The Big Picture: Global cyber security - India in top 10

CONTEXT: According to a United Nations report, **India has jumped 37 places to 10th position in the Global Cyber Security Index (GCI) 2020**. Meanwhile **at UNSC India has also flagged sophisticated use of cyberspace by terrorists and reiterated its committed to open, secure, free, accessible & stable cyberspace.**

ABOUT THE GLOBAL CYBER SECURITY INDEX (GCI) 2020:

- The GCI is a **composite index created, analyzed and published by the International Telecommunication Union**, a specialized agency of the United Nations.
- The latest report is the fourth GCI edition, the first version of which was launched six years ago.
- Breaking into the top 10 in the list, India also **ranks fourth in the Asia-Pacific region**.
- GCI measures countries' commitment to cybersecurity on a global scale, to raise awareness of the importance and various dimensions of the issue.
- The top rank in the GCI was achieved by the US with a score of 100. The UK and Saudi Arabia finished second.
- Other countries at the top of the index include South Korea and Singapore rank fourth globally, Russia, the United Arab Emirates and Malaysia at fifth place, Lithuania at sixth, Japan at seventh and Canada, France and India at the subsequent positions.
- Each country's development or engagement is assessed along **five pillars –**
  1. Legal measures
  2. Technical measures
  3. Organizational measures
  4. Capacity development, and
  5. Cooperation- and then aggregated into a composite score

FLAGGING CYBERSECURITY CONCERNS AT UNSC:

- India raised **concerns about cross-border state-sponsored cyber-attacks** during the UNSC Open Debate on "Maintenance of International Peace and Security: Cyber Security".
- The world is already witnessing the use of cyber tools to compromise state security through **attacking critical national infrastructure**, even **disrupting social harmony through radicalization**.
- **"Open societies" have been "particularly vulnerable" to cyber-attacks and "disinformation" campaigns,** as opposed to states like China that control all forms of online communication.
- **The borderless nature of cyberspace and more importantly, the anonymity of actors** involved have challenged the traditionally accepted concepts of sovereignty, jurisdiction and privacy.
- Countries cannot work in "isolation" and member states have to **adopt a "collaborative" rules-based approach** in cyberspace and work towards ensuring its openness, stability and security.
- Fostering **equitable access to cyberspace and its benefits** should also form an important component of this international co-operation.
- There is a need to **bridge fissures in digital inequalities through "capacity building".**

WHAT IS CYBERSPACE?

"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."

NEED FOR CYBERSECURITY

Global Scenario:

- 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.
- Cyber-attacks continue to pose **risks to critical infrastructure** as can be seen with the July 2018 incident In the U.S., when hackers gained access to the control rooms of utility companies, as well as the September 2019 drone attacks on the Saudi Aramco refineries.
- WEF Global Risks Report 2019 notes that malicious cyber-attacks and lax cyber security protocols led to massive breaches of personal information in 2018.

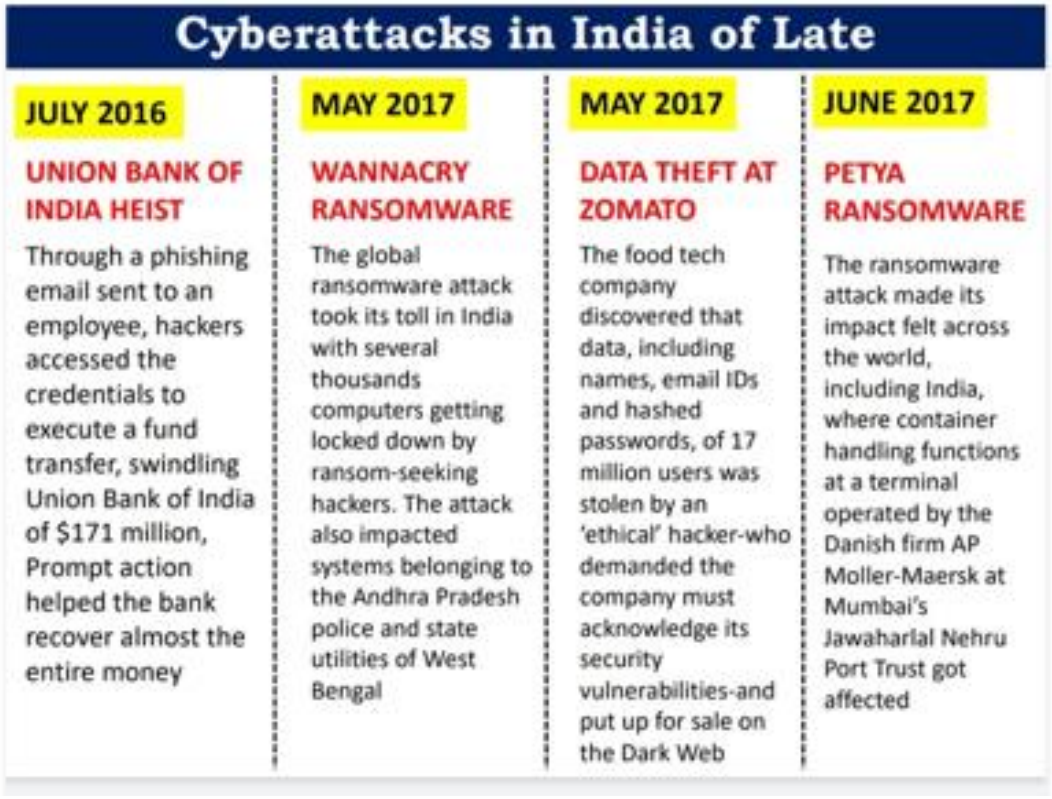
Indian Scenario:

- **Various programs of government** such as Aadhaar, MyGov, Government e-Market, DigiLocker, Bharat Net etc. prompt users to transact online.
- **Start-ups digital push**
- India the **fifth most vulnerable country in the world** in terms of cybersecurity breaches.
- India saw at least **one cybercrime every 10 minutes** during the first half of 2017 including more sophisticated cyber threats such as the WannaCry and Petya ransomware.
- India **accounted for 5.09 per cent of all cyberattacks** such as malware, spam and phishing attacks detected globally in 2017.
- The **estimated cost of cyber-attacks in India stands at four billion dollars which is expected to reach $20 billion in the next 10 years.**
- India **ranks 3rd in terms of number of internet users after USA and China**.
- India secures a spot amongst the top 10 spam-sending countries in the world alongside USA
- In February 2019, India's Ministry of Electronics and IT (MeitY) outlined **India's digital vision of unlocking the potential of a $1 trillion digital economy by 2025 from its current value of around $200 billion.** To realize this potential and build a stable digital economy, it is imperative that all government and private digital systems are safe, secure and resilient.

RECENT BREACH INCIDENTS

- CERT-In has reported a rapid increase in the number of cyber security incidents in recent years: a **steep four-fold rise of incidents** from 53,117 in 2017 to 208,456 in 2018.
- 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.

- **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**.
- **Cambridge Analytica data-mining scandal, cyber-attacks on Kudankulam Nuclear Power Project** are examples.



CHALLENGES IN ENSURING CYBER SECURITY:

- **Digital illiteracy** makes Indian citizens highly susceptible to cyber fraud, cyber theft, etc.
- In India, majority of devices used to access internet have **inadequate security infrastructure** making them susceptible to malwares
- **Rampant use of unlicensed software and underpaid licenses** also make them vulnerable.
- **Lack of adoption of new technology**
- There are variety of devices used with **non-uniform standards** which makes it difficult to provide for a uniform security protocol.
- **Import dependence** for majority of electronic devices put India into a vulnerable situation.
- There are currently around 30,000 cyber security vacancies in India but **demand far outstrips supply of people with required skills.**
- Even advanced precision threats carried out by hackers is **difficult to attribute to specific actors, state or non- state.**
- **Lack of coordination** among various agencies working for cyber security.
- **Absence of geographical barriers, majority of servers located outside India** are other factors.

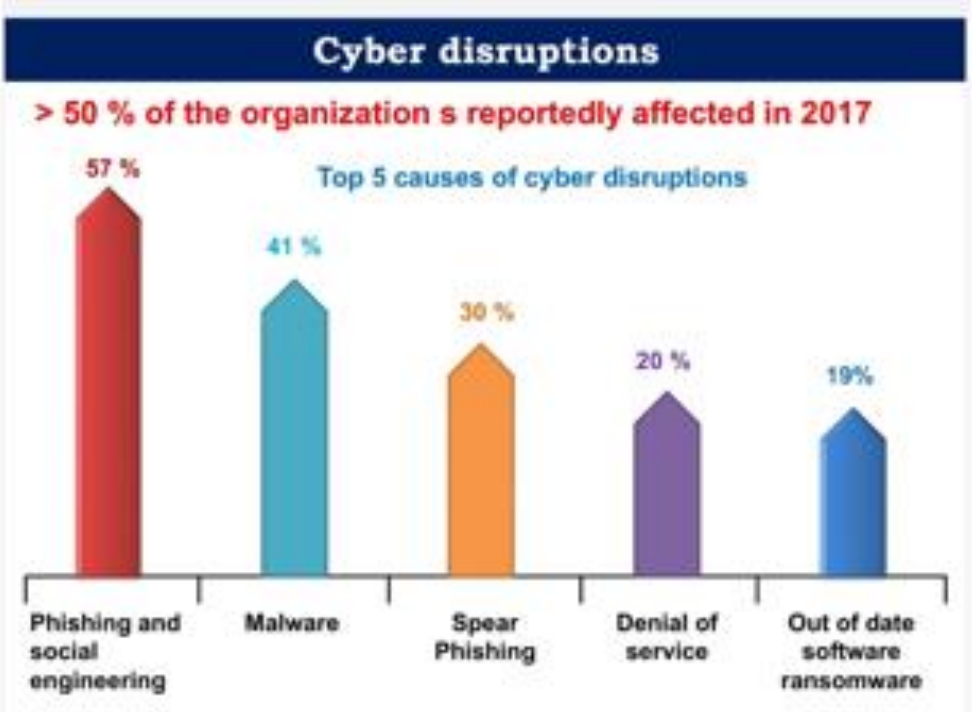
CYBER THREATS AND SOURCES

Sources

- Nation States
- Cyber Criminal Organisations
- Terrorists, DTOs, etc.
- Hackers / Hacktivists

Threats

- Malware – Malicious software to disrupt computers
- Viruses, worms
- Theft of Intellectual Property or Data
- Hactivism – Cyber protests that are socially or politically motivated
- Mobile Devices and applications and their associated Cyber Attacks
- Social Engineering – Entice Users to click on malicious links
- Spear Phishing – Deceptive Communications (e-mails, texts, tweets)
- Domain Name System (DNS) Attacks
- Router Security – Border Gateway Protocol (BGP) Hijacking
- Denial of Service (DoS) – blocking access to websites
- AI and machine learning, IoT, 5G offer number of threats



INSTITUTIONAL FRAMEWORK

Policies, Acts, Schemes

- **INFORMATION TECHNOLOGY ACT 2000** continues to be the omnibus legislation that governs cyber security policy and it includes provisions for e-governance, e-commerce, data protection, cyber offences, critical information infrastructure, interception, monitoring and cyber terrorism.
- **REGULATORY GUIDELINES** are issued by sectoral regulators such as RBI, TRAI, SEBI, IRDA for organizations under their purview.
- **NATIONAL CYBER SECURITY POLICY (NCSP) 2013** document was prepared by the Ministry of Communications and Information Technology to facilitate the creation of a secure cyberspace ecosystem and strengthen the existing regulatory frameworks.
- **CERT-In Rules 2013** outline proactive measures for protecting cyber security, including forecasts and alerts on security incidents, and the prediction and prevention of future incidents.
- The Ministry of Home Affairs developed the **NATIONAL INFORMATION SECURITY POLICY AND RELATED GUIDELINES** in 2014 for securing classified information in all government organizations.
- **Draft IoT Policy** was released) by MeiTY in 2014-15 with a view to solicit inputs from the industry and others on cyber security concerns in the IoT ecosystem.
- **DRAFT M2M (MACHINE-TO-MACHINE) TELECOM ROADMAP:** Developed by DoT, discusses cyber security issues in M2M interactions.
- **NATIONAL DIGITAL COMMUNICATIONS POLICY 2018:** outlines a focus on ensuring individual autonomy and choice, data ownership, privacy and security; while recognizing data as a crucial economic resource.

- MeitY has engaged with the Data Security Council of India for creating cybercrime awareness among law enforcement authorities through workshops at different cities across India.
- A **NATIONAL CYBER SECURITY STRATEGY 2020** is being formulated by the Office of National Cyber Security Coordinator at the National Security Council Secretariat. Aim is to improve cyber awareness and cybersecurity through more stringent audits.

Offices

- **INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-IN),** established within the Ministry of Electronics and Information Technology (MeitY), issues alerts and advisories regarding the latest cyber threats and countermeasures on a regular basis.Power sector CERTs have been created.
- PMO includes within it several cyber portfolios. Among these are the **NATIONAL SECURITY COUNCIL,** usually chaired by NSA, and NSA also chairs the **NATIONAL INFORMATION BOARD**, which is meant to be the apex body for cross-ministry coordination on cybersecurity policymaking.
- Office of the **NATIONAL CYBER SECURITY COORDINATOR** was established under the National Security Council Secretariat as the nodal agency for cyber security established for the purpose.
- **NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTER** was established for the protection of critical information infrastructure in the country, as per the provisions of section 70A of the Information Technology (IT) Act, 2000.
- **Proposed CERT-Fin**: creation of a separate CERT for the financial services sector.
- **IB-CART** at IDRBT: CERT-IN has created a Centre of Excellence (CoE) for cyber security within IDRBT in Hyderabad.
- **NATIONAL CYBER COORDINATION CENTRE** was set up to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.
- **84 SECURITY AUDITING AGENCIES** have been empaneled to support and audit implementation of Information Security Best Practices.
- The government has launched the **'CYBER SWACHHTA KENDRA'** (Botnet Cleaning and Malware Analysis Centre) that provides detection of malicious programs and free tools to remove them.

GLOBAL CYBER SECURITY NORMS AND FRAMEWORKS

- There have been multiple global forums such as **Global Commission on the Stability of Cyberspace.**
- **ITU Global Cyber Security Agenda & Global Cyber Security Index:** goal is to foster a global culture of cyber security and its integration at the core of information and communication technologies.
- **Tallinn Manual 2.0:** is an influential resource for legal frameworks around cyber issues and details four sections comprising general legal principles in the cyber domain as well as specific specialized legal regimes.
- **UN Group of Governmental Experts (UN GGE)**: comprises 20 nations equitably distributed based on geography and includes nation states regarded as leaders in cyber areas.
- The UN General Assembly adopted two resolutions on cyber, one creating a **working group to study cyber norms and possible dialogues,** and another setting up a **working group of government experts to study applicability of international law to states in cyberspace**.
- **Paris Call for Trust And Security In Cyberspace**: launched by French President in 2018, as a high-level declaration for cooperation.
- **Open Ended Working Group At UN**: developing norms of responsible state behaviour in cyber space.
- **Cyber security Tech Accord:** Around 34 global technology and security companies came together in 2018 to sign a Cyber security Tech Accord with a pledge to "protect and empower civilians online and to improve the security, stability and resilience of cyberspace."

- **Budapest convention on cybercrime:** This convention of the council of Europe is the only binding international instrument on this issue that addresses Internet and computer crime by harmonizing national laws, improving legal authorities for investigative techniques, and increasing cooperation among nations.

WAY FORWARD

- Much-needed **SYNERGY** among various institutions and work out a coordinated approach to cyber security, including cyber deterrence.
- India needs to make a proper assessment of an **OFFENSIVE CYBER DOCTRINE** adopted by many countries where they are acquiring offensive capabilities by building 'cyberweapons' to do enormous damage to the adversary's networks.
- **DOCTRINE ON CYBER CONFLICTS** that holistically captures India's approach to cyber conflict, either for conducting offensive cyber operations, or the extent and scope of countermeasures against cyber-attacks.
- Currently the average cost of a **CYBER INSURANCE** in India is around $7.5 million which in comparison to developed countries is about 20-25% lesser.
- **INVESTMENT IN IT SECURITY** has to be increased with adoption of a cybersecurity plan, purchase of cyber-insurance as well as appointment of a data security officer.
- The regulations need to keep pace with the changing cyber scenario to ensure penalties serves as deterrence for crimes.
- **SKILL DEVELOPMENT:** By 2025, the cybersecurity space is expected to generate around a million jobs in India.
- **SECURITY AUDIT** adhering to international standards may be made applicable for all govt. websites, applications before hosting and publishing.
- Establishing cybersecurity framework at state level

https://youtu.be/M15WPSw_-V8

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

https://www.thehindu.com/todays-paper/tp-opinion/patching-the-gaps-in-indias-cybersecurity/article34001731.ece

https://www.indiatoday.in/india/story/un-security-council-india-cyber-attacks-warfare-pakistan-china-1820899-2021-06-29

https://indianexpress.com/article/business/economy/security-watch-interconnected-sectors-raise-need-for-robust-cyber-defence-strategy-7211796/