasters and other causes of accidents, basically adopting an "all-hazard" cross-sectoral approach.[40] A key pillar of this programme is the 2008 directive on European critical infrastructures, which established a procedure for identifying and designating European critical infrastructures (ECI) and a common approach to enhance their protection. The directive applies specifically to the energy and transport sectors.[41] A Critical Infrastructure Warning Information Network (CIWIN) under the EPCIP is a communication system for exchanging information, studies and best practices across the member states. Going forward, the EPCIP plans to extend its scope to EU-wide electricity transmission grid, gas transmission network, air traffic management and GALILEO (European programme for global satellite navigation).[42]

---

39 "A Strategy for Secure Information Society—Dialogue, Partnership and Empowerment", available at http://ec.europa.eu/information_society/policy/nis/strategy/activities/index_en.htm, accessed on 05 November 2016.

40 European Commission, "Critical Infrastructure", available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm, accessed on 05 November 2016.

41 Ibid.

42 European Commission, "Protection of Critical Infrastructure", available at http://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure, accessed on 05 November 2016.

In March 2009, the European Commission had adopted a policy initiative on CIIP to address this challenge and a European Public–Private Partnership for Resilience (EP3R) was established in order to support such coordination.[43] A number of EU member states have gained substantial experience with public–private partnerships, where they have brought together key stakeholders, including government departments, national agencies, regulators and industry. Incentives for a cooperative partnership between public and private sectors have been recognized by many stakeholders, such as economic and qualitative incentives deriving from information sharing.[44] The EP3R engages with national public–private partnerships to address CIIP issues at the European level.[45] It sets out the work to be done under each pillar by the Commission, the member states and/or industry, with the support of ENISA.[46] In the environment where CIIs operate, it is imperative to bring together key stakeholders, including government departments, national agencies, regulators and industry, to elevate the level of preparedness.

The ENISA was established in 2004 to contribute to the goals of "ensuring a high and effective level of NIS within the European

---

[43] ENISA, "European Public Private Partnership for Resilience", available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r, accessed on 05 November 2016.

[44] ENISA, "Cooperative Models for Effective Public Private Partnerships", 2011, p. 11, available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps, accessed on 05 November 2016.

[45] ENISA, "Public Private Partnerships", available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership, accessed on 05 November 2016.

[46] The ENISA is an EU agency which acts as a centre of expertise for the EU member states and European institutions. It gives advice and recommendations on good practice, and acts as a "switchboard" for exchanging knowledge and information. The agency also facilitates contacts between the European institutions, the member states and private business and industry.

Community" and developing a culture of NIS for the benefit of EU citizens, consumers, enterprises and administrations. The EU is an exemplary case study and model for other regions, where infrastructures (electricity grids, transportation, civil aviation, navigation services and energy pipelines) are closely knit. The CIIs across Europe are highly interconnected, and their security and resiliency ought to be a shared objective and key priority. The EU has to work with all governments of member states to find the common denominators; however, the regimes to ensure the security and resilience of CIIs, as well as the level of expertise and preparedness, differ across member states.[47] There are significant differences in national approaches, and the effectiveness of this shared governance mechanism also depends upon access to reliable information.[48] With different political entities (member states) under the aegis of a unified/shared model of governance in the form of the EU, information sharing for reliable and actionable data and corroboration with the private sector is desirable and much anticipated.

6.2.2 CIIP at the UN GGE

The 2015 UN GGE report underscores the issue of attacks targeted against the critical infrastructure and associated information systems of a state, under "Existing and Emerging Threats", designating it to be "real and serious".[49] The report lays down "Norms, rules and principles for the responsible behaviour of States". In this context, as "A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of

---

[47] Commission of the European Communities, "Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, Brussels, 30 March 2009, pp. 5–6.

[48] Ibid.

[49] UNGA, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 22 July 2015, p. 6, available at http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174, accessed on 05 December 2016.

critical infrastructure to provide services to the public"; and "States should take appropriate measures to protect their critical infrastructure from ICT threats", it compels the states to:

> respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.[50]

The report further suggests confidence-building measures for states, although voluntary in nature, "to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders" and to develop "mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure".[51]

The UN GGE report has opened up space for discussions over possibility of defining norms and principles for the responsible behaviour of states. Given the strategic importance of critical infrastructure and the unfolding risks from a myriad of threats, non-binding mechanisms in form of norms and principles might be an ineffective measure. This would be incapable of deterring nation states and non-state actors from attacking the critical infrastructure or the corresponding CII. However, it is a welcome move as a beginning step to bring CIIP-related issues on the discussion table at the United Nations.

6.2.3 CIIP and the G8 Countries

The G8 countries have adopted "Principles for Protecting Critical Information Infrastructures", which include identifying threats to and reducing the vulnerability to damage or attack, minimizing damage and recovery time and identifying the cause of damage or the source

---

[50] Ibid, p. 8.

[51] Ibid, p. 9.

of attack for analysis by experts and/or investigation by law enforcement agencies. The countries have agreed upon the importance of communication, coordination and cooperation, nationally and internationally, among all stakeholders—industry, academia, the private sector and government entities, including infrastructure protection and law enforcement agencies—for effective protection.[52] The principles, which encourage G8 countries to develop strategies to reduce risks to the CII, revolve around establishing emergency warning networks regarding cyber vulnerabilities, threats and incidents; raising awareness and promoting partnership among the stakeholders; examining infrastructures and identifying interdependencies among them; maintaining crisis communication networks; deploying contingency plans; devising procedural laws; and training manpower to investigate and prosecute attacks on CIIs. The principles urge the countries to engage in international cooperation and coordinate investigations of attacks on such infrastructures in accordance with domestic laws.[53]

6.2.4 CIIP and the Meridian Process

The Meridian Process, as a multilateral platform for government officials, aims to facilitate extensive exchange of ideas and cooperation among the governmental bodies on the issues pertaining to CIIP.[54] Over the years, it has created a community of senior government policymakers in CIIP; it is open to all countries/economies willing to foster international collaboration on CIIP issues of mutual concern. The Meridian annual conference, the flagship event of the Meridian Process since 2005, is a forum for government delegates, promoting open discussion and exchange of ideas without any commercial pressures.[55] The conference has discussed a range of policy issues, such

---

[52] "G8 Principles for Protecting Critical Information Infrastructures", Adopted by the G8 Justice & Interior Ministers, May 2003, p. 1, available at http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf, accessed on 05 December 2016.

[53] Ibid.

[54] "The Meridian Process", available at https://www.meridianprocess.org/, accessed on 05 December 2016.

[55] Ibid.

as "information sharing between governments and the private sector, as well as between governments internationally, for good risk assessments" at Budapest in 2006; "issues arising from globalization and the impact of new technologies that affect the development of national policies for the protection of critical services and the underlying information infrastructure" at Stockholm in 2007; and "CIIP and the international interdependencies" at Qatar in 2011.[56] The subsequent editions of the annual conference in Berlin (2012), Buenos Aires (2013), Tokyo (2014) and Leon (2015) delved on the dimensions of economy, legislation and preparedness.

6.2.5 CIIP in OECD

The recommendations of the OECD Council on the Protection of Critical Information Infrastructure provide a policy framework for the development of national policies and international cooperation for CIIP. The recommendations reflect the central role of the governments, in form of their leadership to steer CIIP, manage the risks and foster partnership with the private sector.[57] It highlights the importance of bilateral and multilateral cooperation at regional and global levels as well. At OECD, Working Party on Information Security and Privacy of the Committee for Information, Computers and Communications Policy spearheads the CIIP initiative.[58]

The OECD recognizes that their economies and societies rely on information systems and networks that are interconnected and interdependent, domestically and across borders, and their protection is a priority area for national policy and international cooperation.[59] The recommendations of the OECD Council on the Protection of

---

[56] "Previous Conferences of the Meridian Process", available at https://www.meridianprocess.org/the-conference/previous-conferences/, accessed on 05 December 2016.

[57] OECD, "Critical Information Infrastructures Protection (CIIP)", available at http://www.oecd.org/sti/ieconomy/ciip.htm, accessed on 05 December 2016.

[58] Ibid.

[59] OECD, "OECD Recommendation of the Council on the Protection of Critical Information Infrastructures", available at https://www.oecd.org/sti/40825404.pdf, accessed on 05 December 2016.

Critical Information Infrastructure underscore the need to share knowledge and experience in developing policies and practices; coordination at the domestic front and across borders, especially with the private sector—the owners and operators of such infrastructures; and the importance of risk assessment process.[60]

They lay down principles for the governments to provide leadership and commitment, by means of clear policy objectives at the highest level of government; designating government agencies and organizations with responsibility and authority to implement these policy objectives; and manage risks to CII by considering interdependencies, conducting risk assessment based on the analysis of vulnerabilities and the threats to the CII and ensuring preparedness, including prevention, protection, response and recovery from natural and malicious threats.[61] Moreover, the recommendations mention the development of common understanding of "risk management" for cross-border dependencies and interdependencies, generic vulnerabilities, threats and impacts on the CII, and to address the security flaws or the spread of malicious software.[62]

Critical information infrastructure protection, as a global governance and policy issue, has gained significant traction in the last one decade, since the UNGA adopted Resolution 58/199 on "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures" in the year 2004. The resolution had put forward the onus of determining CIIs on the member states, while noting the increasing links among the countries' critical infrastructures, such as the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health.[63] Thereupon, all the multilateral

---

60 Ibid.

61 Ibid.

62 Ibid.

63 UNGA, "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures", Resolution 58/199 adopted by the General Assembly, 30 January 2004, p. 3, available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf, accessed on 05 December 2016.

platforms have drawn attention of the policymakers towards the interdependencies and complexities of CII components, and their exposure to the wide variety of threats and vulnerabilities as a result of interconnectivity, which cuts across political borders. Cooperation at regional and international forums is pivotal, as they are the right platforms for nation states to establish emergency warning networks regarding vulnerabilities, threats and incidents, and mechanisms for investigating attacks on such infrastructures. It is an operational imperative for the governments to work in cohesion with each other, and these multilateral platforms augment the national efforts as states are at different degree of maturity in terms of their domestic policies, regulations and legislations.

6.3 Lessons for India

The efforts regarding CIIP have distinguishing characteristics and tenets, and some of them are useful as case studies to draw lessons. Since CIIP is an evolving process, best of the models available could be studied and reflected upon in domestic policy initiatives. The SSAs in the case of the US and assigning lead government departments in the case of the UK take into account the unique characteristics and conditions of their specific sectors, and this approach could be helpful for India as well. In a similar way, self-organized, self-run and self-governed private sector councils, known as Sector Coordinating Councils, are requisite for India to facilitate discussion and representation of owners and operators of critical infrastructure.

Cross-sector coordination, based on the model of Critical Infrastructure Cross-Sector Council in the US, is also essential for India to coordinate most important cross-sector issues, initiatives and interdependencies. In order to strengthen national understanding of the systems, networks, assets and dependencies (across organizational, sectoral and national levels), the practices in Australia and the UK are beneficial to draw lessons from. The UK strategy also lays emphasis on "criticality" as a measure to identify the critical elements within the infrastructure to allocate utmost priority. Such a qualitative/quantitative approach would certainly aid the policymakers in India to zero in on the priority areas.

The TISN of Australia and the active participation of governmental regulatory agencies from sectors such as aviation, communications, offshore oil and gas and banking are prime case studies for India. In the absence of trust, information sharing is a futile exercise. Information sharing could also be enabled over informal links between industry sectors and the regulators. The lack of a platform where national security matters can be discussed over business–government engagement can be overcome with a set-up on the lines of ICONS in Australia.

As domestic and multilateral efforts gain thrust, the policies and strategies tend to exhibit some trends. There are certain commonalities, characteristics and understandings arising out of different national critical infrastructure/CII protection strategies/policies. The next chapter underscores these emerging trends and throws light on the way forward.

Chapter 7

Emerging Trends for Policymaking

Nation states across the globe have begun approaching CIIP as an integral part of their national security calculus. In the last decade-and-a-half, ever since acts of terrorism against critical infrastructure—be it New York, Madrid, London or Mumbai—have altered the threat perceptions, a wide range of political and administrative initiatives have been experimented with and thereupon developed. With varying degrees of maturity and different policy–industrial–economic dynamics, specific solutions have been devised. Some aspects of each of these solutions are a great source of learning for other nations. Some trends can be discerned in the emerging global discourse on CIIP and they are as follows:

1. *Identifying Critical Assets/Processes/Systems*: The identification of critical assets/processes/systems within the critical infrastructure sectors is the foundation of an effective CIP policy or strategy. This exercise begins at the organizational level, where every department or unit is involved to provide an assessment of the assets. There is a general acceptance of two facts: (a) not all the elements of critical infrastructure are critical; and (b) it is practically impossible to secure each and every element of critical infrastructure, all the time, from all probable threats, and that is due to various technical and financial constraints. Given the extent of operations, criticality assessment is indispensable, as explained in the sector resilience plan of the UK. The NCIIPC framework for evaluating cyber security in CII also requires organizations to identify critical business processes, cyber assets and criticalities.

2. *Detangling Interdependencies*: One of the primary reasons for critical infrastructure being so complex is the cascade of dependencies and the web of interdependencies. Practitioners, management or

risk analysts, keep a close tab on the incoming dependencies; the factors which influence the capacity of the organization to deliver its products or services. On a daily basis, every unit of every organization conducts this risk analysis. However, the lack of scientific analysis and tools for comprehending inter-sector and intra-sector dependencies is the primary reason that interdependencies have not been understood adequately.

As discussed earlier, innovative simulations or software tools to model the flow of entities, services and materials are a direct outcome of the national policies marking interdependencies as a priority area for advanced research. The NIPP of the US, evaluation framework of NCIIPC in India or the policy initiative on CIIP of the EU, all have laid prime focus on interdependencies.

3. *Focus on Critical Infrastructure Resilience* : Despite best of the technology, management or security policies and practices at one's disposal, it is practically impossible to secure all critical elements of infrastructure against all eventualities. The evolving trend now is to heighten the resilience of the CII to such an extent that the critical business functions or services are restored at the earliest and cascading effects are mitigated. This is a significant departure from the earlier notions of security, centred on building defences. Since resilience is commonly embedded in processes, rather than individual physical assets,[1] the strategic guidance of Department of Homeland Security of the US, Critical Infrastructure Resilience Strategy of the Australian government, strategic framework for resilience of critical infrastructure in the UK and the Public–Private Partnership for Resilience of the EU are firm steps in this direction. Business continuity and crisis management plans at the organizational level are the building blocks for sectoral and national resiliency of critical infrastructure; therefore, the responsibility and execution lies with the owners and operators of critical infrastructure.

---

[1] Crisis and Risk Network, "Focal Report 1: Critical Infrastructure Protection", Center for Security Studies, ETH Zurich, October 2008, available at http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Focal-Report-1-CIP.pdf, accessed on 06 December 2016.

4. *Adopting an "All-hazards" Approach* : The probability of a threat actor being able to execute an attack exploiting a vulnerability, also termed as likelihood, is a desired input for quantitative risk assessment. In the absence of credible data to support the calculation of likelihood, the new approach emerging from the documented strategies or policy initiatives is to spotlight on the likely effect(s) of the failure of a specific infrastructure or asset and work towards preparedness or mitigation of these adverse effects. A comprehensive protection strategy, in practice, intends to secure the assets and processes irrespective of the nature or attributes of the threats. Preparedness encompasses a broad range of both man-made and natural hazards, which also includes acts of terrorism. From an operator's perspective, the source or cause of the incident is secondary, while the continuity of service and the mitigation of unanticipated cascading effects is the primary task at hand.

5. *Amalgamation of Regulatory and Partnership Models* : Critical infrastructure owners and operators are unevenly spread across the governments, private and public sectors. With deregulation of sectors such as energy, transportation and communication, multiple players with varying degree of maturity in security practices are now part of the critical infrastructure. Over the years, governments have learnt that voluntary participation or adoption of stringent security measures has operational disadvantages. Therefore, after revisions and corrective actions, the new avenue is an amalgamation of both partnership and regulatory models.

   At a strategic level, governments are inclined to enforce supervision over the best practices and guidelines issued for the critical infrastructure sectors. Designating a governmental department as lead agency—the sector-specific departments/agencies in the case of the US, Australia and the UK—serves the dual purpose of coordination and supervision. These agencies/departments have the powers to exercise and guide the institutions or enterprises under their jurisdiction, and supervise the implementation of national CIP policies. The representation of different stakeholders at Sector Coordinating Councils/Cross-Sector Council in the US, Critical Infrastructure Advisory Council in Australia and NCIIPC Advisory Committee in India fosters the partnerships at multiple

strata, between and among the sectors. Moreover, placing all the CIP/CIIP related activities under the aegis of one agency—Department of Homeland Security, NCIIPC, CPNI—suggests that centralization is the emerging trend, under the firm supervision and with direct intervention of the government, given the national security imperatives.

6. *Stratified Information Sharing Network* : Once a strategy and an executive apparatus are in place, information sharing is the key driver of an effective CIP policy initiative. In this respect, scope of information is wide; it encompasses threat information, incident reporting/analysis, best practices, protective measures, advisories, vulnerability or audit notes, crisis management, alerts and warnings. Information sharing is vital to communication, situational awareness, policy implementation, collaboration and coordination. Graduating from the hierarchical model, information sharing now works like a network, and there are multiple agencies, strata and channels, both formal and informal.

   The CIWIN in the EU, TISN in Australia and Homeland Security Information Network–Critical Infrastructure (HSIN-CI) in the US are the examples of overarching information-sharing mechanisms. Information sharing and analysis centres are emerging, which collect, analyze and disseminate actionable information to the members of the relevent sectors. They are playing a significant role in disseminating information to each and every segment of the web of critical infrastructure and in maintaining situational awareness.

The Way Forward

As the global society has moved towards an information age, economies, societies, markets, capital, resources, etc., transact and traverse over networks. Interestingly, their associations and interactions take the form of global networks. Information in digital format exchanges hands across the globe in real time over computer and mobile telephony networks. Information, as an enabler and a vital decision-making asset, gains strategic importance. The basic services, without which it is impossible to imagine the state of life today, such as electricity, transportation, mobile communication or banking, are the core infrastructure on which our modern societies and economies rest. New

business models and products are being built upon the layers of physical and virtual infrastructures.

Communication and networking is the basic need of an enterprise, especially when it operates across different time zones. Time and cost-saving measures have introduced automation, real-time tracking and monitoring, remote control and supervision and IT-related products and services in every business initiative or industrial house. Digital networks, networking devices, databases, enterprise solutions and applications built upon them underpin our critical infrastructures, throwing open numerous challenges for policymakers and security agencies.

The recent developments in the cyber domain have unearthed a whole new dimension of security, due to the vulnerabilities underlying the information infrastructure. Unfortunately, the vulnerabilities are sewn with the infrastructure, and infrastructure is omnipresent. Therefore, vulnerabilities are not restricted to a specific vendor, developer, integrator, country or region. The exploitation of these vulnerabilities in the different layers of the network architecture, mostly in the form of malicious software, serve different objectives of nation states, terror outfits and criminal syndicates.

The security, protection or defence of the CII is a daunting task and efforts have already been elevated at enterprise, national and international strata. A comprehensive protection strategy or defence-in-depth methodology needs to understand and analyze the interconnected, interrelated and highly interdependent nature of the critical infrastructure and their associated information infrastructure. These characteristics have escalated the risks as predicting failures and their cascading effects are practically infeasible to compute through traditional ways and means of risk management. With the growing impetus on research in this arena, simulation tools and scientific analysis of interdependencies, criticalities and their interplay would help the practitioners in solving many practical problems.

The risks arise out of both internal and external threats. Internal threats in the form of individual(s) with the access and/or inside knowledge of a company, organization or enterprise are of the highest order as they are aware of the entity's security, systems, services, products or

facilities. The external threats from foreign governments, their agencies or their agents/proxies pose tremendous risks like crippling of CII, security-related or industrial espionage, and at the most may amount to acts of terrorism or even war.

The technical, practical and financial constraints of comprehensive protection raise the need to undertake criticality analysis of critical infrastructure and CII spread across sovereign territories and, if applicable, beyond the political or geographical boundaries of a nation state. The individual organizations and sector-specific agencies have equally vital roles to play.

Going forward, the protection strategy for critical infrastructure and CII has to address technological, policy and legal dimensions. The immediate challenge before nation states is to develop a deep understanding of CII interdependencies; to develop policy and legal frameworks; and to bring the private sector on board and to strike the right balance between their offensive and defensive capabilities with respect to cyberspace. The trust deficit arising out of espionage attempts, malware targeted at critical installations and APT campaigns dampens international efforts. The UN GGE also calls out for norms, rules and principles for the responsible behaviour of states with respect to critical infrastructure and CII.

The entire IT infrastructure is owned, managed and operated by no single authority, government or organization. A significant part of critical infrastructure and CII is developed, operated and maintained by the private sector. The protection of critical infrastructure and CII is infeasible without a coordinated effort of all the players and stakeholders. Governments have to move beyond their traditional roles as regulators, and rather forge partnerships. The idea of public–private partnership to bring everyone on a single platform for dialogue, information and expertise exchange can be fruitful if participants trust each other.

India, as a key stakeholder in the future of cyberspace governance and a progressive economy relying upon its CII, has to pitch its voice to preserve its national interests. At multilateral platforms such as UN GGE, India has to start shaping the future discourse which calls for a more proactive diplomacy and representation. On the domestic front,

the legislation governing cyber security and CIIP, IT (Amendment) Act, 2008, needs periodic reviews to keep the penalties and provisions abreast with the global advancements. The institutions built to or tasked with security and protection of CII need to evolve above the traditional hierarchical approach and adopt a networked approach to find/implement the technical/policy measures in shortest time possible. Credible assessment of CII threats and existing vulnerabilities, identification of critical processes and assets, adoption/implementation of best practices, adherence to guidelines and real-time intelligence of/response to cyber-attacks on any of the CII sectors will help India develop safe, secure and resilient information infrastructure for its critical sectors.

Basic services such as electricity, transportation, mobile communication and banking are the core infrastructures on which modern societies and economies rest. The seamless functioning of these critical information infrastructures is essential for the social and economic development and well-being of a nation-state. Recent developments in the cyber domain have unearthed a whole new dimension of security attributing to underlying vulnerabilities and interdependencies. The exploitation of these vulnerabilities in the different layers of cyber architecture, serve different objectives of nation-states, terror outfits and criminal syndicates. Despite the best of technology, management as well as security policies and practices at a nation-state's disposal, it is practically impossible to secure all critical elements of infrastructure against all odds. This monograph delves into the various aspects of definitions and understandings of critical information infrastructure and explores the threat actors, perspectives and trends in the emerging practice of critical information infrastructure protection.

Munish Sharma is an Associate Fellow with the Cybersecurity Project at the Institute for Defence Studies and Analyses, New Delhi. His research interests include cybersecurity, critical information infrastructure protection, space security and defence technologies. He is the co-editor of the book Securing Cyberspace: International and Asian Perspectives (2016).

idsa
INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

Institute for Defence Studies and Analyses
No.1, Development Enclave, Rao Tula Ram Marg,
Delhi Cantt., New Delhi - 110 010
Tel.: (91-11) 2671-7983 Fax: (91-11) 2615 4191
E-mail: contactus@idsa.in Website: http://www.idsa.in