Samyak
An Institute For Civil Services

DAILY MAINS ANSWER WRITING – 7 MAY

"A digitally empowered India demands a robust cybersecurity ecosystem." Examine the key challenges confronting cybersecurity in the country and recommend measures to enhance cyber talent and institutional capabilities. (250 words)

The goal of Digital India is to transform India into a digitally empowered society and knowledge economy. However, the transition to a Digital India comes with a new set of vulnerabilities. With India being the 3rd largest internet user base, cyber threats have grown significantly. CERT-In recorded a fourfold increase in incidents between 2017–18. Major attacks include Union Bank heist, WannaCry, and Zomato data breach.

Challenges to Cybersecurity

- **Absence of National Cyber Architecture**: Lack of unified strategy weakens threat assessment and response.
- **Skilled Workforce Gap**: Demand for cybersecurity experts far exceeds supply despite a large IT talent pool.
- **Insecure Devices**: Less than 1% of users access high-security mobile phones.
- **Reliance on Imports**: Foreign hardware/software may carry embedded vulnerabilities.
- **Awareness Deficit**: Limited knowledge of cyber laws and threats among individuals and corporations.

Strengthening Cyber Expertise

- **Update Cyber Policy**: A revised National Cyber Security Policy is needed to match evolving threats.
- **Integrated Governance**: Define clear roles for agencies and enhance state-level capacities.
- **Human Capital**: Invest in training skilled professionals in cybersecurity domains.
- **Public-Private Partnership**: Leverage private sector resources and innovation through budgetary and policy support.

With the digital economy forming 14–15% of India's GDP securing cyberspace is vital for economic resilience. A robust cybersecurity framework is critical to safeguard India's digital future.

"डिजिटल रूप से सशक्त भारत हेतु एक मजबूत साइबर सुरक्षा तंत्र की आवश्यकता है।" देश में साइबर सुरक्षा के समक्ष प्रमुख चुनौतियों की जांच करें तथा साइबर प्रतिभा और संस्थागत क्षमताओं को बढ़ाने के उपायों पर चर्चा करें। (250 शब्द)

डिजिटल इंडिया का लक्ष्य भारत को डिजिटल रूप से सशक्त समाज और ज्ञान अर्थव्यवस्था में बदलना है। हालाँकि, डिजिटल इंडिया में परिवर्तन के साथ ही कई नई चुनौतियां भी जुड़ी हैं। तीसरा सबसे बड़ा इंटरनेट उपयोगकर्ता होने के कारण, भारत में साइबर खतरे काफ़ी बढ़ गए हैं। CERT-In ने 2017-18 के मध्य घटनाओं में चार गुना वृद्धि दर्ज की। प्रमुख हमलों में यूनियन बैंक डकैती , वानाक्राई और ज़ोमैटो डेटा ब्रीच शामिल हैं।

साइबर सुरक्षा की चुनौतियाँ

- **राष्ट्रीय साइबर संरचना का अभाव** : एकीकृत रणनीति का अभाव खतरे के आकलन और प्रतिक्रिया को कमजोर करता है।
- **कुशल कार्यबल का अंतर** : विशाल आईटी प्रतिभा पूल के बावजूद साइबर सुरक्षा विशेषज्ञों की मांग, आपूर्ति से कहीं अधिक है।
- **असुरक्षित उपकरण**: 1% से भी कम उपयोगकर्ता उच्च सुरक्षा वाले मोबाइल फोन का उपयोग करते हैं।
- **आयात पर निर्भरता**: विदेशी हार्डवेयर/सॉफ्टवेयर में अंतर्निहित मुद्दे हो सकते हैं।
- **जागरूकता की कमी**: नागरिकों और निगमों में साइबर कानूनों एवं खतरों का सीमित ज्ञान।

साइबर विशेषज्ञता को सुदृढ़ बनाना

- **साइबर नीति का अद्यतन**: उभरते खतरों से निपटने हेतु एक संशोधित राष्ट्रीय साइबर सुरक्षा नीति की आवश्यकता है।
- **एकीकृत शासन**: एजेंसियों के लिए स्पष्ट भूमिकाएं परिभाषित करें और राज्य-स्तरीय क्षमताओं को बढ़ाएं।
- **मानव पूंजी**: साइबर सुरक्षा क्षेत्र में कुशल पेशेवरों के प्रशिक्षण में निवेश करें।
- **सरकारी निजी भागीदारी**: बजटीय एवं नीतिगत समर्थन के माध्यम से निजी क्षेत्र के संसाधनों एवं नवाचार का लाभ उठाना।

डिजिटल अर्थव्यवस्था भारत के सकल घरेलू उत्पाद का 14-15% हिस्सा बनाती है; आर्थिक लचीलेपन हेतु साइबरस्पेस को सुरक्षित रखना बहुत ज़रूरी है। भारत के डिजिटल भविष्य की सुरक्षा के लिए एक मज़बूत साइबर सुरक्षा ढांचा बहुत ज़रूरी है।