National Cyber Security Strategy

For Prelims: Data Security Council of India (DSCI), Government Initiatives for Cyber Security, Indian Computer Emergency Response Team (CERT-In), Related Initiatives

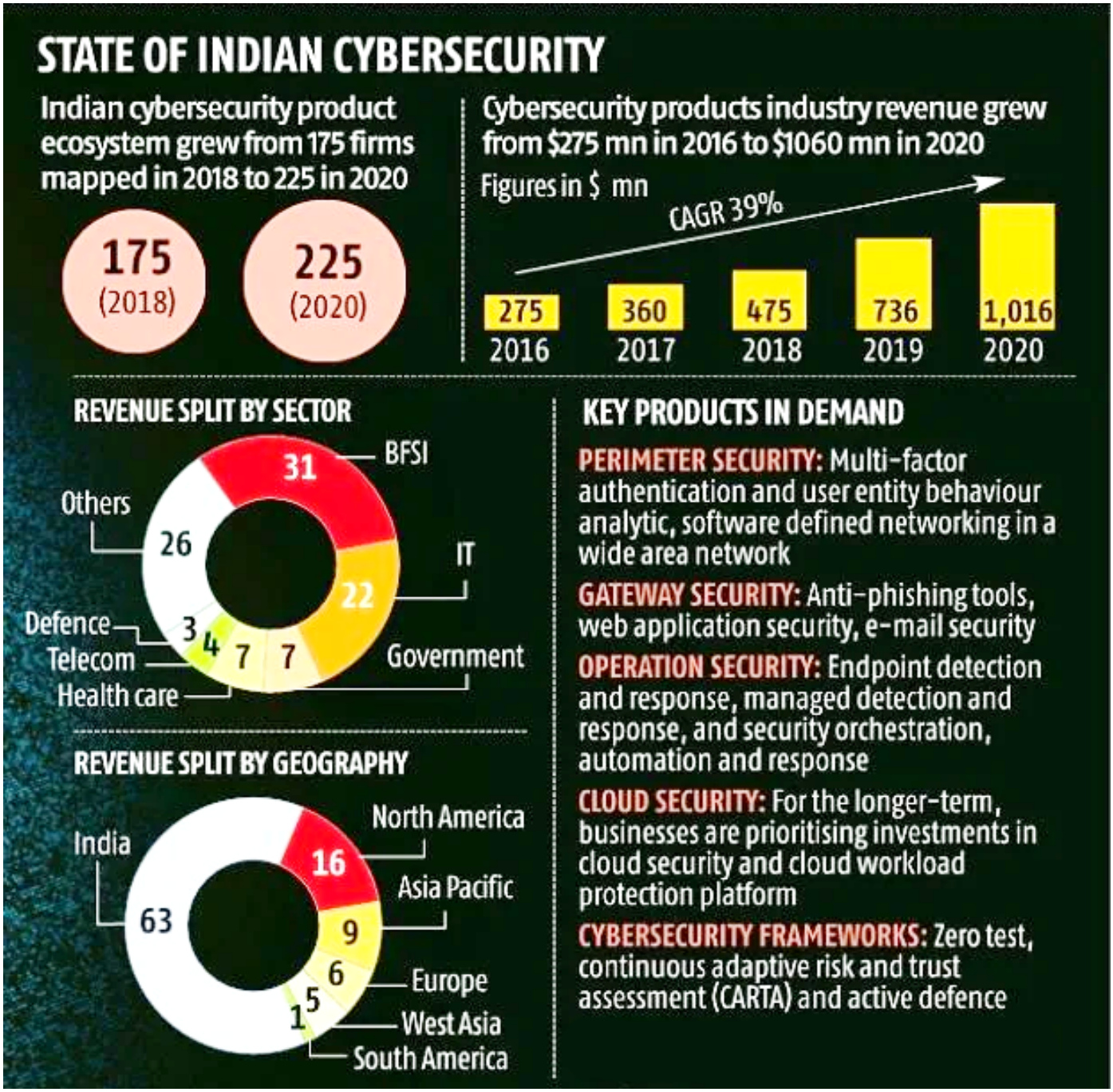
For Mains: Challenges to Internal Security Through Communication Networks, National Cyber Security Strategy, Cyber Security

Why in News?

In 2020, the **National Cyber Security Strategy** was conceptualised by the **Data Security Council of India (DSCI)** headed by **Lt General Rajesh Pant.** The report focused on 21 areas to ensure a safe, secure, trusted, resilient, and vibrant cyberspace for India.

- However, amid a surge in cyberattacks **on India's networks**, the Centre is yet to implement the **National Cyber Security Strategy.**

//



What is the Need for a National Cyber Security Strategy?

- **Increasing Number Of Cyber Attacks:** As per **American cybersecurity firm Palo Alto Networks' 2021 report, Maharashtra** was the **most targeted state in India** — facing 42% of all ransomware attacks.
    - The report stated that India is among the more **economically profitable regions for hacker groups** and hence these hackers ask Indian firms to pay a ransom, usually using cryptocurrencies, in order to regain access to the data.
    - **One in four Indian organisations suffered a ransomware attack in 2021 —** higher the the global average of 21%.
- **Cyber Warfare Offensives:**
    - The **US** is just one of many countries that have invested significant amounts of money in developing not just defences against attack, but the ability to mount **damaging cyber warfare offensives.**
    - The countries which are believed to have the most developed cyber warfare capabilities are the **US, 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.
- **For Protecting Critical Sectors:**
  - It is particularly significant given the increasing interconnectedness of sectors and proliferation of entry points into the internet, which could further grow with the **adoption of** 5G**.**
  - There were **6.97 lakh cyber security incidents** reported in the first eight months of 2020, nearly equivalent to the previous four years combined, according to information reported to and tracked by the **Indian Computer Emergency Response Team (CERT-In).**
- **Recent Cyber Attacks:**
  - 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.**
  - Red Echo used malware called **ShadowPad, which involves the use of a backdoor to access servers.**
  - The 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.
- **For Government:**
  - A local, state or central government maintains a huge amount of confidential data related to the **country (geographical, military-strategic assets etc.)** and citizens.
- **For Individuals:**
  - Photos, videos and other personal information shared by an individual on social networking sites can be inappropriately used by others, leading to serious and even life-threatening incidents.
- **For Businesses:**
  - Companies have a lot of data and information on their systems.
  - A cyber attack may lead to loss of **competitive information** (such as patents or original work), and loss of employees/customers' private data resulting in complete loss of public trust in the integrity of the organisation.

What are the Main Components of the National Cyber Security Strategy?

- **Large Scale Digitisation of Public Services:** Focus on security in the early stages of design in all digitisation initiatives.
  - **Developing institutional capability** for assessment, evaluation, certification, and rating of the core devices
  - Timely reporting of vulnerabilities and incidents.
- **Supply Chain Security:** Monitoring and mapping of the supply chain of the **Integrated Circuits (ICT)** and electronics products.
  - Leveraging the country's **semiconductor** design capabilities globally at strategic, tactical and technical levels.
- **Critical Information Infrastructure Protection:** Integrating **Supervisory Control And Data Acquisition (SCADA)** security
  - Maintaining a repository of vulnerabilities.
  - Preparing an aggregate level **security baseline of the sector** and tracking its controls.
  - Devising **audit parameters for threat preparedness** and developing cyber-insurance products.
- **Digital Payments:** Mapping and modelling of devices and platforms deployed, supply chain, transacting entities, payment flows, **interfaces and data exchange.**
- **State-Level Cyber Security:** Developing state-level cybersecurity policies,
  - Allocation of dedicated funds,
  - Critical scrutiny of digitization plans,
  - Guidelines for security architecture, operations, and governance.
- **Security of Small And Medium Businesses:** Policy intervention in cybersecurity granting incentives for a higher level of cybersecurity preparedness.
  - Developing security standards, frameworks, and architectures for the adoption of the **Internet of Things (IoT)** and **industrialisation.**

What steps does the report suggest?

- **Budgetary Provisions:** A minimum allocation of **0.25% of the annual** budget, which can be **raised upto 1%** has been recommended to be set aside for cyber security.
    - In terms of separate ministries and agencies, **15-20% of the IT/technology expenditure should be earmarked for cybersecurity.**
    - It also suggests setting up a **Fund of Funds for cybersecurity** and providing Central funding to States to build capabilities in the same field.
- **Research, Innovation, Skill-Building And Technology Development:** The report suggests investing in modernisation and **digitisation of ICT,** setting up a short and long term agenda for cyber security via outcome-based programs and providing investments in deep-tech **cyber security innovation.**
    - DSCI further recommends creating a **'cyber security services'** with cadres chosen from the **Indian Engineering Services.**
- **Crisis Management:** For adequate preparation to handle a crisis, DSCI recommends **holding cybersecurity drills** which include real-life scenarios with their ramifications.
- **Cyber Insurance:** Cyber insurance being a yet to be researched field, must have an actuarial science to **address cybersecurity risks in business and technology** scenarios as well as calculate threat exposures.
- **Cyber Diplomacy:** Cyber diplomacy plays a huge role in **shaping India's global relations**. Hence cyber security preparedness of key regional blocks like **Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC)** and **Shanghai Cooperation Organisation (SCO)** must be ensured via programs, exchanges and industrial support.
    - To further better diplomacy, the government should promote brand India as a responsible player in cyber security and also create **'Cyber envoys'** for the key countries/regions
- **Cybercrime Investigation:** With the increase in cybercrime across the world, the report recommends unburdening the judicial system by creating laws to resolve spamming and fake news.
    - It also suggests charting a **5-year roadmap factoring possible technology** transformation, setting up exclusive courts to deal with cybercrimes and removing the backlog of cybercrime.
    - Moreover, DSCI suggests advanced forensic training for agencies to keep up in the age of AI/ML, **Blockchain,** IoT, Cloud, Automation.

What are Present Government Initiatives for Cyber Security?

- **Cyber Surakshit Bharat Initiative.**
- **Cyber Swachhta Kendra.**
- **Online cybercrime reporting portal.**
- **Indian Cyber Crime Coordination Centre (I4C).**
- **National Critical Information Infrastructure Protection Centre (NCIIPC).**
- **Information Technology Act, 2000.**

UPSC Civil Services Examination, Previous Year Questions (PYQs)

Q. The terms 'WannaCry, Petya and EternalBlue' sometimes mentioned in the news recently are related to (2018)

(a) Exoplanets
(b) Cryptocurrency
(c) Cyber attacks
(d) Mini satellites

Ans: (c)

- Ransomware is a form of malicious software (or malware). Once it takes over the computer, it threatens users with harm, usually by denying access to data. The attacker demands a ransom from the victim, promising to restore access to the data upon payment.
- WannaCry, Petya and EternalBlue are a few of the ransom ware, which created havoc by demanding the victim ransom payment in bitcoin **(cryptocurrency)**.

Source: TH