State-Sponsored Cyber Attacks

For Prelims: State-Sponsored Attacks, **Pegasus Project**, Cyber Attack, Privacy Violations, Indian Cyber Crime Coordination Centre (I4C), Cyber Security.

For Mains: Pegasus Project and Need for Surveillance Reforms, Government policies and interventions for development in various sectors and issues arising out of their design and implementation.

Source: TH

Why in news?

Recently, Apple Inc. has sent notification to individuals, including opposition leaders and journalists, about "State-Sponsored Attackers who are remotely **trying to compromise" their iPhones.**

- This is the second time that Opposition politicians and civil society actors in India have been warned that they **have been targets of spying attempts.**
- In 2021, the Paris-based Forbidden Stories collective reported that the **Pegasus spyware**, which was sold only to government agencies by an Israeli firm NSO Group, was allegedly used on a range of journalists, civil society groups and politicians in India.

Note

A **cyber attack** is a malicious and deliberate attempt to breach the security of computer systems, networks, or digital devices, with the intent of stealing, damaging, altering, or accessing sensitive data, disrupting operations, or causing harm in the digital realm.

What are State-Sponsored Cyber Attacks?

- **About:**
  - State-sponsored cyber attacks, also known as nation-state cyber attacks are cyberattacks **conducted or supported by governments or government agencies** against other nations, organizations, or individuals.
  - These attacks are characterized by their **high level of sophistication, organization, and resources,** as they are backed by the extensive capabilities and funding of a nation-state.
  - Examples of state-sponsored cyberattacks include the Stuxnet worm, which targeted Iran's nuclear program, the alleged **Russian interference in the 2016 U.S. presidential election,** and the 2017 WannaCry ransomware attack, which was linked to North Korea.
- **Implications on National Security:**
  - **Data Theft:** State-sponsored attacks can lead to the theft of sensitive national security information, military secrets, and **critical infrastructure data.** Such breaches can

compromise a nation's defense capabilities.
    - **Economic Impact:** Attacks on key industries and critical infrastructure can result in economic losses. For instance, the disruption of energy or financial systems can have severe economic consequences.
    - **Political Influence**: Cyberattacks can be used to manipulate public opinion, influence elections, and undermine political stability. Disinformation campaigns and hacking can have far-reaching political implications.
    - **National Sovereignty:** Cyberattacks can infringe upon a nation's sovereignty and compromise its ability to govern and protect its citizens.

What is Pegasus?

- **About:**
    - It is a **type of malicious software** or malware classified as a spyware.
        - It is designed to gain access to devices, without the knowledge of users, and gather personal information and relay it back to whoever it is that is using the software to spy.
    - Pegasus has been developed by the **Israeli firm NSO Group that was set up in 2010.**
        - Pegasus infections can be achieved through so-called **“zero-click” attacks** by exploiting flaws in operating system, which do not require any interaction from the phone’s owner in order to succeed.
- **Target:**
    - Human **Rights activists, journalists and lawyers around the world** have been targeted with phone malware sold to authoritarian governments by an Israeli surveillance firm.
    - Indian ministers, government officials and opposition leaders also figure in the list of people whose phones may have been compromised by the spyware.
        - In 2019, **WhatsApp filed a lawsuit** in the US court against Israel's NSO Group, alleging that the firm was incorporating **cyber-attacks** on the application by infecting mobile devices with malicious software.

What are the Initiatives to Foster Cyber Security?

- **Indian:**
    - **Cyber Surakshit Bharat Initiative**
    - **National Cyber security Coordination Centre (NCCC).**
    - **Cyber Swachhta Kendra**
    - **Indian Cyber Crime Coordination Centre (I4C)**
    - **Computer Emergency Response Team - India (CERT-IN)**
- **International Mechanisms:**
    - **International Telecommunication Union (ITU)**
    - **Budapest Convention on Cybercrime**

Way Forward

- There is a need to develop and implement comprehensive national cybersecurity policies and strategies that address **both defense and offense in the cyber domain.**
- Allocate resources to bolster cybersecurity infrastructure, including advanced intrusion detection systems, secure networks, and cybersecurity training for government agencies.
- Collaborate with other nations and international organizations to share threat intelligence and coordinate responses to state-sponsored threats.

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)**