Global Cybersecurity - India in Top 10: RSTV - Big Picture

Anchor: - Vishal Dahiya

Participants:

1. Jiten Jain, Cyber Security Expert
2. R. Ramanan, Mission Director, Atal Innovation Mission, NITI Aayog

Context:

India has been ranked 10th in the **Global Cyber Security Index 2020**. Meanwhile, at UNSC, India has also flagged the sophisticated use of cyberspace by terrorists and reiterated its commitment to open, secure, free, accessible & stable cyberspace.

At the UN, India commented on the rising tide of cyber threats and said that cyber threats cannot be dealt with in isolation. The Foreign Secretary also said that India is committed to an open, secure, free, accessible, and stable cyberspace environment, which will become an engine for innovation, economic growth, sustainable development, ensure free flow of information, and foster respect for cultural and linguistic diversity.

Introduction:

Computer security, cybersecurity, or information technology security (IT security) is the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

The field is becoming increasingly significant due to the increased reliance on computer systems, the Internet, and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things".

Also read: Types of cyber attacks

Recent cases of cyber attacks

- **Colonial Pipeline** was hit with a devastating cyberattack that forced the company to shut down approximately 5,500 miles of pipeline in the United States, crippling gas delivery systems in southeastern states.
- Chinese group Red Echo used malware called **ShadowPad** to cripple the power sector in Mumbai.

Causes for increase in cyber attacks:

- A drastic increase in the number of internet and smartphone users.
- Fast evolving technologies like IoT and artificial intelligence.
- Presence of non-traceable payment systems like Bitcoin.
- State backing to organized cyber attacks.
- Forced assent for the usage of apps.
- Digitization of banking

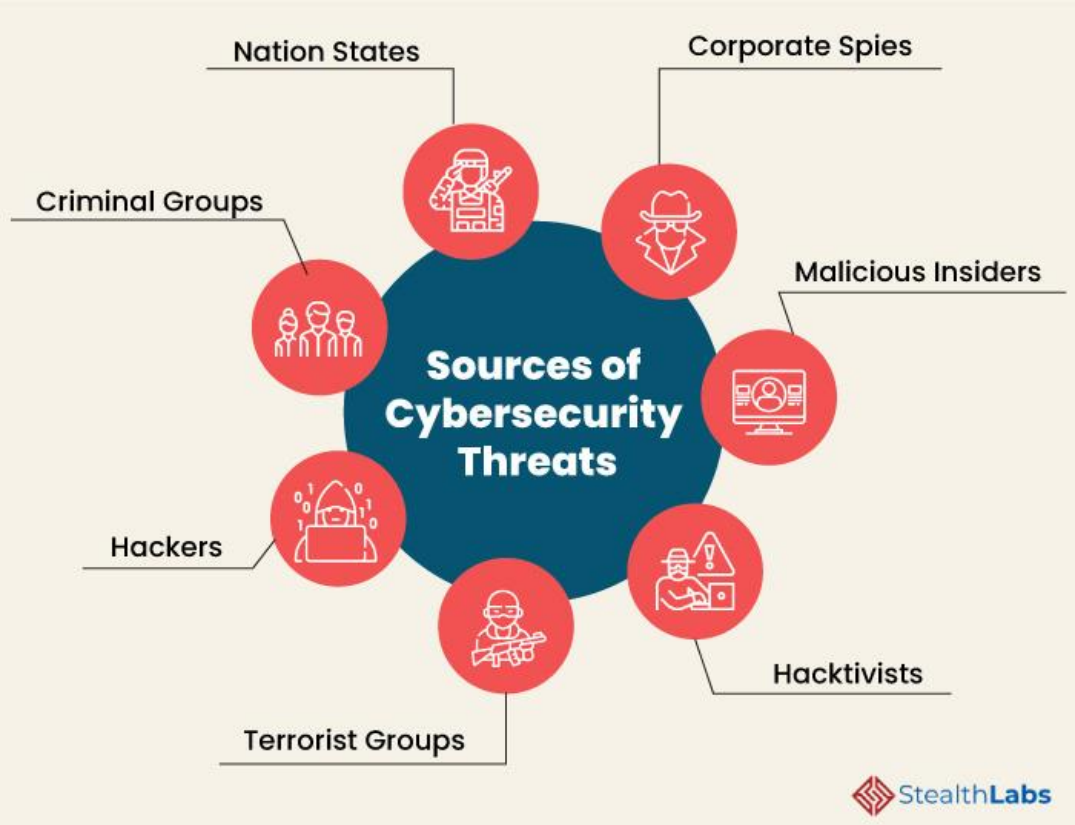

Image source: https://www.stealthlabs.com/

Cybersecurity infrastructure:

1.
    1. National Cyber Security Policy, 2013 aims at:
        1. Protection of information infrastructure in cyberspace
        2. Reducing vulnerabilities
        3. Building capabilities to prevent and respond to cyberthreats
    2. **CERT-IN** issues alerts and advisories regarding the latest cyber threats and countermeasures on a regular basis.
    3. **The National Critical Information Infrastructure Protection Centre** has been established for the protection of critical information infrastructure in the country.

- **Information Technology Act, 2000**

1. **Indian Cyber Crime Coordination Centre** scheme has been rolled out by the Ministry of Home Affairs (MHA) for the period 2018-2020, to combat cybercrime in the country, in a coordinated and effective manner.
2. **Cyber Surakshit Bharat Initiative** aims to spread awareness of cybercrime and build capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.

Way forward:

Cyberspace is an evolving arena so we need to continuously work on the following aspects for perpetual security.

- We need updated laws like the new Cybersecurity Strategy.
- SOPs need to be constructed in case of theft.
- Hackathons need to be conducted on a regular basis to find Zero-day vulnerabilities.
- We need to spread awareness of Cyber Hygiene.
- The CERT-IN needs to be upgraded to a Cyber Defence Agency.

A holistic approach is therefore required to maintain a Cyber Surakshit Bharat.

Second image give image source: https://www.itgovernance.co.uk/

Read all the RSTV articles in the link.