PLUTUS IAS
CURRENT AFFAIRS
CURRENT AFFAIRS
Argasia Education PVT. Ltd. (GST NO.-09AAPCAI478E1ZH)
Address: Basement C59 Noida, opposite to Priyagold Building gate, Sector 02,
Pocket I, Noida, Uttar Pradesh, 201301, CONTACT NO:-8448440231

**Date –24- October 2024**

# EMPOWERING CYBERSECURITY: A COLLECTIVE INITIATIVE AMONG KEY NATIONS

## WHY IN THE NEWS?

Recent collaborations among key nations, such as the U.S., India, Australia, and Japan, are being highlighted as they announce new agreements focused on enhancing cybersecurity measures. Additionally, ongoing geopolitical tensions are driving countries to unite in their efforts to bolster cyber defences and mitigate vulnerabilities. The rapid advancement of technology further complicates the cybersecurity landscape, necessitating coordinated strategies to address emerging threats.

## WHAT IS CYBER SECURITY?

Cybersecurity refers to the practices, technologies, and processes designed to protect computer systems, networks, and data from theft, damage, or unauthorized access. It encompasses a wide range of measures aimed at safeguarding sensitive information and ensuring the integrity, confidentiality, and availability of digital assets.

### Various Types of Cybersecurity

**1. Network Security:** Focuses on protecting networks from intrusions, attacks, and misuse.This includes firewalls, intrusion detection systems, and secure network architecture.

**2. Application Security:** Involves measures taken to improve the security of applications throughout their lifecycle. This includes secure coding practices, testing for vulnerabilities, and implementing security updates.

**3. Information Security:** Aims to protect data, both in transit and at rest, from unauthorized access and corruption. This includes encryption, access controls, and data masking.

**4. Cloud Security:** Focuses on protecting data and applications hosted in the cloud. This involves security measures specific to cloud computing environments, including identity management and secure configurations.

## WHAT IS CYBER CRIME?

Cybercrime refers to illegal activities conducted through the internet or involving computer systems. It encompasses a wide range of offences, from individual attacks to large-scale operations targeting organizations or governments. Cybercriminals exploit vulnerabilities in technology to steal information, disrupt services, or cause harm.

### Various Types of Cyber Crime

**1. Hacking:** Unauthorized access to computer systems or networks to steal data or disrupt operations. This includes activities like data breaches and system intrusions.

**2. Phishing:** Fraudulent attempts to obtain sensitive information (like passwords or credit card numbers) by disguising it as a trustworthy entity in electronic communications, typically via email.

**3. Malware:** Malicious software designed to harm or exploit any programmable device, service, or network. This includes viruses, worms, ransomware, and spyware.

**4. Ransomware:** A type of malware that encrypts a victim's files, demanding payment (ransom) for the decryption key. This can severely disrupt individuals and organizations.

**5. Identity Theft:** Stealing personal information to impersonate someone else, often for financial gain. This can involve obtaining social security numbers, bank account information, or credit card details.

## CYBERSECURITY SCENARIO IN INDIA:

**1. Increase in Cyber Crimes:** Reported cyber crimes in India surged by 300% in 2020, reflecting a significant rise in threats.
**2. CERT-In Incident Handling:** The Indian Computer Emergency Response Team (CERT-In) reported over 53,000 cyber incidents in 2021, with a notable increase in ransomware and phishing attacks.

**3. Government Budget Allocation:** The Indian government allocated ₹1,500 crore (approximately $200 million) for cybersecurity in the 2022-23 budget to enhance national cyber defences.

**4. Cybersecurity Workforce Gap**: India faces a shortage of approximately 1 million cybersecurity professionals, highlighting the skills gap in the sector.

**5. Public Awareness:** Surveys indicate that only 30% of Indian internet users are aware of basic cybersecurity practices, indicating a critical need for public education.

**6. Cyber Crime Reporting Portal:** The National Cyber Crime Reporting Portal was launched to facilitate citizen reporting of cyber crimes, making it easier to address issues.

**7. Cybersecurity Policies:** The National Cyber Security Policy (2020) aims to create a secure cyberspace by promoting innovation and enhancing infrastructure.

**8. Impact on Critical Sectors:** Cyber threats pose risks to critical infrastructure sectors, including finance, energy, and transportation, necessitating targeted protective measures.

## GOVERNMENT INITIATIVES FOR CYBERSECURITY IN INDIA:

**1. National Cyber Security Policy (2020):** This comprehensive policy aims to create a secure cyberspace by promoting cybersecurity awareness, research, and innovation while also protecting critical information infrastructure.

**2. Cyber Surakshit Bharat Initiative:** Launched by the Ministry of Electronics and Information Technology (MeitY), this initiative focuses on enhancing the cybersecurity ecosystem through training and awareness programs for government officials and stakeholders.

**3. Indian Computer Emergency Response Team (CERT-In):** Established to respond to cyber incidents, CERT-In provides guidelines, training, and incident management support to enhance national cybersecurity preparedness.

**4. National Cyber Crime Reporting Portal:** This platform allows citizens to report cyber crimes easily, helping authorities address incidents more effectively and promoting public participation in cybersecurity efforts.

**5. Cybersecurity Education and Training:** The government supports various educational programs and partnerships with institutions to train cybersecurity professionals, aiming to bridge the skills gap in the sector.

**6. Digital India Initiative:** Part of a larger vision to transform India into a digitally empowered society, this initiative includes cybersecurity as a critical component to ensure safe digital transactions and infrastructure.

**7. Public Awareness Campaigns:** The government conducts various campaigns to educate the public about safe online practices, phishing threats, and the importance of cybersecurity hygiene.

**8. Collaboration with International Agencies:** India collaborates with organizations like INTERPOL and the United Nations to share knowledge and best practices in combating cyber threats.

## CHALLENGES TO TACKLING CYBERSECURITY IN INDIA:

**1. Transborder Cyber Threats:** Cybercriminals operate across borders, making it difficult for national law enforcement to address cyber crimes effectively. The lack of international cooperation can hinder timely responses and investigations.

**2. Absence of Proper Legislation:** While India has the Information Technology Act, it lacks comprehensive laws specifically addressing emerging cyber threats, such as data breaches and cyberbullying. This legislative gap can impede effective enforcement.

**3. Skill Shortage:** There is a significant shortage of skilled cybersecurity professionals in India. The gap between the demand for expertise and the availability of trained personnel poses challenges in effectively mitigating cyber risks.

**4. Rapid Technological Advancements:** The fast pace of technological change creates new vulnerabilities. Organizations may struggle to keep up with the latest cybersecurity measures and best practices.

**5. Public Awareness:** Many individuals and small businesses lack awareness of cybersecurity risks and best practices. This knowledge gap can lead to increased susceptibility to cyber-attacks.

**6. Infrastructure Vulnerabilities:** Critical infrastructure sectors, such as energy and finance, often have outdated systems that are more vulnerable to attacks. Strengthening these infrastructures requires significant investment.

**7. Compliance and Regulatory Issues:** Organizations often face difficulties in complying with existing regulations due to their complexity and the lack of clear guidelines, leading to potential legal vulnerabilities.

## WAY FORWARD:

**1. Strengthen International Cooperation:** Foster collaboration with global law enforcement and cybersecurity agencies to enhance information sharing and joint efforts in tackling transborder cyber threats.

**2. Enhance Legislative Framework:** Develop comprehensive and updated legislation that addresses emerging cyber threats, ensuring that laws are in place to protect data privacy and combat cybercrime effectively.

**3. Invest in Skill Development:** Launch targeted training programs and partnerships with educational institutions to cultivate a skilled workforce in cybersecurity, addressing the existing skills gap.

**4. Promote Public Awareness Campaigns**: Increase efforts to educate the public and businesses about cybersecurity risks and best practices through awareness campaigns and workshops.

**5. Upgrade Critical Infrastructure:** Invest in modernizing the cybersecurity measures of critical infrastructure sectors to protect against vulnerabilities and potential attacks.

**6. Adopt Advanced Technologies:** Encourage the use of AI, machine learning, and other advanced technologies to enhance threat detection and response capabilities in cybersecurity.

**7. Establish Clear Compliance Guidelines:** Develop straightforward compliance guidelines for organizations to help them adhere to cybersecurity regulations and standards more effectively.

**8. Implement Incident Response Plans:** Encourage organizations to create and regularly update incident response plans, ensuring they are prepared to handle cyber incidents swiftly and effectively.

## CONCLUSION:

India needs everyone to work together—government, businesses, and the public. Key steps include boosting international cooperation, creating strong laws to handle new threats, and training more skilled professionals. It's also important to raise awareness about online safety and update critical infrastructure to protect against attacks. Using advanced technology for better detection and encouraging partnerships between different sectors will strengthen defences. By taking these actions, India can build a strong cybersecurity system that protects digital assets and builds trust in our connected world.

## PRELIMS QUESTION:

**Q. With reference to the global initiatives in cybersecurity, consider the following statements:**

1. The initiative aims to enhance cooperation among nations to combat cyber threats.

2. It focuses exclusively on the technical aspects of cybersecurity, ignoring policy frameworks.

**Which of the above statements is/are correct?**

A. 1 only

B. 2 only

C. Both 1 and 2

D. Neither 1 nor 2

**Answer: A**

**MAINS QUESTION:**

**Q. Critically assess the role of technology transfer and capacity building in enhancing cyber security capabilities in developing nations. What are the potential benefits and drawbacks of such initiatives?**

**(250 words, 15 marks)**

Ritik singh

# “MODERNIZING LAND RECORDS FOR A NEW INDIA: THE DILRMP INITIATIVE”

## WHY IN THE NEWS?

**Union Minister of Rural Development Shri Shivraj Singh Chouhan inaugurated an International Workshop on Modern Technologies in Survey-Resurvey for Urban Land Records, recently organized by the Department of Land Resources.**

## THE DIGITAL INDIA LAND RECORDS MODERNIZATION PROGRAMME (DILRMP)

### DILRMP:

The Digital India Land Records Modernization Programme (DILRMP), formerly known as the National Land Record Modernization Programme, was revamped into a Central Sector Scheme effective April 1, 2016, with 100% funding from the Centre. Its objective is to create a modern, comprehensive, and transparent land record management system. The DILRMP is implemented by the Ministry of Rural Development, Government of India.

### KEY OBJECTIVES:

**Real-time Land Information:** Improve access to accurate and timely data.
**Resource Optimization:** Enhance the utilization of land resources.
**Support for Stakeholders:** Benefit landowners and prospective buyers.
**Policy Assistance:** Aid in effective planning and policy-making.
**Dispute Reduction:** Minimize land-related conflicts.
**Fraud Prevention:** Curb fraudulent and benami transactions.
**Digital Access:** Reduce the necessity for physical visits to Revenue and Registration offices.
**Information Sharing:** Facilitate collaboration with various organizations and agencies.

### KEY ACHIEVEMENTS

**Computerization of Land Records:** 95.08% of Record of Rights (RoR) completed across 625,062 villages out of 657,396.
**Digitization of Cadastral Maps:** 68.02% completed, with 24,957,221 maps digitized out of 36,692,728.
**Computerization of Registration:** 94.95% completed in 5,060 out of 5,329 Sub-Registrar Offices (SROs).

**Integration of SROs with Land Records:** 87.48% integration completed (4,662 out of 5,329 SROs).
**Five-year extension for the DILRMP (2021-22 to 2025-26):** Consent-based integration of Aadhaar with land records. Computerization of Revenue Courts and their integration with land records.

## INNOVATIVE INITIATIVES

### Unique Land Parcel Identification Number (ULPIN) or Bhu-Aadhar

A 14-digit unique ID based on geo-coordinates for each land parcel.
Facilitates real estate transactions and helps resolve boundary issues.
Implemented in 29 States/UTs, with pilot testing ongoing in additional regions.

### National Generic Document Registration System (NGDRS) or E-Registration

A uniform registration process for deeds and documents, streamlining registration through online services.
Adopted in 18 States/UTs, with data sharing implemented in 12 states.

### Linkage of e-Court with Land Records/Registration Database

Provides authentic information to courts for speedy case disposal.
Integration approved in 26 States/UTs to enhance legal processes.

### Transliteration of Land Records

Converts local language records into any of the 22 languages in Schedule VIII.
Pilot tests are underway in 8 States, with 17 States/UTs already using the tool.

### Bhoomi Samman (Platinum Grading Certificate Scheme)

Targets saturation in basic components like record computerization and cadastral map digitization.
As of December 20, 2023, 168 districts in 16 States achieved Platinum Grading for completing over 99% of essential tasks.

## SIGNIFICANCE OF LAND RECORDS

**High Litigation:** Accurate land records reduce disputes and litigations over land ownership, ensuring smoother legal processes.

**Agricultural Credit:** Land serves as collateral for farmers to obtain loans. Reliable land records are essential for securing agricultural credit and improving farmers' access to financial resources.

**Development of New Infrastructure:** As India's economy transitions from agrarian to manufacturing and services, comprehensive land records facilitate the development of infrastructure projects, ensuring efficient land utilization and planning.

**Urbanization and Housing Shortage:** Rapid urbanization has altered land use patterns, increasing the demand for accurate land records to address housing shortages and manage urban expansion effectively.

**Benami Transactions:** Reliable land records help curb Benami transactions, where properties are held under fictitious names. This transparency is vital in combating black money, as highlighted in the White Paper on Black Money (2012).

**Women's Land Titles:** Proper land records are essential for ensuring women can secure land titles, promoting gender equality, and empowering women economically by providing them with ownership rights.

**Proper Government Support:** Accurate and updated land records enable the government to implement policies effectively, ensuring proper support for land reform initiatives, social justice, and sustainable development.

## CHALLENGES OF THE DIGITAL INDIA LAND RECORDS MODERNIZATION PROGRAMME (DILRMP)

**Local Administration Issues:** Local administrations struggle to maintain accurate land records and effectively implement DILRMP initiatives.

**Fraud and Malpractices:** The land registration and administration system is vulnerable to fraudulent activities and malpractices, undermining public trust.

**Time Delays:** The processing of land records and registration often experiences significant time delays, affecting efficiency and accessibility.

**Human Error:** Manual data entry and management increase the likelihood of human errors, leading to incorrect land records.

**Inaccurate Land Records:** Many land litigations arise from inaccuracies in land records, causing disputes and legal complications.

**Lack of Awareness:** There is a general lack of awareness among landowners and stakeholders about the DILRMP and its benefits, limiting public engagement and utilization.

**Corruption During Record Entry:** Corruption in the recording process leads to manipulated data entries, affecting the integrity of land records.

**Lack of Data from Remote Areas:** Remote regions often lack comprehensive data, making it difficult to implement uniform land record systems across the country.

## WAY FORWARD

**Effective Implementation:** Ensure rigorous adherence to proper recording practices for land ownership and transactions to maintain accuracy and reliability.

**Faster Use of Digitalization:** The Parliamentary Standing Committee suggests leveraging innovative technologies for rapid digitalization of land records, making the process more efficient and accessible.

**Accurate Recording in Remote and Border Areas:** Focus on improving land record accuracy in remote and border regions, where challenges in data collection and management persist.

**Cooperation Among States**: Foster collaboration between states and central agencies to facilitate comprehensive land record management and address discrepancies.

**Adoption of the Torrens System:** Implement the Torrens system for recording and registering land ownership, which offers guaranteed titles to property owners, thereby enhancing legal clarity and reducing disputes.

**Reducing Registration Costs:** Work on minimizing the costs associated with land property registration, making the process more accessible for landowners.

**Proper Maintenance of Land Records and Spatial Data:** Establish robust systems for the ongoing maintenance of land records and associated spatial data to ensure their accuracy and relevance over time.

**Capacity Building:** Invest in capacity-building initiatives to enhance the skills of personnel involved in data collection and storage at village, city, and block levels. This will strengthen land management practices and facilitate effective updating of records.

## CONCLUSION

The digitization of land records is an urgent necessity, as land is integral to our culture and tradition. The Digital India Land Records Modernization Programme (DILRMP) serves as a significant step in this regard, but it is essential to implement it effectively. Recent experiences over the last few years indicate that the scheme is working in the right direction, yet it is crucial to address and remove existing glitches.

## PRELIMS QUESTION:

**Q. With reference to the Consider the following statement:**

1. The Digital India Land Records Modernization Programme (DILRMP) is launched during the eleventh Five year plan.
2. The one of the objectives of DILRMP is to provide the Bhu-Aadhar to farmers
3. The Scheme is implemented by the state agriculture departments.

How many of the above-given statements are correct?

A. Only one<br>
B. Only two<br>
C. All three<br>
D. None

## ANSWER: A

## MAINS QUESTION:

**Evaluate the objectives of the Digital India Land Records Modernization Programme (DILRMP) in achieving land rights for women, reducing land-related disputes, and easy traceability of formal credits. ( Answer in 250 words)**

**Munde Dhananjay Navnath**