SESSION 4

# DIGITAL INFRASTRUCTURE FOR ADAPTIVE SOCIAL PROTECTION


## Building Block 3 : Data and Information for Social Protect

Fireside Chat: the **Role of AI and Information Security in Adaptive Social Protection**

**Dr. Haider Abbas,** Director General National CERT

**Moderated by:** Dr. Hashim Chunpir

- How do you see the role of AI in enhancing social protection initiatives in Pakistan?

# Role of AI in Social Protection Systems

## 1 Predictive Analytics

AI can help predict potential crises and allocate resources effectively.

## 2 Automated Decision-Making

AI can automate decisions related to resource allocation, benefit eligibility, and program design.

## 3 Chatbots

AI-powered chatbots can provide beneficiary support and resolve queries efficiently.

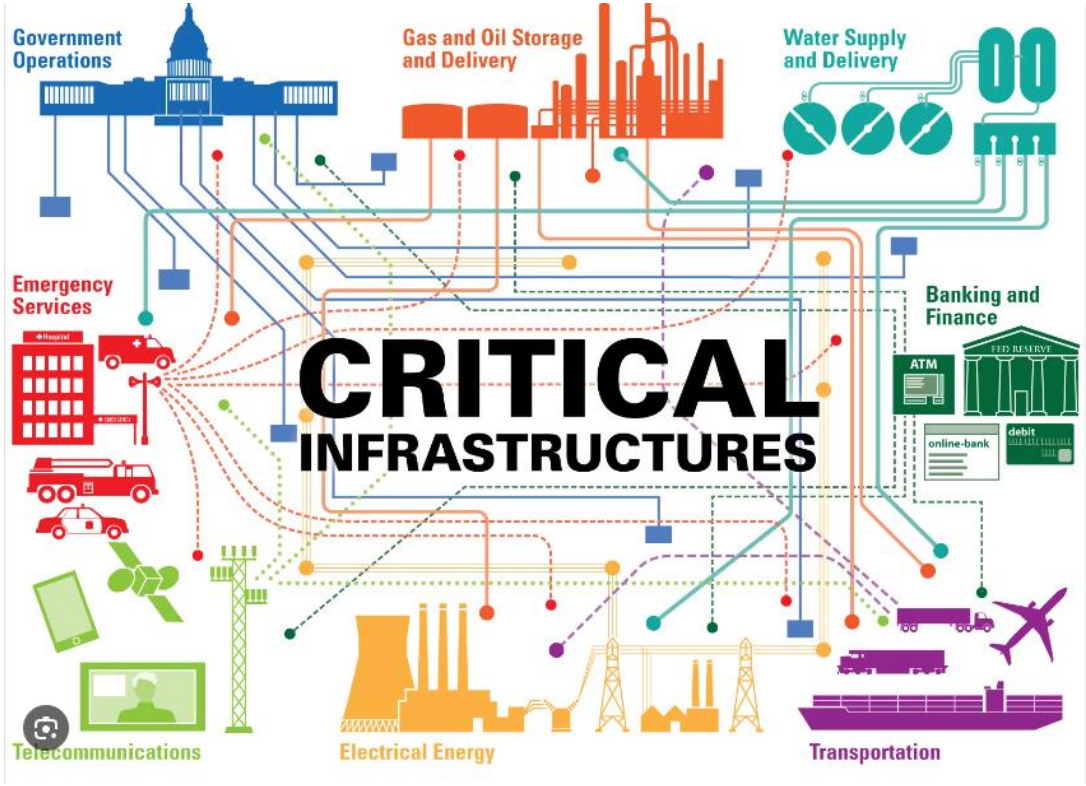
## 4 Fraud Detection

AI can identify fraudulent activities and anomalies in data, ensuring the integrity of social protection programs.

- What potential challenges / technical or institutional barriers do you foresee in integrating AI into adaptive social protection systems in Pakistan, particularly in low-resource and non-sustainable settings?

# Cyber Crisis in Adaptive Social Protection

A cyber crisis in adaptive social protection refers to a significant cyber-related disruption that compromises the resilience, responsiveness, and effectiveness of digital systems supporting adaptive social protection programs.




- What are the biggest risks to information security as adaptive social protection systems become more digitized and interconnected?

# Risks & Threats to Adaptive Social Protection System

**Service Disruption:** Cyber incidents can halt the distribution of benefits such as pensions, unemployment aid, or healthcare subsidies, affecting vulnerable populations

**Data Breaches:** Leakage of sensitive personal information (e.g., identity records, financial details) can lead to fraud, identity theft, and loss of public trust

**Misinformation & Manipulation:** Cyberattacks may spread false information about social benefits, causing confusion, panic, or even social unrest

**Targeted Cybercrime:** Hackers may exploit weaknesses in digital social protection systems for financial gain, disrupting the fair allocation of aid

**Manipulation of Social Protection Algorithms:** Cybercriminals or adversaries could exploit AI-driven decision-making tools, leading to the misallocation of aid or systematic exclusion of deserving populations.

**National Security Risks:** A cyber crisis in social protection can escalate into a broader national security concern, particularly if foreign adversaries or cybercriminals target government welfare infrastructure.

- What is the significance of data protection and information security in the context of social protection?

# Importance of Information Security

**Data Protection**

Sensitive beneficiary data, such as personal information and financial records, needs robust protection.

**Cyberattack Prevention**

Social protection systems are vulnerable to cyberattacks, which can disrupt operations and compromise sensitive information.

**Data Integrity and Confidentiality**

Ensuring data integrity and confidentiality is crucial for maintaining the trust and legitimacy of social protection programs.

**Compliance**

Social protection systems must comply with national and international regulations related to data privacy and security.

- What are the challenges and future prospects in our adaptive social protection (ASP) context?

also

- What advice would you give to policymakers aiming to adopt AI and data/systems interoperability in a secure and ethical way?

# Challenges and Future Prospects in This Project's Context

### AI Ethics

Balancing the benefits of AI automation with ethical concerns related to bias, transparency, and accountability is crucial.

### Cybersecurity Threats

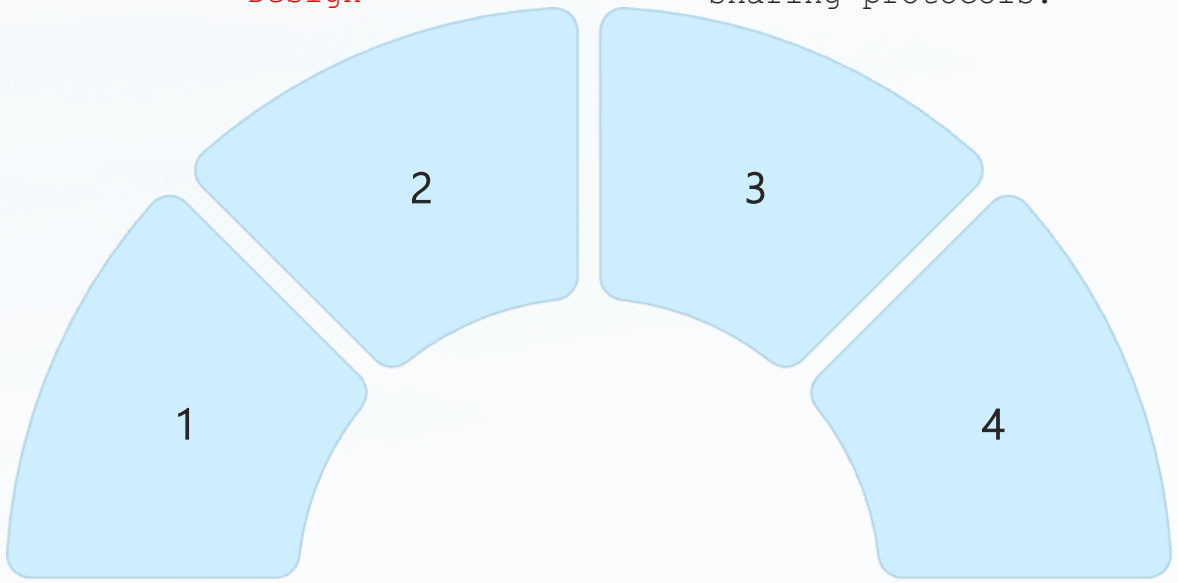
Addressing evolving cybersecurity threats in digital social protection systems requires proactive measures and continuous adaptation. Security By Design

### Interoperability and Security

Achieving interoperability without compromising security requires careful planning, robust security measures, and secure data sharing protocols.

### Governance and Transparency

Effective governance mechanisms are needed to ensure fairness, transparency, and accountability in digital social protection systems.



- How do you envision the future of AI, information security, and interoperability transforming social protection in the next 5–10 years?

# Role of National CERT in Securing Social Protection Systems


One important role of National CERT is to ensure security of the social protection systems by continuously monitoring and responding to cyber threats, issuing security advisories for relevant platforms, and conducting audits and risk assessments to identify vulnerabilities. It collaborates with international security organizations to enhance threat intelligence and resilience. Additionally, National CERT provides cybersecurity training for stakeholders, ensuring best practices are implemented to safeguard sensitive data and maintain the integrity of social protection services.

1

**Threat Monitoring**

National CERT constantly monitors and responds to cyber threats targeting social protection systems.

2

**Security Advisories**

National CERT provides security advisories and guidance to stakeholders for securing social protection platforms.

3

**Audits and Assessments**

National CERT conducts audits and risk assessments of social protection systems to identify vulnerabilities and weaknesses.

4

**International Collaboration**

National CERT collaborates with international security organizations to share best practices and strengthen national cybersecurity posture.

5

**Capacity Building**

National CERT trains stakeholders on cybersecurity best practices to build a resilient and well-informed cybersecurity workforce.

# Audience: Do you have questions?