



## Rising up to Cyber Security Challenges

This editorial is based on [“Cyberattacks are rising, but there is an ideal patch”](#) which was published in the Hindu on 25/02/2023. It highlights the challenges posed by cyber threats while also envisaging greater role by India for consensus on Cyber security through G20 Presidency.

**For Prelims:** Cyber security, Ransomware, Indian Cyber Crime Coordination Centre (I4C), Budapest Convention on Cybercrime, Indian Computer Emergency Response Team (CERT-In), Cyber Surakshit Bharat, Cyber Swachhta Kendra, National Cyber security Coordination Centre (NCCC), Draft Digital Personal Data Protection Bill 2022, G20

**For Mains:** Recent Instances of Cyber Attacks in India, Major Types of Cyber Threats, Challenges Related to India's Cyberspace.

The past few incidents have highlighted the **vulnerabilities of our fast-expanding digital networks**. The first one targeted the [servers of India's All India Institute of Medical Science](#) (AIIMS), **compromising around 40 million health records** and causing a **two-week-long system outage**.

Another attack involved a ransomware group, **BlackCat**, **breaching the parent company of Solar Industries Limited, a Ministry of Defence ammunition and explosives manufacturer, and stealing over 2 Terabytes of data**.

These incidents highlight the **urgent need for increased cybersecurity measures** to prevent such attacks from happening in the future.

### What are the Challenges related to Cyber Security?

- **Recent Cyber Attacks:**
  - Ransomware attacks are becoming more frequent and costly, with over 75% of Indian organizations having faced such attacks and each breach costing an average of ₹35 crore of damage.
- **Vulnerability of Critical Infrastructure:**
  - The lines between the physical and digital realms are blurring rapidly, making **Critical infrastructure** extremely vulnerable to attacks from **hostile state and non-state actors**.
  - Cyber capabilities can be used to undermine critical infrastructure, industry, and security, **as seen in the ongoing conflict in Ukraine** where **electronic systems in warheads, radars, and communication devices have reportedly been rendered ineffective** using hacking and GPS jamming.
- **Under-Preparedness:**
  - CERT-In has introduced guidelines for organizations to comply with when connected to the digital realm, but **most organizations lack the tools to identify and prevent**

### **cyberattacks.**

- Also, there is an **acute scarcity of cybersecurity professionals** in India.
- **Limited Private Sector Participation:**
  - Private sector participation remains limited in India's cybersecurity structures, and collaboration with like-minded intergovernmental and state frameworks is necessary to protect users and customers from cyber breaches.
- **Added Complexity:**
  - With more inclusion of [artificial intelligence \(AI\)](#), [machine learning \(ML\)](#), [data analytics](#), [cloud computing and Internet of Things \(IoT\)](#), cyberspace will become a complex domain, giving rise to issues of a techno-legal nature.
  - The **introduction of 5G and the arrival of quantum computing** will increase the potency of malicious software.

## **What are the Initiatives Regarding Cyber Security?**

- **Global Initiatives:**
  - **Budapest Convention on Cybercrime:** It is an [international treaty](#) that seeks to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It came into force on 1<sup>st</sup> July 2004. **India is not a signatory** to this convention.
  - [Internet Governance Forum \(IGF\)](#): It brings together all stakeholders i.e., government, private sector and civil society on the Internet governance debate.
  - **UNGA Resolutions:** The [United Nations General Assembly](#) established two processes on the issues of security in the information and communication technologies (ICT) environment.
    - The **Open-ended Working Group (OEWG)** through resolution by Russia
    - The **Group of Governmental Experts (GGE)** through resolution by USA
- **Indian Initiatives:**
  - [National Cyber Security Strategy 2020](#): It seeks to improve cyber awareness and cybersecurity through **more stringent audits**. Empanelled cyber auditors will look more carefully at the security features of organisations than are legally necessary now.
  - [National Critical Information Infrastructure Protection Centre \(NCIIPC\)](#): The NCIIPC, created under Information Technology Act, 2000, operates as the **nodal agency for protection and resilience of critical information infrastructure**
  - [Indian Cyber Crime Coordination Centre \(I4C\)](#): It was setup in 2020 to **deal with all types of cybercrimes** in a comprehensive and coordinated manner.
  - Cyber Surakshit Bharat Initiative: It was launched in 2018 with an aim to spread **awareness about cybercrime and building capacity** for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.
  - **Cyber Swachhta Kendra:** In 2017, this platform was introduced for internet users to clean their computers and devices by wiping out viruses and malware.
  - **Information Technology Act, 2000:** The Act regulates use of computers, computer systems, computer networks and also data and information in electronic format.
  - [National Cyber Crime Reporting Portal](#): It is a citizen-centric initiative which will **enable citizens to report cybercrimes online** and all the complaints will be accessed by the concerned law enforcement agencies for taking action as per law.
  - [Computer Emergency Response Team - India \(CERT-In\)](#): It is an organization of the **Ministry of Electronics and Information Technology** which collects, analyses and disseminates information on cyber incidents, and also issues alert on cybersecurity incidents.
  - **Cybersecurity Treaties:** India has already signed **cybersecurity treaties with countries such as the US, Russia, the UK, South Korea, and the European Union.**
  - **Multilateral Frameworks:** Efforts are being made in multinational frameworks such as the **Quad and the I2U2 to enhance cooperation in cyber incident responses, technology collaboration, capacity building, and in the improvement of cyber resilience.**
  - [India's draft Digital Personal Data Protection Bill 2022](#): It seeks to ensure usage of personal data for lawful purposes only and proposes a penalty of up to ₹500 crore for data

breaches.

- **Defence Cyber Agency (DCyA):** It is created by Indian armed forces and is capable of offensive and defensive manoeuvres.

## How can India Utilize G20 Summit to Build Consensus on Cyber Security?

- **Utilizing the Opportunity of the G20 Summit:** As the host nation for the [G20 summit](#), India can use this opportunity to bring together all the stakeholders driving the global levers of power to discuss cybersecurity.
- **Creating a Global Framework:** India could take the lead in conceptualizing a **global framework of common minimum acceptance for cybersecurity**. This would be a significant contribution to collective security and a step towards building consensus on cybersecurity.
- **Raising Awareness:** India can use the G20 summit to raise awareness about cybersecurity issues, **emphasizing the importance of taking preventive measures and developing effective cybersecurity policies**.

## What can be the Way Forward?

- **International Cooperation:** It is of critical importance to ensure global cooperation through **information sharing and strengthening joint efforts** in cybersecurity research and development as most cyberattacks **originate from beyond the borders**.
  - India can **consider joining Budapest Convention along with Multilateral initiatives like QUAD**.
- **Plugging the Gaps:** It is **important for the corporates or the respective government departments to find the gaps in their organisations** and address those gaps and create a **layered security system**, wherein security threat intelligence sharing is happening between different layers.
- **A Truly Global Framework:** It is needed as the current efforts are operating in silos. **An apex body will be able to ensure operational coordination** amongst various agencies.
- **Coordination and Information Dissemination:** Formalize the coordination and **prioritization of cyber security research and development activities**; disseminate vulnerability advisories and threat warnings in a timely manner.

### Drishti Mains Question

India is facing increased threat of cyber-crimes since pandemic. How can India tackle these threats and develop Global consensus on cyber security? Analyse in the context of India's G20 Presidency.

## 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)**

---

PDF Reference URL: <https://www.drishtiias.com/current-affairs-news-analysis-editorials/news-editorials/27-02-2023/print>

