Pegasus Spyware and Surveillance Concerns

For Prelims: Pegasus Spyware, Spyware, Zero-Day Vulnerability, Phishing, RTI, Indian Telegraph Act, 1885, Indian Telegraph Rules, 2007, IT Act, 2000, Interception Rules, 2009, Right to privacy, Article 21, KS Puttaswamy Case, 2017, Right to Freedom of Speech and Expression, Parliamentary Oversight, Articles 32 and 226, Supreme Court, Digital Personal Data Protection Act, 2023, End-to-End Encryption.

For Mains: Spyware and Privacy Concerns, Cyber Attacks.

Source: IE

Why in News?

The **Pegasus spyware** has stirred controversy worldwide, including India, over its **misuse for surveillance**, raising serious **privacy and fundamental rights concerns**.

- Recently, a US court ruled that **Pegasus spyware** violated the **Computer Fraud and Abuse Act, 1986** by surveilling 1,400 WhatsApp users, including **300 from India.**

What is Pegasus Spyware?

- **About:**
  - **Pegasus** is a spyware developed by **NSO Group**, an Israeli cybersecurity firm founded in **2010.** It is capable of **hacking iOS and Android** devices to extract data, record conversations, capture photos, and access app data.
  - Spyware is a **malicious software** that secretly **monitors and collects information** from a device **without the user's consent.**
- **Features:**
  - **Advanced Exploitation**: It uses zero-day vulnerabilities to jailbreak iOS devices remotely while the Android version uses software like **Framaroot** for rooting devices.
    - A zero-day vulnerability is an **undiscovered security flaw** in software with **no available defense or patch.**
    - Rooting is the process of **unlocking or jailbreaking** a device, such as a smartphone or tablet to **gain administrative control**.
  - **Invisibility**: It operates **covertly**, with **no visible signs** except for the browser closing after clicking a phishing **link**.
- **Pegasus Clients and Related Controversy:**
  - As per the NSO Group, the use of **Pegasus is limited to governments** around the world.
  - Pegasus is **controversial** because, although meant to **fight terrorism and crime**, it has been used by governments to **spy on journalists, opposition leaders, activists, and critics**.

How Pegasus was Used in India?

- **Pegasus Project**: A global collaborative investigation reported that over **300 verified Indian mobile numbers** were targeted using Pegasus spyware developed by the Israeli NSO Group.
    - It targeted **ministers, opposition leaders, journalists, lawyers, businessmen, scientists, rights activists, and government officials.**
- **Amnesty International Research:** Amnesty International's **Security Lab** confirmed that Pegasus was used to **target 37 phones, of which 10 belonged to Indians**.
- **Bhima Koregaon Case:** In 2019, Pegasus was allegedly used against **lawyers and activists** associated with the **Bhima Koregaon case** and Dalit rights movements in Maharashtra and Chhattisgarh.
- **RTI Response:** In response to an **RTI** request in **2013**, the Central Government disclosed **issuing 7,500 to 9,000 telephone interception** orders monthly.
    - However, **RTI requests** for such information are **now denied** citing threats to national security and to the physical safety of persons.
- **WhatsApp Allegations:** WhatsApp alleged that between April 2018 and May 2020, the NSO Group had **reverse-engineered and decompiled** its source code to create installation vectors (points of entry) named **"Heaven", "Eden" and, "Erised"**—all part of a sophisticated hacking suite called **"Hummingbird"** that NSO Group sold to its government clients.

What is India's Legal Framework for Surveillance and Data Protection?

- **Telecommunications Act, 2023**: Section 20(2) of the **Telecommunications Act, 2023** empowers the Centre or states to **temporarily take control of telecom services or networks** during public emergencies, **disasters, or for public safety.**
    - However, **Rule 419(A) of the Indian Telegraph Rules, 2007** mandates government authorization for lawful communication interception.
- **Information Technology (IT) Act, 2000**: Section 69 of the **IT Act, 2000** and the **Interception Rules, 2009** allow the government to **monitor, intercept, or decrypt** any information through a computer resource.
- **Digital Personal Data Protection (DPDP) Act, 2023: DPDP Act, 2023** is a comprehensive **privacy and data protection law** that includes provisions regarding **consent, legitimate uses, breaches, data fiduciary** and processor responsibilities, and **individuals' rights over their data.**

What are the Concerns Surrounding Surveillance in India?

- **Impact on Fundamental Rights**: Surveillance directly infringes on the **right to privacy** under **Article 21** of the Constitution, as recognized in the **KS Puttaswamy Case, 2017.**
    - The mere existence of surveillance systems to **monitor citizens' activities** discourages free speech under **Article 19(1)(a)**.
        - According to **Article 19(1)(a),** all citizens shall have the **right to freedom of speech and expression** which is subject to be curtailed under certain conditions but are **frequently denied** in the name of undermining **sovereignty and integrity** of India or **public order.**
- **Lack of Transparency**: Surveillance is conducted covertly with **no judicial or parliamentary oversight**.
    - The **executive holds disproportionate power**, undermining the principle of **separation of powers** enshrined in the Constitution.
- **Inability to Approach Court**: Individuals subjected to surveillance are **not able to approach courts** or raise their complaints since they themselves are **unaware of such surveillances.**
    - This undermines **Articles 32 and 226**, which empower citizens to **seek remedies** for the enforcement of their **fundamental and other rights**.
- **Executive Overreach:** Reports of the surveillance of **constitutional functionaries**, such as sitting **Supreme Court** judges, highlight the absence of safeguards against executive overreach.
- **Suppressing Free Expression**: The fear of surveillance **stifles open discussions, creativity, and dissent**, which are essential for a vibrant democracy.

Way Forward

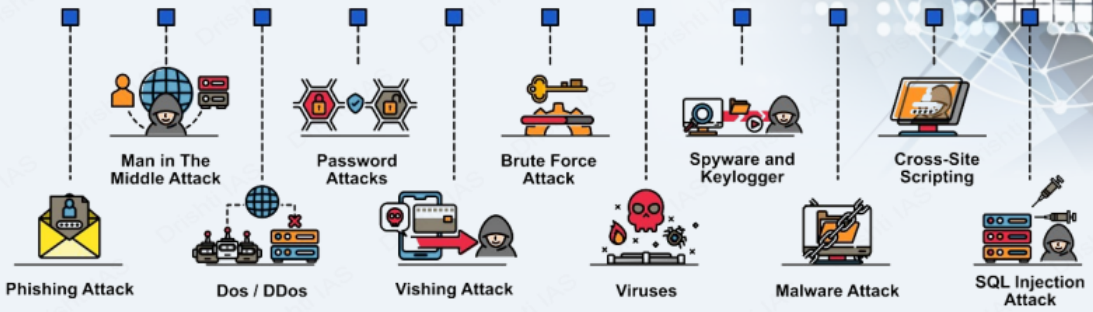
- **Judicial Oversight:** It is critical to introduce **judicial oversight** for surveillance activities. Courts should be empowered to review whether surveillance is necessary, proportionate, and in line with constitutional rights.
- **Prevent Mass Surveillance**: A **proportionality test** should be introduced, ensuring that the surveillance is only used when absolutely necessary and that less invasive alternatives are exhausted.
- **Limiting Spyware Use**: Globally, strict guidelines are needed for **cybersecurity** and **spyware exports** like Pegasus to prevent misuse. **End-to-end encryption** and other **security protocols** must be prioritized to protect users' data from unauthorized surveillance.

//

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

Drishti Mains Question:

Discuss the surveillance laws in India. What reforms are needed to address the challenges posed by

modern surveillance technologies like Pegasus?

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims

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

1. Service providers 2. Data centres
2. 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)