Public-Private Synergy in Cybersecurity

This editorial is based on "Handling cybercrimes through public-private partnership model" which was published in The Hindu on 29/01/2025. The article brings into picture the rising threat of cybercrime in India and the challenges faced by law enforcement. While initiatives like CCITR are commendable, India must focus on stronger policies, capacity building, and collaboration to enhance cyber resilience.

For Prelims: Cybercrime, Key Cyber Threats India is Facing, Advanced Persistent Threats, Ransomware attack, Cryptocurrency, AI-driven misinformation, Deepfakes, National Cyber Security Strategy, Cloud platforms, CERT-In mandated 6-hour breach reporting.

For Mains: Role of Private Sector in Enhancing India's Cybersecurity Infrastructure, Major Challenges in Onboarding Private Sector in Cybersecurity Landscape

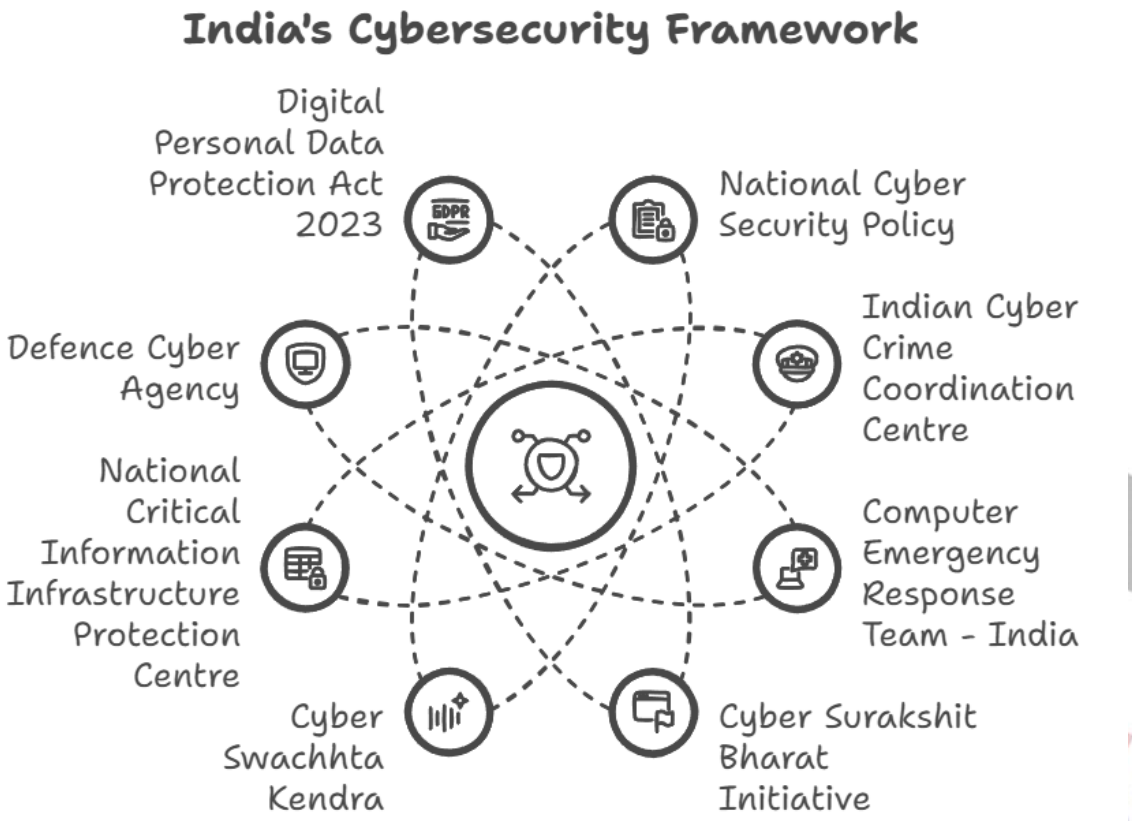
Cybercrime is a growing global threat, with **costs projected to hit $10.5 trillion annually by 2025.** In India, law enforcement faces a surge in cyber threats, **including fraud, hacking, online harassment, and investment scams.** Recognizing the need for a collective effort, **Karnataka's CID launched the Centre for Cybercrime Investigation Training & Research (CCITR) in 2019** through a public-private partnership with **Infosys Foundation and DSCI.** While initiatives like CCITR are promising, India must focus on strengthening cyber resilience through enhanced **policies, capacity building, and collaboration between government, industry, and academia.**

What are the Key Cyber Threats India is Facing?

- **Rising Cyber Espionage from State Actors:** India faces growing threats from foreign state-sponsored groups targeting critical sectors like defense, energy, and government institutions.
    - **Advanced Persistent Threats (APTs) from China and Pakistan** conduct surveillance, steal sensitive data, and disrupt strategic projects.
    - The lack of robust indigenous cybersecurity infrastructure makes India vulnerable to such attacks.
        - A **2021 report** suggested that **Chinese state-sponsored actors may have targeted Indian power grids** and seaports with malware amid rising tensions along the LAC.
- **Growing Ransomware Attacks on Critical Infrastructure: Ransomware groups** are increasingly targeting India's financial, healthcare, and IT sectors, crippling essential services.
    - Hackers use sophisticated malware to lock systems and demand **ransom payments, often in cryptocurrency, making tracking difficult.**
    - Indian enterprises often lack the **necessary cyber hygiene**, making them easy prey for these attacks.
        - AIIMS Delhi servers were compromised in November 2022, with reports suggesting a **possible cyberattack linked to foreign actors**.

        - According to a recent report, India has emerged as a major target for ransomware attacks, **ranking second in the Asia Pacific and Japan (APJ) region.**
- **Increasing Cybercrime Targeting Financial Sector:** India's rapid digital banking expansion has led to a **surge in phishing, UPI frauds, and digital payment scams.**
    - Fraudsters **take advantage of loopholes in digital payment gateways** and exploit unsuspecting users through social engineering tactics.
    - Weak cybersecurity awareness and the use of outdated software in banking networks make financial institutions vulnerable.
    - **UPI, with over 400 million unique users,** has seen a surge in financial frauds, rising by **166% in 2023-24** compared to the 2022-23, as per the RBI annual report.
- **Deepfake and AI-Driven Misinformation:** The rise of **AI-driven misinformation** and **deepfake videos** threatens India's **electoral process, social harmony, and public perception.**
    - **Political parties, foreign actors, and malicious groups** are weaponizing AI to spread propaganda, manipulate public sentiment, and defame opponents.
    - For instance, a **deepfake of actress Rashmika Mandanna** went viral in 2023, highlighting the tech's dangers.
    - According to experts surveyed for the **World Economic Forum's 2024 Global Risk Report,** India was ranked **highest for the risk of misinformation and disinformation.**
- **Supply Chain Cyber Attacks on Indian Enterprises:** Hackers increasingly target **third-party vendors and software supply chains** to gain entry into larger Indian corporations.
    - The interconnected nature of digital ecosystems means one weak link can compromise multiple firms.
        - **Lack of stringent cybersecurity policies among MSMEs**, who serve as vendors to big firms, further exacerbates risks.
    - India's growing reliance on foreign software and cloud solutions also makes it vulnerable to backdoor exploits.
    - An example of this is **SolarWinds Supply Chain Attack** discovered in December 2020, where hackers compromised **SolarWinds' Orion software—**a widely used IT management tool.
- **Cyberterrorism and Dark Web Activities:** Terror groups are leveraging the dark web, **encrypted messaging platforms**, and cryptocurrency transactions to fund operations and coordinate attacks.
    - Radicalization through **social media and online hate groups** is a growing national security threat.
    - **Cyberterrorists exploit India's weak surveillance mechanisms** and VPN networks to remain anonymous. Many sleeper cells are using these platforms for recruitment and planning without detection.
        - **Security agencies have reported that ISIS-affiliated groups use Telegram and dark web forums for recruiting Indian youth.**
            - The NIA arrested over 35 ISIS operatives in 2016, uncovering **encrypted extremism**, where Indian youth were being recruited on communication apps like Telegram and Signal.
- **IoT and Smart City Vulnerabilities:** The rapid adoption of **smart city technology**, including **surveillance cameras, traffic management, and public utilities, has created new cybersecurity risks.**
    - Many IoT devices deployed in India lack proper encryption and are vulnerable to hacking.
    - Compromised IoT networks can lead to large-scale disruptions, including blackouts, traffic gridlocks, and privacy breaches.
    - Hacktivist groups and hostile nations have already been probing these vulnerabilities.
        - For instance, **Mumbai's power outage in 2020** was linked to a cyberattack from China.

//



What Role can the Private Sector Play in Enhancing India's Cybersecurity Infrastructure?

- **Strengthening Cybersecurity R&D and Indigenous Solutions:** The private sector can drive innovation in cybersecurity by **investing in indigenous research and developing advanced security solutions** tailored to India's needs.
    - **Dependence on foreign cybersecurity firms** increases vulnerability to geopolitical risks and potential backdoors in imported technologies.
    - **Indigenous solutions, supported by private players,** can ensure data **sovereignty** and reduce risks from external dependencies.
    - For instance, **C3iHub, a cybersecurity Technology Innovation hub at IIT Kanpur** has partnered with **Tata Advanced Systems to advance cybersecurity solutions**
- **Collaborating with the Government on Cyber Threat Intelligence:** Private companies can work with government agencies to **share real-time threat intelligence** and **prevent cyberattacks on national infrastructure.**
    - Although CERT-In has introduced initiatives like **mandatory breach reporting**, intelligence-sharing remains fragmented with limited coordination between private firms and law enforcement.
    - A robust public-private threat intelligence network can enhance proactive threat detection and incident response.
        - This is crucial to counter cyber threats from state-sponsored actors.
        - For instance, **IBM's X-Force Threat Intelligence** collaborates with Indian authorities to identify and mitigate cyber threats.
- **Enhancing Cybersecurity in the Financial Sector:** With the rapid **digitization of banking, fintech, and UPI payments,** private players must strengthen security frameworks to prevent fraud and financial cybercrime.
    - Private-sector-led innovations like **AI-driven fraud detection and blockchain-based**

security can help secure financial transactions.
        - For instance, **ComplyAdvantage offers AI-driven fraud** and AML risk detection for financial institutions.
- **Building a Skilled Cybersecurity Workforce: Private-sector investment in cybersecurity education and skill development** is crucial to address India's acute shortage of trained cybersecurity professionals.
    - Many **Indian firms struggle to find skilled experts**, leading to weak cybersecurity postures in enterprises and government institutions.
        - In May 2023, nearly **40000 cybersecurity professional job vacancies** in India were not filled due to talent shortages.
    - Corporate entities can partner with universities, **offer cybersecurity boot camps, and provide in-house training to bridge this skill gap.** The private sector can also help establish global certification programs to upskill IT professionals.
- **Developing Secure Cloud and Data Protection Infrastructure:** As India moves towards **data localization,** private companies can help in building secure cloud and data storage solutions to safeguard national data assets.
    - Currently, **a significant portion of Indian data is hosted on foreign cloud platforms ,** posing risks of surveillance and unauthorized access.
        - Private firms can invest in AI-driven encryption and **zero-trust security frameworks to strengthen data protection.**
        - For instance, **Reliance Jio launched its indigenous JioCloud platform** to offer secure cloud storage solutions.
- **Regulating Deepfake and AI-Driven Cyber Threats:** With AI-generated **deepfake scams**, misinformation, and cyber fraud rising, private firms can help to develop detection tools to counter these threats.
    - Big tech firms and cybersecurity startups can create AI-based detection models to flag and counter deepfake content.
        - For instance, **McAfee® Deepfake Detector alerts people in seconds if it detects AI-generated audio in a video**, helping Indian consumers discern real from fake.
- **Promoting a Cyber-Aware Corporate Culture:** Private organizations can foster a **cybersecurity-first mindset** among employees by conducting regular training, phishing simulations, and policy enforcement.
    - **Human error remains one of the biggest cybersecurity vulnerabilities**, leading to **data breaches** and system compromises.
    - Regular cyber hygiene drills and incident response plans can significantly reduce cyber risks.
        - This is especially critical for **IT, BFSI, and healthcare sectors** handling sensitive data.

What are the Major Challenges in Onboarding Private Sector in Cybersecurity?

- **Lack of Clear Regulatory Framework and Policy Incentives:** The absence of a **well-defined cybersecurity framework** discourages private sector participation in national cyber defense initiatives.
    - Policies like the **National Cyber Security Strategy** remain largely unimplemented, and existing regulations are fragmented across multiple agencies.
    - Without **clear incentives, tax benefits, or liability protections,** private firms remain hesitant to invest in national cybersecurity efforts.
- **High Cost of Cybersecurity Investments:** Implementing robust cybersecurity infrastructure requires substantial financial investment, which **many private companies, especially MSMEs, struggle to afford.**
    - Advanced security solutions like **AI-driven threat detection, Zero Trust frameworks,** and cloud security demand continuous upgrades.
    - The **cost factor discourages private players** from proactively investing in cybersecurity, leaving them vulnerable to cyberattacks.
        - Indian organizations spend an average of just **$2.8 million annually** on cybersecurity, which typically amounts to **less than 10% of their IT budgets.**

- **Weak Public-Private Threat Intelligence Sharing:** Effective cybersecurity requires **real-time intelligence-sharing between government agencies and private firms,** but India lacks a structured framework for this.
    - Private firms fear regulatory backlash and reputational damage if they disclose cyber incidents.
    - **CERT-In mandated 6-hour breach reporting,** but compliance remains low due to fear of penalties.
- **Dependence on Foreign Cybersecurity Solutions:** M**any private firms in India rely heavily on foreign cybersecurity tools and software,** increasing risks of geopolitical vulnerabilities and surveillance backdoors.
    - While private companies prefer cost-effective foreign solutions, this creates a **strategic risk for national security.**
        - The lack of indigenous cybersecurity products forces Indian firms to depend on global vendors for critical security infrastructure.
- **Weak Cybersecurity Standards for Supply Chain Vendors:** Many **private firms depend on third-party vendors**, but India lacks strong cybersecurity compliance requirements for supply chains.
    - Attackers increasingly target **weaker links in supply chains** to gain access to larger corporations, particularly in BFSI, telecom, and IT sectors.
        - For instance, **over half (55%) of smart manufacturing firms** in India reported more than **6 intrusions** in 2023.

What Measures can be Adopted to Enhance Public-Private Partnership in Cybersecurity?

- **National Cybersecurity Coordination Body:** A unified **National Cybersecurity Council** with strong **private-sector representation** should be created to streamline public-private collaboration.
    - Currently, cybersecurity efforts are fragmented across **MeitY, CERT-In, NCIIPC, and RBI, leading to inefficiencies.** A centralized body can ensure seamless intelligence-sharing, coordinated incident response, and policy alignment.
- **Implementing a Secure Threat Intelligence-Sharing Platform:** A **National Cyber Threat Intelligence Exchange (NCTIX)** should be set up to facilitate real-time, automated intelligence-sharing between government agencies and private enterprises.
    - A **structured, anonymized data-sharing framework** with liability protections can encourage participation.
    - Advanced AI-driven monitoring can help detect, analyze, and mitigate cyber threats more effectively.
- **Offering Tax Incentives for Cybersecurity Investments:** To encourage private companies, especially MSMEs, to adopt robust cybersecurity measures, **tax credits and subsidies** should be provided for investments in cyber defenses.
    - The government can offer **R&D incentives for indigenous cybersecurity solutions** to reduce dependence on foreign tech.
    - Special grants should be allocated to firms working on AI-driven cyber defense solutions.
- **Strengthening Cybersecurity Skill Development Programs:** Corporations can collaborate with **universities, IT training institutes, and government programs** like **Skill India** to offer specialized cyber training.
    - Cybersecurity should be integrated into engineering and management curricula. Regular **cyber drills, hackathons, and ethical hacking contests** can create a skilled talent pool.
- **Mandating Cybersecurity Standards for Private Enterprises:** A **Cybersecurity Compliance Index** should be introduced, categorizing businesses based on their security maturity levels.
    - Private firms, especially in critical sectors like **BFSI, telecom, and IT**, should be required to meet **minimum cybersecurity standards** under a risk-based compliance framework.
    - The government can **subsidize security audits** for MSMEs to improve adoption. Strengthening **enforcement of the Digital Personal Data Protection Act (DPDPA) 2023** will ensure accountability.
- **Indigenous Cybersecurity Technology Ecosystem:** The government should work with **private firms and startups to develop indigenous cybersecurity tools** to reduce dependence on

foreign tech.
    - Incentives should be provided to **startups focusing on AI-driven threat detection, blockchain security, and cloud encryption**.
    - A dedicated **Cybersecurity Startup Fund** can accelerate innovation in this space.

Conclusion

Strengthening India's cybersecurity requires a **collaborative approach involving both the government and the private sector.** While initiatives like the CCITR show promise, India must **prioritize clear regulatory frameworks, enhanced policy incentives, and robust public-private partnerships.** Fostering indigenous cybersecurity solutions, sharing intelligence, and upskilling the workforce are crucial steps.

Drishti Mains Question:

Discuss the potential benefits and challenges of involving the private sector in India's cybersecurity framework. How can public-private partnerships enhance the country's cyber resilience?

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims

Q.1 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 specialised consultant to minimise 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)

Q.2 In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only

(b) 1 and 2 only

(c) 3 only

(d) 1, 2 and 3

Ans: (d)

Mains

Q. What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**
