Global Cybersecurity Outlook 2025

For Prelims: **World Economic Forum (WEF)**, Global Cybersecurity Outlook 2025, **Cybercrime**, **Information Technology Act, 2000**, **Digital Personal Data Protection Act, 2023**, **Indian Computer Emergency Response Team**, **National Critical Information Infrastructure Protection Centre** , **Bharat National Cybersecurity Exercise 2024**, **Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024**, **Budapest Convention on Cybercrime**.

For Mains: Key Highlights of Global Cybersecurity Outlook 2025 report, Current Framework for Cyber Security, Key Emerging Cyber Threats, Way Forward.

Source: DTE

Why in News?

The **World Economic Forum (WEF)** has recently released the **Global Cybersecurity Outlook 2025 report**.

- The report highlights **rising cyber threats to critical infrastructure**, driven by **geopolitical tensions, outdated systems, and a cybersecurity skills gap,** stressing the need for enhanced security and resilience.

World Economic Forum (WEF)

- **About:** The **WEF** is an international organization for public-private cooperation, engaging global leaders from politics, business, culture, and other sectors to **shape agendas at global, regional, and industry levels**.
- **Headquarters:** Geneva, Switzerland.
- **Foundation:** Established in **1971** by **Klaus Schwab,** a German professor. Initially named the **European Management Forum.**

Note:

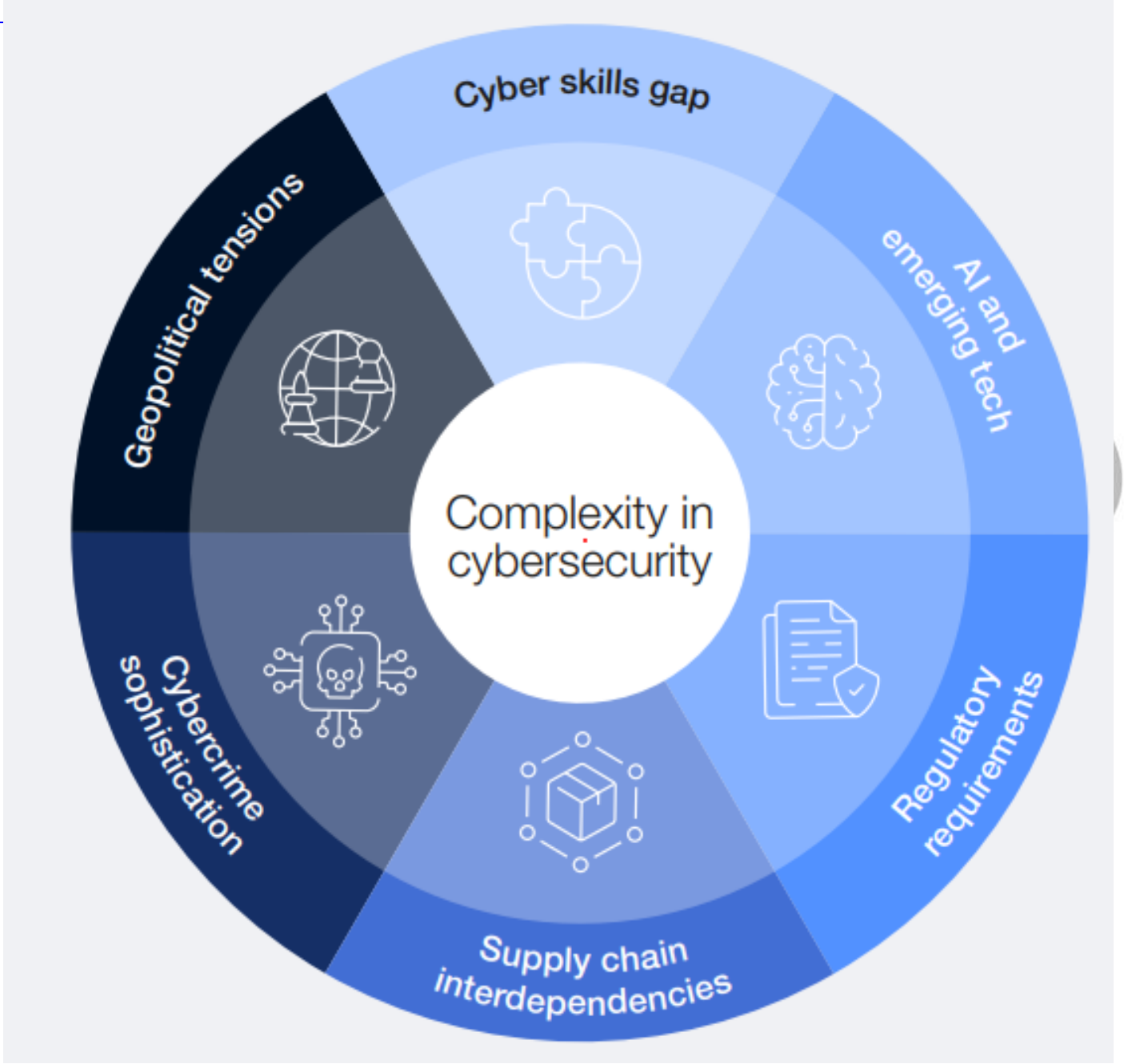
- The index, named **Global Cybersecurity Index (GCI)** , is published by the **International Telecommunication Union (ITU)** to assess and rank countries based on their **commitment to cybersecurity.**
- **India** has achieved a major milestone in cybersecurity by securing **Tier 1 status in the 5th edition of GCI 2024.**

What are the Key Issues Highlighted in Global Cybersecurity Outlook 2025?

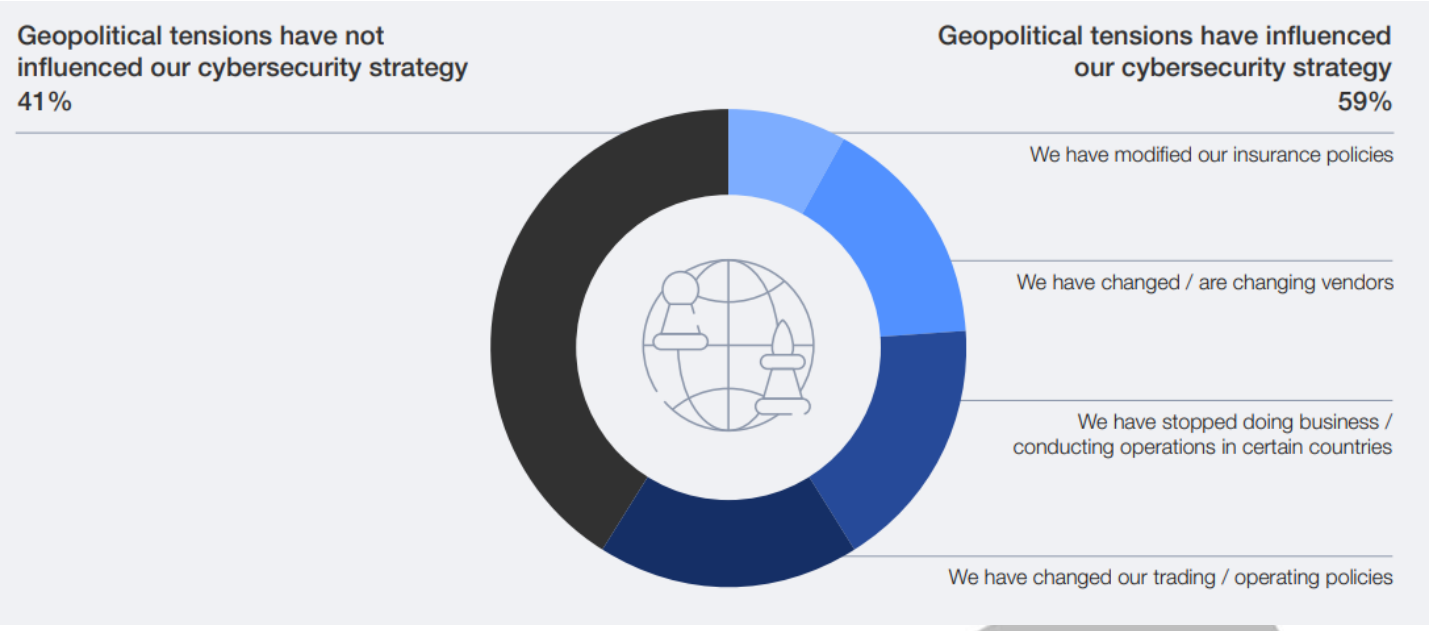
- **Vulnerability of Critical Infrastructure:** Critical infrastructure sectors like **water, biosecurity,**

communications, energy, and **climate** are vulnerable to **cyberattacks** due to **outdated technologies and interconnected systems.**
    - Cybercriminals and state actors **target operational technology,** including **undersea cables**, risking global data flow.
    - In 2024 there was a **sharp increase in phishing and social engineering attacks,** with 42% of organizations reporting such incidents.
    - **Example:** A **2024 cyberattack on a US water utility** disrupted operations, highlighting vulnerabilities in water treatment facilities.

//



- **Geopolitical Tensions:** Geopolitical conflicts, like the **Russia-Ukraine war,** have **heightened cyber and physical attacks on critical sectors** such as energy, telecommunications, and water.
    - Nearly **60% of organizations** state that **geopolitical tensions have affected their cybersecurity strategy.**

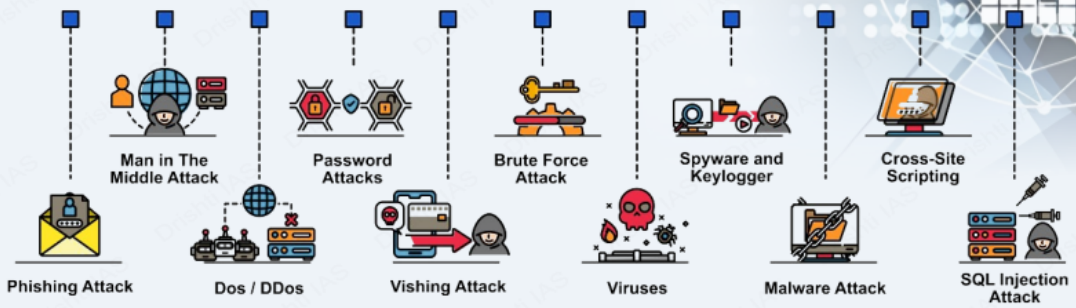


- **Biosecurity Threats:** Advancements in **Artificial intelligence (AI)**, **genetic engineering,** and **biotechnology** have **heightened biosecurity risks**, with cyberattacks on bio-laboratories **threatening research and safety protocols.**
  - The **World Health Organization (WHO)** has warned of these dangers, as seen in **2024 attacks on labs in South Africa and the UK**.
- **Cybersecurity Skills Gap:** The report highlights a **critical cybersecurity skills gap**, with a **shortage of up to 4.8 million professionals globally**.
  - Two-thirds of organizations face notable skills gaps, with **only 14% having the required skilled personnel** for the current cyber landscape.
- **Cyber Resilience: 35% of small organizations** feel their **cyber resilience is insufficient.**
  - **Public-sector organizations** face greater challenges, with **38% reporting low resilience** and 49% lacking cybersecurity talent, a 33% rise from 2024.
- **Regional Cybersecurity Disparities:**
  - The report highlights global cybersecurity disparities, with low confidence in **incident response rising from 15% in Europe/North America to 36% in Africa and 42% in Latin America.**
- **Losses Due to Cybercrime:** Cybercrime has become a **highly profitable venture,** with minimal operational costs and potentially high returns.
  - The **US Federal Bureau of Investigation (FBI)** estimates losses from cybercrime exceeded **USD 12.5 billion in 2023.**

CYBER SECURITY

Cybersecurity refers to any technology, measure, or practice for preventing cyberattacks or mitigating their impact.

CYBER SECURITY ATTACKS



'Crime in India' Report 2022 (NCRB) highlighted 24.4% surge in cybercrimes in India since 2021.

Common Cybersecurity Myths

- Strong passwords alone are adequate protection
- Major cybersecurity risks are well-known
- All cyberattack vectors are contained
- Cybercriminals don't attack small businesses

Cyber Warfare

- Digital attacks to disrupt vital computer systems, to inflict damage, death, and destruction.

CYBER THREAT ACTORS

CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

Types of Cybersecurity

- Critical infrastructure security (Robust access controls)
- Network security (Deploying firewalls)
- Application security (Code reviews)
- Cloud Security (Tokenization)
- Information security (Data masking)

Recent Major Cyber Attacks

- WannaCry Ransomware Attack (2017)
- Cambridge Analytica Data Breach (2018)
- Financial data of 9M+ cardholders, including SBI, leaked (2022)

Regulations & Initiatives

- **International:**
  - UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace
  - NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE)
  - Budapest Convention on Cybercrime, 2001 **(India not a signatory)**
- **India:**
  - IT Act, 2000 (Sections 43, 66, 66B, 66C, 66D)
  - National Cyber Security Policy, 2013
  - National Cyber Security Strategy 2020
  - Cyber Surakshit Bharat Initiative
  - Indian Cyber Crime Coordination Centre (I4C)
  - Computer Emergency Response Team-India (CERT-In)

Steps Needed for Cyber Security

- Network Security
- Malware Protection
- Incident Management
- User Education and Awareness
- Secure Configuration
- Managing User Privileges
- Information Risk Management Regime

Drishti IAS

Way Forward

- **Strategic Investment in Cybersecurity:** The **Global Cybersecurity Outlook 2025** calls for **strategic investment in cybersecurity,** urging governments to **modernize legacy systems, upgrade operational technologies,** and **protect critical sectors** like water, energy,

and biosecurity from rising threats.
    - The **2022 cyberattacks on Costa Rica** highlighted the need to **view cybersecurity as a critical investment** for the future, **not just an expense.**
    - **Balancing investments in cybersecurity with competing business priorities** is critical.
- **Public-Private Collaboration: Public-private collaboration** is vital for **sharing threat intelligence, developing secure technologies**, and enhancing cybersecurity resilience.
    - Also, Small and medium enterprises (SMEs) may find it challenging to invest in cybersecurity without strong government incentives.
- **Investing in Cybersecurity Skills:** There is a need for **expanding specialized training programs,** offering certifications, and **incentivizing workforce development** to build a skilled talent pool to counter evolving **cyber threats.**
- **Focus on Resilience over Prevention**: With evolving cyber threats, nations must **prioritize resilience by enhancing rapid response mechanisms,** establishing **crisis** management frameworks, and ensuring continuity of essential services during attacks.
- **International Cooperation:** To address borderless cyber threats, nations must **collaborate through forums like the United Nations (UN) and G20** to establish cybersecurity standards, while **developed nations should assist emerging economies** in strengthening their cybersecurity frameworks and resilience against cyberattacks.

What is the Current Framework for Cybersecurity in India?

- **Legislative Measures:**
    - **Information Technology Act, 2000 (IT Act)**
    - **Digital Personal Data Protection Act, 2023**
- **Institutional Framework:**
    - **Indian Computer Emergency Response Team (CERT-In)**
    - **National Critical Information Infrastructure Protection Centre (NCIIPC)**
    - **Indian Cyber Crime Coordination Centre (I4C)**
    - **Cyber Swachhta Kendra**
- **Strategic Initiatives:**
    - **Bharat National Cybersecurity Exercise 2024**
    - **National Cyber Security Policy, 2013:** Provides vision and strategies for securing cyberspace and protecting critical information infrastructure.
- **Sector-Specific Regulations:**
    - **Cybersecurity Framework for SEBI Regulated Entities:** Mandates cybersecurity policies for securities markets.
    - **Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024**

Conclusion

The Global Cybersecurity Outlook 2025 highlights rising cyber threats to critical infrastructure, emphasizing the need for strategic investments, international cooperation, and robust cybersecurity frameworks. As cyber threats evolve, nations must prioritise protecting critical infrastructure to ensure national security, public safety, and economic stability.

Drishti Mains Questions:

Discuss the key cybersecurity challenges India faces in the digital age and suggest measures to enhance its cybersecurity framework for protecting critical infrastructure.

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims

Q.1 In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one's computer
2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialised consultant to minimise the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only

(b) 1, 3 and 4 only

(c) 2 and 3 only

(d) 1, 2, 3 and 4

Ans: (b)

Q.2 In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only

(b) 1 and 2 only

(c) 3 only

(d) 1, 2 and 3

Ans: (d)

Mains

Q. What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**