Sansad TV Vishesh: Safe Cyber Space

For Prelims: Indian Cyber Crime Coordination Centre (I4C), Cyber Crime, Software, Internet, Telecommunications Networks, Viruses, Ransomware, Spyware, Trojans, National Crime Records Bureau (NCRB) Report, Phishing, IP Addresses, Terrorist Organizations, Critical Infrastructure, Financial Crimes, Cooperative Federalism, Cert-In, Cyber Surakshit Bharat, Digital India, Malware.

For Mains: Cyber Crime Implications and Significance of Safe Cyberspace in India.

Why in News?

Recently, the first foundation day of the Indian Cyber Crime Coordination Centre (I4C) was marked by an event held in **New Delhi,** which showcased significant advances in cyber crime prevention with the launch of several key initiatives.

What is Cyber Security?

- **Cyber security:** It is the **protection of information systems,** including hardware, software, and data, from cyber threats. It aims to defend against unauthorized access, theft, damage, and other malicious activities that could compromise the integrity, confidentiality, and availability of digital information.
- **Cyber Space:** The global network of **interconnected information technology infrastructures,** including the Internet, telecommunications networks, and computer systems, where data and communications occur.
- **Critical Information Infrastructure (CII)**: Defined by **Section 70(1) of the** Information Technology Act, CII includes computer resources whose incapacitation or destruction could severely impact national security, **economic stability, public health, or safety.**
- **Cyber Attack:** A **deliberate and malicious attempt** by individuals or organizations to breach information systems, driven by motives ranging from financial gain to political activism or espionage.
- **Types of Cyber Attacks:**
    - **Malware:** Malicious software, including viruses, worms, ransomware, spyware, and trojans, designed to damage or disrupt systems, steal information, or gain unauthorized access.
    - **Phishing: Deceptive emails or websites** that trick individuals into revealing personal information, such as login credentials or financial details.
    - **Denial of Service (DoS) Attacks**: Attacks aimed at shutting down a machine or network by overwhelming it with **excessive traffic**, making it inaccessible to legitimate users.
    - **Man-in-the-Middle (MitM) Attacks:** Intercepting and altering communications between two parties without their knowledge, enabling data theft or manipulation.
    - **SQL Injection**: Exploiting vulnerabilities in databases by inserting malicious code into queries to access or manipulate data.
    - **Cross-Site Scripting (XSS)**: Injecting **malicious script**s into websites to run in users' browsers, potentially stealing personal information or performing unauthorized actions.
    - **Social Engineering**: Manipulating individuals into breaching security protocols or

disclosing confidential information through psychological tricks.

What are Government Initiatives to Counter Cyber Crime?

- **Recent Initiatives:**
  - **Cyber Fraud Mitigation Centre (CFMC):** This centre brings together representatives from **major banks, financial intermediaries, telecom service providers, IT intermediaries, and law enforcement agencies.**
    - It serves as a cooperative platform for addressing online financial crimes and exemplifies cooperative federalism in law enforcement.
  - **Samanvay Platform**: A **web-based module** designed as a central repository for cybercrime data, facilitating data sharing, crime mapping, and coordination among law enforcement agencies across India.
  - **Cyber Commandos Program**: Aiming to train around **5,000 cyber commandos** over the next five years, this program focuses on developing a specialized cadre of cyber security professionals to assist state and central agencies in securing the digital space.
  - **Suspect Registry:** This national-level registry consolidates information on cyber crime suspects, enhancing fraud risk management within the **financial ecosystem**.
- **Previous Initiatives:**
  - **Information Technology Act, 2000:** Regulates the use of computers, networks, and data in electronic formats, including provisions for offenses like **hacking, cyber terrorism, and data theft.**
  - **Indian Cybercrime Coordination Centre (I4C):** Established by the **Ministry of Home Affairs, I4C** aims to address cybercrime in India through coordinated efforts.
    - Approved on October 5, 2018, I4C **enhances coordinatio**n among law enforcement and stakeholders, boosts national capabilities, and improves citizen satisfaction in handling cybercrime.
  - **Indian Computer Emergency Response Team (CERT-In)**: CERT-In plays a critical role in managing cybersecurity incidents and coordinating response efforts. It serves as the central authority for incident management, vulnerability assessment, and security oversight in India's digital landscape.
  - **Cyber Surakshit Bharat**: Launched by the **Ministry of Electronics and Information Technology (MeitY) i**n collaboration with the **National Electronic Governance Division (NeGD),** Cyber Surakshit Bharat aims to support the **"Digital India"** vision by increasing awareness of current cyber threats and challenges.
  - **Cyber Swachhta Kendra:** This initiative focuses on identifying and eliminating malicious botnet programs from computers and devices. It offers free tools for malware analysis and enhances system and device security.
  - **National Cyber Security Strategy, 2020**: It aims to enhance **cyber awareness and strengthen cybersecurity** by implementing more rigorous audits.
    - **Cyber auditors** will conduct more thorough assessments of organizational security measures beyond the current legal requirements.
- **International Initiatives:**
  - **Budapest Convention on Cybercrime:** An international treaty for harmonizing laws and enhancing cooperation on cybercrime. Effective since July 1, 2004. India is not a signatory.
  - **Internet Governance Forum (IGF):** A platform for dialogue among governments, private sector, and civil society on internet governance.
  - **UNGA Resolutions**: Established two processes for ICT security namely **Open-ended Working Group (OEWG) and Group of Governmental Experts (GGE).**

What are the Challenges Associated with Cyber Security in India?

- **Increased Cyber Crime Rate:** The National Crime Records Bureau (NCRB) report reveals a **24.4% rise in cybercrime case**s in 2022. In 2022 crime rate (per lakh population) under cybercrime category has increased from 3.9 in 2021 to 4.8.
  - In 2022, 64.8% of cybercrime cases were fraud-related, 5.5% involved extortion, and 5.2% were for sexual exploitation.
  - As per the **Indian Cyber Crime Coordination Centre (I4C),** in May 2024, an average of **7,000 cybercrime complaints** were recorded daily.

- **Increased Use of Mobile Technology and the Internet:** India has **more than 1 billion** smartphone users, and many mobile apps lack robust security features, increasing the risk of data breaches.
- **Proliferation of Internet of Things (IoT)**:The widespread use of IoT devices like smart home gadgets and wearables often exposes them to attacks due to weak security features, making them easy targets for cyber intrusions.
- **Complex Software Systems**: The increasing complexity of **modern software systems,** including their numerous components and interactions, can create vulnerabilities that attackers might exploit.
    - This complexity often leads to security gaps that are difficult to identify and address, making these systems more susceptible to cyber attacks.
- **Human Error:** Mistakes in security practices, such as **misconfiguring settings** or falling for phishing schemes, create potential entry points for attackers.
    - For instance, an employee might accidentally expose sensitive data by misconfiguring access controls or clicking on a **malicious link** that leads to a data breach.
    - These errors often stem from a lack of awareness or training, underscoring the need for ongoing education and stringent protocols to mitigate risks and strengthen overall security.
- **Use of Proxy Servers and VPNs:** Attackers often mask their IP addresses, complicating efforts to trace their origin.
- **Technological Lag**: Attack techniques evolve rapidly, often outpacing the development of countermeasures.
    - For example, while new types of **ransomware** might emerge with enhanced encryption methods, existing antivirus software may not yet be equipped to detect or neutralize these threats.
- **Insufficient Training:** Many individuals and employees **lack adequate training** in cyber security practices.
    - A recent **Nasscom** study predicts that **1 million** new **cybersecurity jobs** will be created by 2027, with **30%** of current positions remaining unfilled due to a **shortage of skilled talent.**
- **Underestimating Threats:** Some organizations and individuals may not fully appreciate the severity of cyber threats, resulting in inadequate protection.
    - This lack of awareness can result in **inadequate defenses and preparedness**, leaving systems vulnerable to attacks that could have been mitigated with a more comprehensive approach to cybersecurity.
- **Shortage of Cyber Security Specialists:** The demand for **skilled cyber security professionals** exceeds supply, leading to competitive hiring and high turnover.
    - Insufficient training programs contribute to the shortage of qualified experts.
- **Increased Use of Cyberspace by Terrorists**:Terrorist organizations exploit the internet for **recruitment and propaganda.** Also there is a risk of terrorists targeting critical infrastructure using cyber attacks.
    - For instance, the **Islamic State (ISIS)** has famously utilized social media to recruit fighters and disseminate extremist content globally. Additionally, there is a growing risk of terrorists **targeting critical infrastructure** through cyberattacks.

Way Forward

- **Public Awareness Campaign:** Increase outreach through diverse media and integrate cyber security education into school curricula. Recently announced **new initiatives at the foundation day event of the I4C** will use TV, radio, and other media to educate the public about cyber crime and the cyber crime helpline 1930. State governments are urged to participate in spreading awareness.
- **Strengthen Technological Measures:** Invest in advanced technologies and enhance collaboration among government, private sector, and international partners.
- **Develop Cyber Security Talent:** Expand training programs and create career development opportunities in cyber security. It is estimated that the global cybersecurity market's growth to **USD 352.25 billion by 2026** presents significant opportunities for India, including the expansion of its **cybersecurity industry and increased job creation.**
- **Monitor and Evaluate:** Conduct regular assessments of cyber security initiatives and establish feedback mechanisms for continuous improvement.

- **Comprehensive Training Programs**: Expanding training initiatives for individuals and organizations to **enhance awareness about cyber threats** and best practices for prevention.
- **Investment in Advanced Security Technologies:** Prioritizing the development and deployment of cutting-edge security solutions to counter emerging threats. Ensuring that software and systems are **regularly updated** to address known vulnerabilities and improve overall security.
- **Inter-Agency Coordination:** Fostering **collaboration between government agencies, private sector entities,** and international partners to share information and strategies for combating cyber crime.

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims:

Q. The terms 'WannaCry, Petya and EternalBlue' sometimes mentioned in the news recently are related to: (2018)

(a) Exoplanets

(b) Cryptocurrency

(c) Cyber attacks

(d) Mini satellites

Ans: (c)

Q. In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one's computer

2. Cost of a new computer if some miscreant wilfully damages it, if proved so

3. Cost of hiring a specialized consultant to minimize the loss in case of cyber extortion

4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only

(b) 1, 3 and 4 only

(c) 2 and 3 only

(d) 1, 2, 3 and 4

Ans: (b)

Mains:

Q. Keeping in view of India's internal security, analyse the impact of cross-border cyber-attacks. Also, discuss defensive measures against these sophisticated attacks. **(2021)**