GS SCORE

An Institute for Civil Services

www.iasscore.in

Gist of RSTV RAJYA SABHA Debate

# CYBER SECURITY

GS SCORE
An Institute for Civil Services

# IAS 2021-22
# GS FOUNDATION

## PATHWAYS
*for* UNDER GRADUATES

### 3 & 2 Year IAS FOUNDATION PROGRAMME

BATCH STARTS
**15 MARCH 2021**

## IAS 2022
## GS FOUNDATION

### 1 Year & 2 Year PROGRAMME

BATCH STARTS
**15 MARCH 2021**

1B, 2nd Floor, Pusa Road Karol Bagh, New Delhi-110005,
(Adjacent to Karol Bagh Metro Gate No. 8)
info@iasscore.in /iasscore

Visit: www.iasscore.in
8448496262

# CYBER SECURITY

## INTRODUCTION

Increasing cyber-attacks on large economies, including India, have highlighted the need to focus on cybersecurity skills. The pandemic has brought to the forefront the key issues every organization faces in the realm of security. It is now imperative for cybersecurity companies to do a radical overhaul and ensure their product or service fits in seamlessly into their customer's system and is fully secure.

In this episode, we will discuss and analyze the challenges in the Cyber Security domain and the ways of tackling those challenges.

## EDITED EXCERPTS FROM THE DEBATE

### Why Cyber Security is crucial in 2021?

- **More digitalization:** With the definitive **Make in India initiatives** announced by the Indian government and estimates reporting that over 5 billion devices would connect to the internet in the coming months and years, India needs to lay down solid cybersecurity plans and policies.
- **Frequent attacks:** The increasing cyber-attacks in the year 2020 have made organizations rethink their security measures, especially in terms of enterprise data security.
- **Increased vulnerability:** As organizations expand work-from-home and remote working solutions for their employees, the number of vulnerable endpoints increases.

### What are the barriers to cybersecurity?

- The biggest barriers to the growth of the cybersecurity industry are:
  - inchoate and diffuse nature of the threats

- lack of awareness about the importance of cybersecurity measures
- lack of investment to improve their cybersecurity measures
- Inability to frame an adequate response in the absence of tangible perpetrators.
- Since cyberspace is relatively new, legal concepts for "standards of care" do not exist

### What needs to be done?

- **Awareness drive:** The Government needs to do a large-scale awareness drive on a national scale to expand the scope of the cybersecurity industry.
- **Inclusive approach:** There is a need to make cybersecurity more inclusive and approachable to the common masses, SMEs, and budding startups.
- **Introduction in education structure:** There is also a need to introduce cybersecurity as a subject in schools and colleges, which will help in building strong information about cybersecurity, right from the beginning.
- **National policy:** Furthermore, the government must formulate a national regulatory policy and facilitate the promotion of cybersecurity research and development. The policy needs to be more strong and more scalable.

## CONCLUSION

A lot of technologies have emerged in the last 10-20 years. These new technologies have redefined how organizations conduct business operations, their communication channels, data processing and storage, and so on. The technological changes in the past decade have resulted in an advanced approach for executing cybercrimes.

Therefore, effective cybersecurity policies should in place which tends to eliminate the possibility of an attack.

## VALUE ADDITION

### Important terms

- **Cyber Space:** Cyber Space is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. It is a term associated with the application of the Internet worldwide.
  - Cyberspace is continuing to expand and has no geographical limitation.
- **Cyberattack:** A cyberattack is an intentional act conducted by one or more cybercriminals to steal data, fabricate information, or disable digital systems.
- **Cyber Security**: Cyber Security is a broad spectrum phrase and relates to preventing any form of unauthorized and malafide access to a personal computer, laptop, smartphone, or a major network like the national banking system or the railway network or a national information technology asset that also has military implications.

## Different types of Cyberattacks

- **Botnet:** Botnet is a network of devices that have been infected with malicious software, such as a virus.
- **Malware:** Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.
- **Phishing:** Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email.
- **Ransomeware:** Among the types of cyber warfare attacks, ransomware stands as one of the riskiest ones as highly critical information can be at stake. In a ransomware attack, the victim is forced to delete all necessary information from their system if they fail to pay a ransom within the timeline given by cybercriminals.
- **Trojan Horses:** A Trojan is a malware software program that aims at hacking digital devices by appearing as useful software to the victims.
  - It is one of the most dangerous types of Cyberattacks. It helps attackers get financial details alongside all other confidential information of the victims.

## Steps Taken to Deal with Cyber Crime and Cyber Security

- **Cybercrime reporting portal:** The Government has launched the online cybercrime reporting portal, www.cybercrime.gov.in to enable complainants to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries, or sexually explicit content.
- **Indian Cyber Crime Coordination Centre (I4C):** The Central Government has rolled out a scheme for the establishment of the Indian Cyber Crime Coordination Centre (I4C) to handle issues related to cybercrime in the country in a comprehensive and coordinated manner.
- **NCIIPC:** Establishment of National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.
- Cyber Swachhta Kendra: Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been launched for providing detection of malicious programs and free tools to remove such programs..

**********

# GS SCORE

An Institute for Civil Services

## OUR CLASSROOM & ONLINE COURSES

### GS FOUNDATION

- ☑ 1 Year IAS Foundation
- ☑ 3 & 2 Year IAS Foundation
- ☑ GS Mains Foundation

### OPTIONAL FOUNDATION

- ☑ Political Science
- ☑ History
- ☑ Geography
- ☑ Public Administration

### MAINS COURSES

- ☑ GS Mains Advance
- ☑ GS Mains QIP
- ☑ Ethics Integrity & Aptitude
- ☑ Essay Writing
- ☑ GS Paper 3

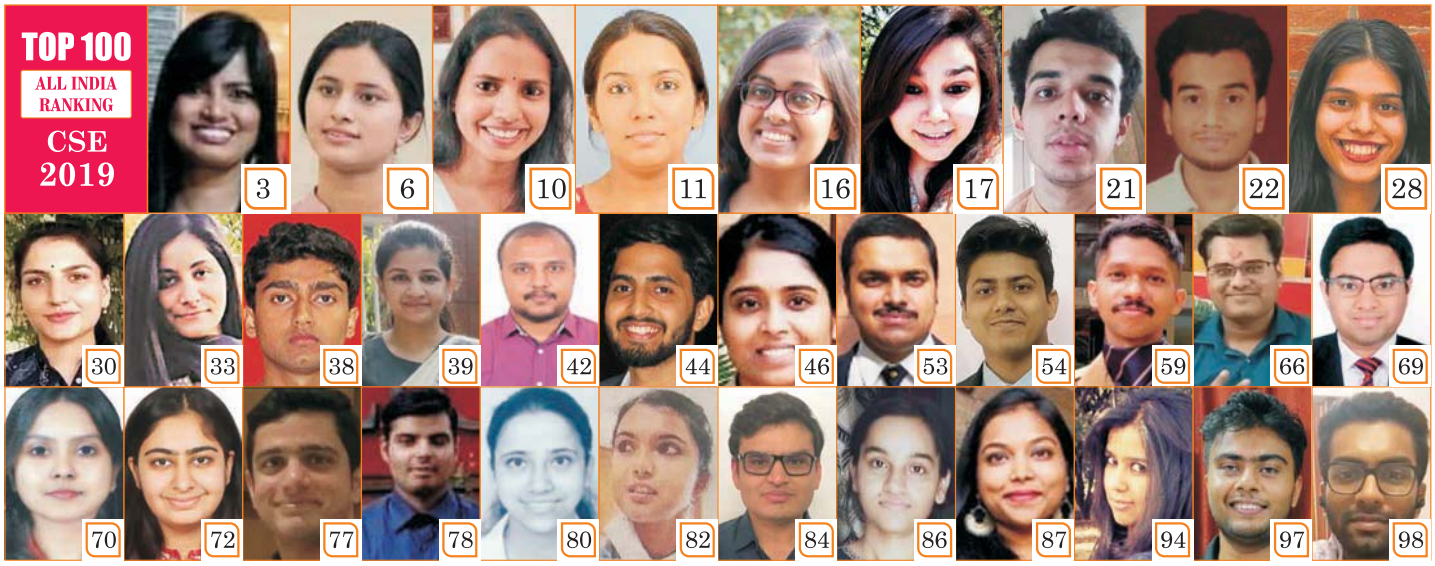
### TEST SERIES

- ☑ Prelims Test Series
- ☑ GS Mains Test Series
- ☑ Essay Test Series
- ☑ Ethics Test Series
- ☑ Optional Test Series
  - ◎ Political Science
  - ◎ Geography
  - ◎ History
  - ◎ Public Administration

Visit: www.iasscore.in

GS SCORE
An Institute for Civil Services

CSE RESULTS




# SUCCESS IS A PRACTICE WE DO!