



RACE IAS

GLOBAL CYBERSECURITY INDEX

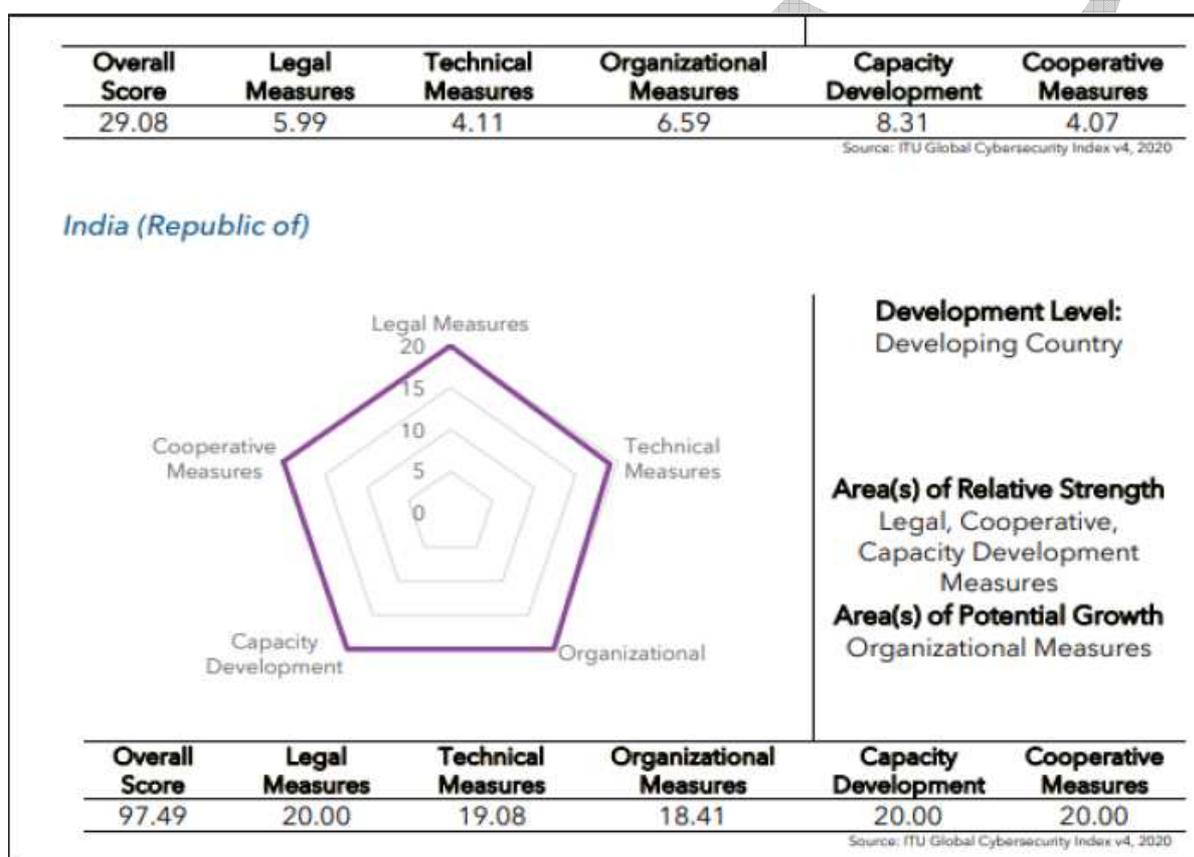
- **About:** The Global Cybersecurity Index (GCI) is a multi-stakeholder initiative to raise cybersecurity awareness and to measure the commitment of countries to cybersecurity and its wide field of application cutting across industries and sectors.
- **Published by:** The International Telecommunication Union (ITU)
- **Global Cybersecurity Index (GCI) 2020:** The Index maps 82 questions on Member State cybersecurity commitments across five pillars:
 - legal measures;
 - technical measures;
 - organizational measures;
 - capacity development measures;
 - cooperation measures
- **Assessment:** The performance is then aggregated into an overall score.
- **Significance:** To help create a trusted and safe cyberspace in the aftermath of the pandemic, the GCI can be a jumping point to understand how the pandemic has impacted cybersecurity efforts, and how countries are working to address cybersecurity and trust.
- **India's rank:** India has made it to the top 10 moving up 37 places to rank as the tenth best country in the world on key cyber-safety parameters.
- **Top ranking:** The US topped first, followed by the United Kingdom and Saudi Arabia tied on the second

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10

position together. Estonia was ranked third in the index.

India's Position:

- India has also secured the fourth position in the Asia Pacific region, underlining its commitment to cybersecurity.
- India scored a total of 97.5 points from a possible maximum of 100 points, to make it to the tenth position worldwide in the GCI 2020.
- Over the last few years, India has performed persistently on all the five pillars, resulting in substantial expansion in its ranking in Global Cyber Security Index.
- India is emerging as a global IT superpower, asserting its digital sovereignty with firm measures to safeguard data privacy and the online rights of citizens.



About ITU:

- The International Telecommunication Union (ITU) is the United Nations specialized agency for information and communication technologies - ICTs. Founded in 1865 to facilitate international connectivity in communications networks.
- The ITU promotes the shared global use of the radio spectrum, facilitates

international cooperation in assigning satellite orbits, assists in developing and coordinating worldwide technical standards, and works to improve telecommunication infrastructure in the developing world.

- It is also active in the areas of broadband Internet, wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, TV broadcasting, amateur radio, and next-generation networks.
- ITU is committed to connecting all the world's people - wherever they live and whatever their means.
- Based in Geneva, Switzerland, the ITU's global membership includes 193 countries and around 900 business, academic institutions, and international and regional organizations.
- ITU is a unique platform for global public-private partnerships

The Current State of Cyber Security in India:

- Around 82% Indian companies suffered a ransomware attack in 2020.
- Also, the cost of recovering from the impact of a ransomware attack in India tripled over the last year, going up from \$1.1 million in 2020 to \$3.38 million in 2021.
- As per the government data presented in the parliament, nearly 1.16 million cases of cyber-attacks in India were reported in 2020, marking an average of 3,137 cyber security issues reported every day of the year.
- An article by Inc42 revealed that ever since the arrival of the COVID-19 pandemic, India has witnessed a 4000% increase in phishing emails and a 400% spike in the number of policy violations.
- 66% of organizations in India have suffered at least one data breach or cyber-attack since shifting to a remote working model during the pandemic.
- The Internet Crime Report by the FBI revealed that India is ranked third in the world among the top 20 countries being victimized by cyber-crimes.

Challenges of Cyber Security in India:

- **Lack of uniformity in devices used for internet access:** With varying income groups in India, not everyone can afford expensive phones. In the US, Apple has over 44% market share. However, in India the iPhones with their higher security norms are used by less than 1% of mobile users.

- **Lack of national level architecture for Cybersecurity:** There is no national security architecture that unifies the efforts of all the agencies to be able to assess the nature of any threat and tackle them effectively.
- **Lack of awareness:** As there is no National regulatory policy in place for cybersecurity there is a lack of awareness at both company level as well as individual level. India doesn't have an 'active cyber defense' like the EU's General Data Protection Regulation (GDPR) or the US' Clarifying Lawful Overseas Use of Data (CLOUD) Act.

Suggestions to improve Cyber Security in India:

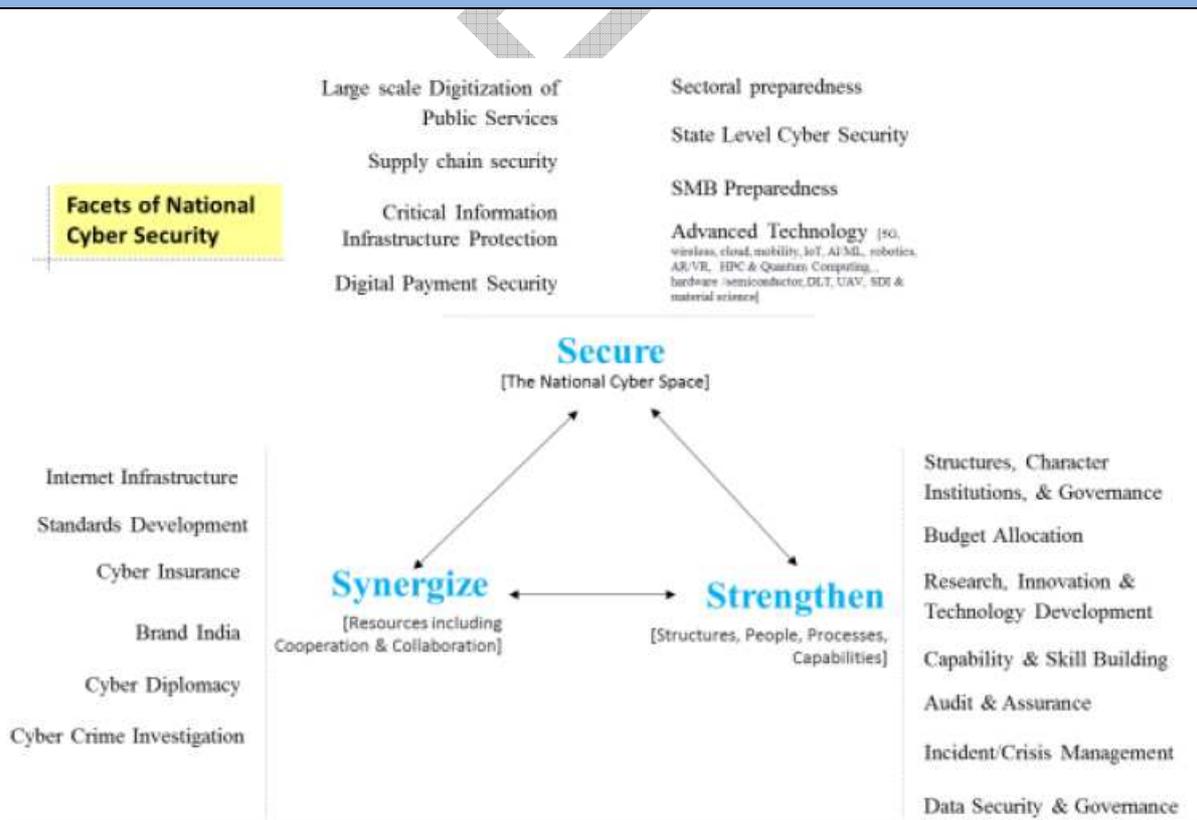
- With India's highly skilled IT workforce, efforts must be harnessed and redirected towards strategic use by the government.
- Incentives provided by the government to the industry would encourage investment from the private sector towards an agency focused on national cybersecurity.
- With strengthened cybersecurity defenses in India's future, Indian businesses will become more competitive on a global level and create a safer digital India.
- There is a need for a robust cybersecurity policy for the country. The first step would be to identify critical infrastructure, followed by an assessment of threats and vulnerabilities and finally an action plan to counter these.
- In the UK, the National Cyber Security Programme (NCSP) with dedicated funding of £860 million over five years ensures critical UK systems and networks are robust and resilient, improves cyber awareness and risk management amongst UK business, ensure members of the public know what they can do to protect themselves. The same can be replicated in India too.
- Incentivization contributions to for developing cybersecurity technology, development of training infrastructure, investing in the testing labs, active participation in technology standards making, demonstration of India's capabilities in the global market, and for improving preparedness of SMB sector.
- Critical infrastructure protection demands fixing the structural problem by empowering security leadership and strengthening security in both IT and OT environment.
- Bootstrap the Cyber Security Capability building program in states through central funding on lines of eGov.

National Cyber Security Strategy 2020:

- India was one of the first few countries to propound a futuristic National Cyber Security Policy 2013(NCSP 2013).
- The Indian Government under the aegis of National Security Council Secretariat through a well-represented Task Force is in the process of formulating the National Cyber Security Strategy 2020 (NCSS 2020) to cater for a time horizon of five years (2020-25).
- Vision is to ensure a safe, secure, trusted, resilient and vibrant cyber space for Nation's prosperity.

National Cyber Crime Reporting Portal:

- This portal is an initiative of Government of India to facilitate victims/complainants to report cyber-crime complaints online. This portal caters to complaints pertaining to cyber-crimes only with special focus on cyber-crimes against women and children.



Way ahead:

- India is the second-fastest digital adapter among 17 of the most-digital economies globally, and rapid digitization does require forward-looking measures to boost cybersecurity. The Government of India is working towards updating its National Cybersecurity strategy in order to improve its position in the cyber space. While India has come a long way since it launched its policy in 2013, there are many new challenges that have emerged due to technology advancement.

RACE IAS