Security Issues for Critical Infrastructure

Workshop on 25th April 2018

ITU – APT Foundation of India

The Kosciuszko Institute - Prediction

- 2017 was a year of “electoral hacking” and an intense information war aimed at shaping the recipients’ viewpoint,

- 2018 – could be year of cyber attacks on critical infrastructure.

National Security

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" .

Critical Infrastructure – NII & GII

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

Critical Infrastructure – NII & GII

The common denominators for both NII and GII are same - primarily they are :

- telecommunications or computer networks,
- computers,
- databases and the resident information,
- software applications,
- encryption process,
- standards and protocols and
- the human resources.

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/ Conspicuous Political Rivalry/ Political Animosity		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

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.	

Critical Infrastructure - India

Transpo- rtation	Power and Energy	Information and Communications Technology	Banking, Financial Services and Insurance	e-Governance and Strategic Public Enterprises
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 3. Payment Gateways	1. NIC 2. e-Governance Infrastructure

Threat Vectors on Critical Infrastructure

Increased cyber attack surfaces

- Digital India initiative
- Thrust towards digital economy
- e-governance

Triggers of global urgency for immediate implementation of cyber security practices

- Increase in ransomware attacks and
- sophistication of weaponized malware
- WannaCry, Petya, NotPetya gained immense notoriety.

Current Security Awareness Scenario

- Growing awareness of cyber hygiene.

- Meridian Annual Conference held in Oslo, Norway on 24-25 October 2017. The Meridian Process aims to exchange ideas and initiate actions for the cooperation of governmental bodies on Critical Information Infrastructure Protection (CIIP) issues globally.
- India also participated (NCIIPC).

Data Protection & Information Privacy

- As India transforming into a digital future, the importance of personal data and citizen's right to privacy is crucial to protect national interests.
- Data protection from the prism of protecting an individual's right to privacy, while ensuring that it is not overpowering to hinder freedom of expression, research, artistic rights, law and order requirements etc.

Supreme Court observation

- *"Informational Privacy is a facet of right to privacy. The dangers to privacy in an age of information can originate not only from the state but non-state actors as well.*
- *The Government needs to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state."*

Challenges

- Private and Public Perspectives
- Multiple Stakeholders
- Scale and Unlimited Boundaries
- An Expanding Network
- Complexity and Interdependencies
- Human Element
- Endless Vulnerabilities and Limited Knowledge
- Information Sharing/Analysis
- Fragmentation
- Asymmetric Angle

Approach for Tackling Security of Critical Infrastructure

- a multi-stakeholder approach transcending organisational, national and international borders.

- regulating cyber space and formulating a Global Treaty.

Thank You

Tulika Pandey
Director
Ministry of Electronics & IT
GoI