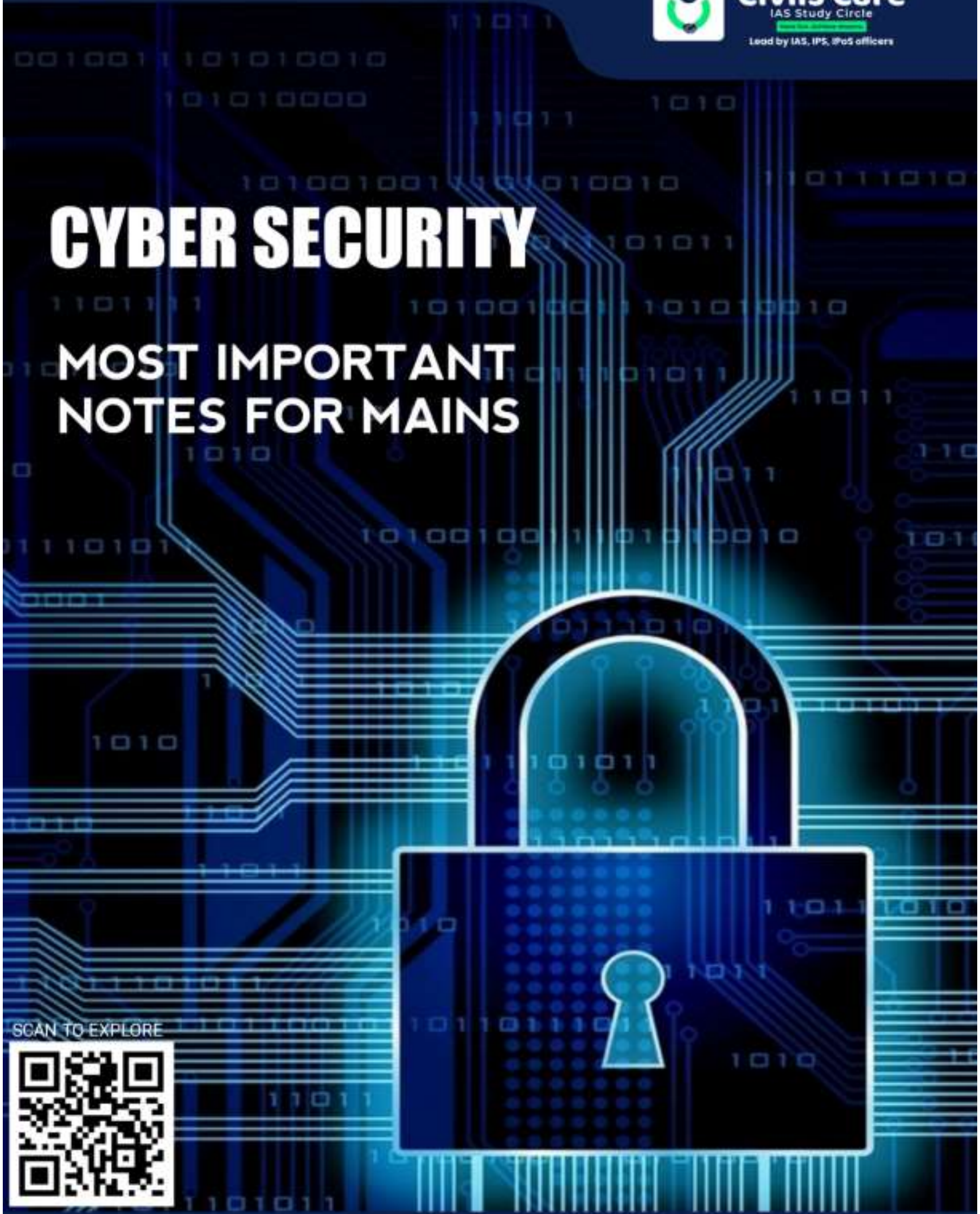
Civils Cafe
IAS Study Circle
Lead by IAS, IPS, IPoS officers

CYBER SECURITY

MOST IMPORTANT NOTES FOR MAINS



SCAN TO EXPLORE

✆ 730 699 4905 ☎ 9048 073 888
www.thecivilscafeias.com

thecivilscafeias
civilscafeiassc

GS 3 -INTERNAL SECURITY

CYBER SECURITY

Cyber Security is protecting cyber space including **critical information infrastructure** from attack, damage, misuse and economic espionage.

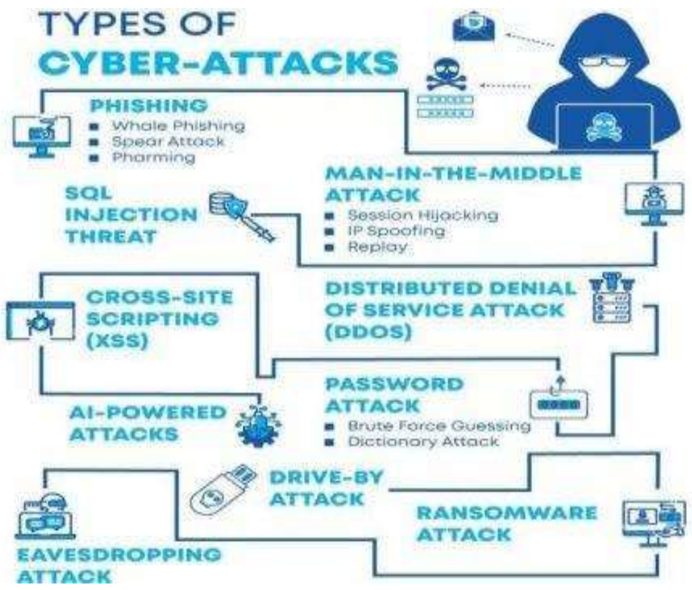
- Global Information Security Survey (GISS) 2018-19 – India edition, one of the highest numbers of cyber threats have been detected in India, and the country ranks second in terms of targeted attacks.
- India already is the 2nd largest online market worldwide.

Critical Information Infrastructure: According to Section 70(1) of the **Information Technology Act,** CII is defined as a “computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety”.

- National Critical Information Infrastructure Protection Centre (NCIIPC) has identified the following as ‘Critical Sectors’: –
  - Power&Energy,Banking,FinancialServices&Insurance,Telecom, Transport,Government,Strategic & Public Enterprises.

Cyber Attack: It is a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation.

Cyber Space: A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers



Importance of Cyber Security

- There has been a rapid increase in the use of the online environment where millions of users have access to internet resources and are providing content on a daily basis.
- The use of internet particularly for the **distribution of obscene, indecent and pornographic content.** Use of internet for child pornography and child sexual abuse is a concern**.**
- The **increasing business transaction** from tangible assets to intangible assets like Intellectual Property has converted Cyberspace from being a mere info space into an important commercial space and also to ensure Business continuity.
- With the growing adoption of the Internet and smart-phones, India has emerged “as one of the favourite countries among cyber criminals.”
    - The number of cyber-crime cases registered under IT Act 2000 in India has risen by 300 percent in the period from 2011 to 2014, according to a joint study by PwC and Assocham.
- India witnessed more than 27,000 cyber security threat incidents in the first half of 2017. Example: WannaCry Ransomware.
- Recently, a Chinese Group named as “Red Echo” was behind a malware attack known as “Shadow pad” on India’s critical information infrastructure such as Ports, power systems etc.
- **Financial loss**: According to the Data Security Council of India, India has

been the second most cyber-attacks affected country between 2016 to 2018. Cyber-crimes in India caused Rs 1.25 lakh crore loss in 2019.

- More than that, people working in the technology-based gig economy depend on the Internet for their livelihoods. E.g. delivery workers for Swiggy, Dunzo and Amazon and the cab drivers of Uber and Ola
- To ensure critical infrastructure systems do not collapse under any situation.
- For the success of government initiatives like Digital India, Make in India and Smart Cities.
- To balance Individual's rights, liberty and privacy in cyberspace.
    - Issues like Fake News, cyber bullying etc are growing in recent days.

ISSUES/CHALLENGES

- **Cyber terrorism-** is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.
- **Digital Data Threat:** Growing online transactions have generated bigger incentives for cybercriminals. Besides, establishments looking to mine data (customer information, results of product surveys, and generic market information), they also create intellectual property that is in itself an attractive target.
- **Cyber warfare:** It involves the actions by a nation-state or international organisation to attack and attempt to damage another nation's computers or information networks.
- **Lack of robust law enforcement mechanisms:** India's approach to cyber security has so far been ad hoc and unsystematic. Despite a number of agencies, policies and initiatives, their implementation has been far from satisfactory.
- **Lack of Coordination:** Due to the existence of too many agencies with overlapping functions in the field of cyber security, coordination between these agencies is poor.

- **Lack of Coordination:** Due to the existence of too many agencies with overlapping functions in the field of cyber security, coordination between these agencies is poor.

- The threats could also be to critical infrastructure systems like nuclear plants, railways, as they use outdated technologies and weaker protocols.

MEASURES TAKEN BY GOVERNMENT IN THE DOMAIN OF CYBER SECURITY

- **Information Technology Act, 2000:** The Information Technology Act, 2000 (amended in 2008) is the primary law for dealing with cybercrime and digital commerce in India.
- **National Cyber Security Policy, 2013:** The policy provides the vision and strategic direction to protect the national cyberspace.
- The **CERT-In** (Cyber Emergency Response Team – India): CERT-In has been operational since 2004. It is the national nodal agency for responding to computer security incidents as and when they occur.
- **Indian Cyber Crime Coordination Centre (I4C)**:The Union Government has decided to set up 14C. It will be an apex coordination centre to deal with cybercrimes.
- **Cyber Swachhta Kendra:** Launched in early 2017, the Cyber Swachhta Kendra provides a platform for users to analyse and clean their systems of various viruses, bots/ malware, Trojans, etc.
- **Cyber Surakshit Bharat**: Ministry of Electronics and Information Technology, launched the Cyber Surakshit Bharat initiative 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.
- **The Cyber Warrior Police Force**: In 2018, the government announced its plans to introduce CWPF. It is proposed to be raised on lines of the Central Armed Police Force (CAPF).
- Cyber-Crime Prevention against Women & Children' Scheme: Implemented by the Ministry of Home Affairs, the scheme aims to prevent and reduce cyber-crimes against women and child.

GLOBAL MECHANISMS IN CYBER SECURITY

- The **International Telecommunication Union (ITU)** is a specialised agency within the United Nations which plays a leading role in the standardisation and development of telecommunications and cyber security issues.

- **Budapest Convention on Cybercrime:** It is an international treaty that seeks to address Internet and computer crime (cybercrime) by harmonising national laws, improving investigative techniques, and increasing cooperation among nations. It came into force on 1 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. It was first convened in October–November 2006.
- Internet Corporation for Assigned Names and Numbers (ICANN): It is a non-profit organisation responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation. It has its headquarters in Los Angeles, U.S.A.

CYBER SECURITY LAWS IN INDIA

- **Information Technology Act (IT Act), 2000**
  - The act regulates use of computers, computer systems, computer networks and also data and information in electronic format.
  - The act lists down among other things, following as offences:

    ✓ Tampering with computer source documents.

    ✓ Hacking with computer system

    ✓ Act of cyber terrorism i.e., accessing a protected system with the intention of threatening the unity, integrity, sovereignty or security of country.

    ✓ Cheating using computer resource etc.

    ✓ **Strategies under National Cyber Policy, 2013**
- Creating a secure cyber ecosystem.
- Creating mechanisms for security threats and responses to the same through national systems and processes.

  ✓ National Computer Emergency Response Team (CERT-in) functions as the nodal agency for coordination of all cyber security efforts, emergency responses, and crisis management.

  ✓ Promoting cutting edge research and development of cyber security technology.

  ✓ Human Resource Development through education and training programs to build capacity.

    - ✓ Promoting cutting edge research and development of cyber security technology
- Protection and resilience of critical information infrastructure with the **National Critical Information Infrastructure Protection Centre** (NCIIPC) operating as the nodal agency.

Way forward

- **AI and machine learning can boost cyber defences**: As artificial intelligence and machine learning gathers pace, and starts to impact more and more industries, it's sure to play a bigger role in cyber security.
- **Real-time intelligence** is required for preventing and containing cyber-attacks.
- Periodical '**Backup of Data'** is a solution to ransomware.
- Using the knowledge gained from actual attacks that have already taken place in building effective and pragmatic defence.
- Increased awareness about cyber threats for which **digital literacy** is required first.
- India needs to secure its computing environment and IoT with current tools, patches, updates and best-known methods in a timely manner.
- The need of the hour for the Indian government is to develop core skills in cyber security, data integrity and data security fields while also setting stringent cyber security standards to protect banks and financial institutions.
- The proposed project **NETRA** for internet surveillance should be taken up. Concerns about privacy and freedom of expression have to be taken care of.
- There is an urgent need to build a **Digital Armed Force** of trained IT professionals to carry on both defensive and offensive operations.
- **Cybersecurity Help Desks** need to be set up to provide guidance and support to first level users.
- State Governments should also take up operations for Cybersecurity.
    - o Example: **SHE Team** of Telangana Government has been successful in protecting women from online harassment and cybercrimes.

- Public Private Partnership (PPP) in cybersecurity. Eg: **Cyberdome project** of Kerala Police.

The Internet has redefined the way we interact, share and transmit information. In this highly interconnected world cybersecurity is critical for social, economic, political wellbeing of the Humankind

National Cyber Security Strategy 2020

The National Cybersecurity Strategy is being formulated by the Office of National Cyber Security Coordinator at the **National Security Council Secretariat.**

- National Security Council (NSC)of India is a three-tiered organisation that oversees political, economic, energy and security issues of strategic concern.
- **Aim:**
    - 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.
- **Need:**
    - Cyber warfare offensives:
        - The United States is just one of many countries that have invested significant amounts of money in developing not just defences against attack, but the ability to mount damaging cyber warfare offensives.
        - The countries which are believed to have the most developed cyber warfare capabilities are the United States, China, Russia, Israel and the United Kingdom.
    - Increased Digital usage post-Covid:
        - Critical infrastructure is getting digitised in a very fast way — this includes financial services, banks, power, manufacturing, nuclear power plants, etc.

- ❖For Protecting Critical Sectors:

    - It is particularly significant given the increasing interconnectedness of sectors and proliferation of entry points into the internet, which could further grow with the adoption of 5G.
    - There were 6.97 lakh cyber security incidents reported in the first eight months of 2020, nearly equivalent to the previous four years combined, according to information reported to and tracked by Indian Computer Emergency Response Team (CERT-In).

- ❖Recent Cyber Attacks:

    - There has been a steep rise in the use of resources like malware by a Chinese group called Red Echo to target a large swathe of India's power sector.
    - Red Echo used malware called Shadow Pad, which involves the use of a backdoor to access servers.
    - A Chinese hacker group known as Stone Panda had identified gaps and vulnerabilities in the IT infrastructure and supply chain software of Bharat Biotech and the Serum Institute of India.
    - SolarWinds hack, impacted national critical infrastructure in the USA.

- ❖For Government:

    - A local, state or central government maintains a huge amount of confidential data related to the country (geographical, military strategic assets etc.) and citizens.

- ❖For Individuals:

    - Photos,videos and other personal information shared by an individual on social networking sites can be inappropriately used by others, leading to serious and even life-threatening incidents.

- For Businesses:
  - Companies have a lot of data and information on their systems. A cyber-attack may lead to loss of competitive information (such as patents or original work), loss of employees/customers' private data resulting in complete loss of public trust on the integrity of the organisation.

.

Civils Cafe
IAS Study Circle
Lead by IAS, IPS, IPoS officers
THE UNBEATABLES 2023
PRELIMS MAINS
INTERVIEW BATCH
ADMISSIONS OPEN
Mentored by Sasikanth
Senthil IAS Ex
730 699 4905 ☎ 9048 073 888
www.thecivilscafeias.com
thecivilscafeias
civilscafeiassc