Cyber Security Policy

Challenges for Pakistan

Dr. Nadia Khadam

8th December 2021

Cyber security after Covid -19

- "Securing our digital society is now more important than ever. These past months have shown how central the digital space is in our lives, with work, education and connecting with family and friends all happening online. This can also make us vulnerable to cyber threats.

(Mariya Gabriel, European Commissioner for Innovation, Research, Culture, Education and Youth)

- One fine day you got to know that another face book profile exists with your name and photo

- What kind of data breach it is?

- Another day you want to access internet banking and unable to do. And later you find out that bank is having trouble in operation and under attack.

- What kind of issue it is?

- **Hackers tried poisoning town after breaching its water facility**
- A hacker gained access to the water treatment system for the city of Oldsmar, Florida, and attempted to increase the concentration of sodium hydroxide (NaOH), also known as lye and caustic soda, to extremely dangerous levels.
- **Through Team viewer**

Cyber security

- Significance of Information & Communication technologies (ICT)- Global Village
- ICT- redefining socio economic development
- Creating commercial, economic, cultural, and social opportunities for users of Cyberspace.

- Digital Transformation

Cyber security

- Use of more ICTs------cyber security threats
- The concerns over safety and security potentially impede the objective of accelerated development and affect the confidence of people in using applications and services offered to traverse cyberspace

PAKISTAN'S CYBER SECURITY LANDSCAPE

- Electronic Transaction Ordinance, 2002 (covering only electronic financial transactions and records),
- Fair Trial Act – 2013,
- Pakistan Telecommunication (Re-Organization) Act - 1996 and
- Prevention of Electronic Crime Act (PECA) 2016
- State Bank of Pakistan (SBP)

Multi stakeholder concept

Scope of Cyber security Policy

- This policy framework is envisaged to secure the **entire cyberspace** of Pakistan including all digital assets of Pakistan, data processed, managed, stored, transmitted or any other activity carried out in public and private sectors, and the information and communication systems used by the citizens of Pakistan.

Objectives

- to establish a concrete legal and structural framework related to cyber security.

- Earlier lack of commitment by Pakistan to cyber security, it performed poorly in global ICT rankings (ICT Development Index value of 2.42). Hence, one of the core objectives of the policy also happens to be the improvement of Pakistan's ICT ranking. Pakistan also ranks 14 out of a total of 18 states in the Asia-Pacific on the Global Cybersecurity Index (GCI) 2020. The policy would help improve Pakistan's GCI ranking too.

Salient Features

- To establish **governance and institutional framework** for a secure cyber ecosystem.
- To enhance the security of **national information systems and infrastructure.**
- To create a **protection and information sharing mechanism** at all tiers capable to monitor, detect, protect and respond against threats to national ICT/ CII infrastructures.
- To protect National Critical Information Infrastructure by mandating **national security standards and processes** related to the design, acquisition, development, use, and operation of information systems.

Salient Features

- To create an **information assurance framework of audits and compliance** for all entities in both public and private sectors.
- To ensure the **integrity of ICT products**, systems, and services by establishing a mechanism of **testing, screening, forensics, and accreditation**.
- To protect the **online privacy of the citizens** by provisioning the required support and system to all the concerned institutions and organizations National Cyber Security Policy 2021, that are dealing with citizens' data-related matters be more equipped and able to render their services, accordingly.

Salient Features

- To develop **public-private partnerships** and collaborative mechanisms through technical and operational cooperation.
- To create a country-wide culture of **Cyber Security awareness** through mass communication and education programs.
- To train **skilled Cyber Security professionals** through capacity building, skill development, and training programs.
- To encourage and support **indigenization and development** of Cyber Security solutions through **R&D Programs** involving both public and private sectors.

Salient Features

- To provide a framework on **national-global cooperation** and collaborations on Cyber Security.
- To Identify and process **legislative and regulatory actions** under the mandates of relevant stakeholders assigned in the policy.
- Risks related to Cyber Security need to be managed continuously. Encourage adoption of a **risk-based approach** to Cyber Security through frameworks including those for regulation, assurance, threat management, and incident management.[AI, cloud computing, hacker for hire services etc.]

Challenges

- Ownership at the Top
- Weak Laws [struggle in Making laws]
- Enforcement of statutes
- Reliance of external sources[Skilled Human Resource+ Digital Forensics]
- Multi stake holder concept
- Ownership by private sector-Financial resources
- Cyber Governance Policy Committee
- Public- Awareness at large level

Thankyou

nadiakhadam@gmail.com