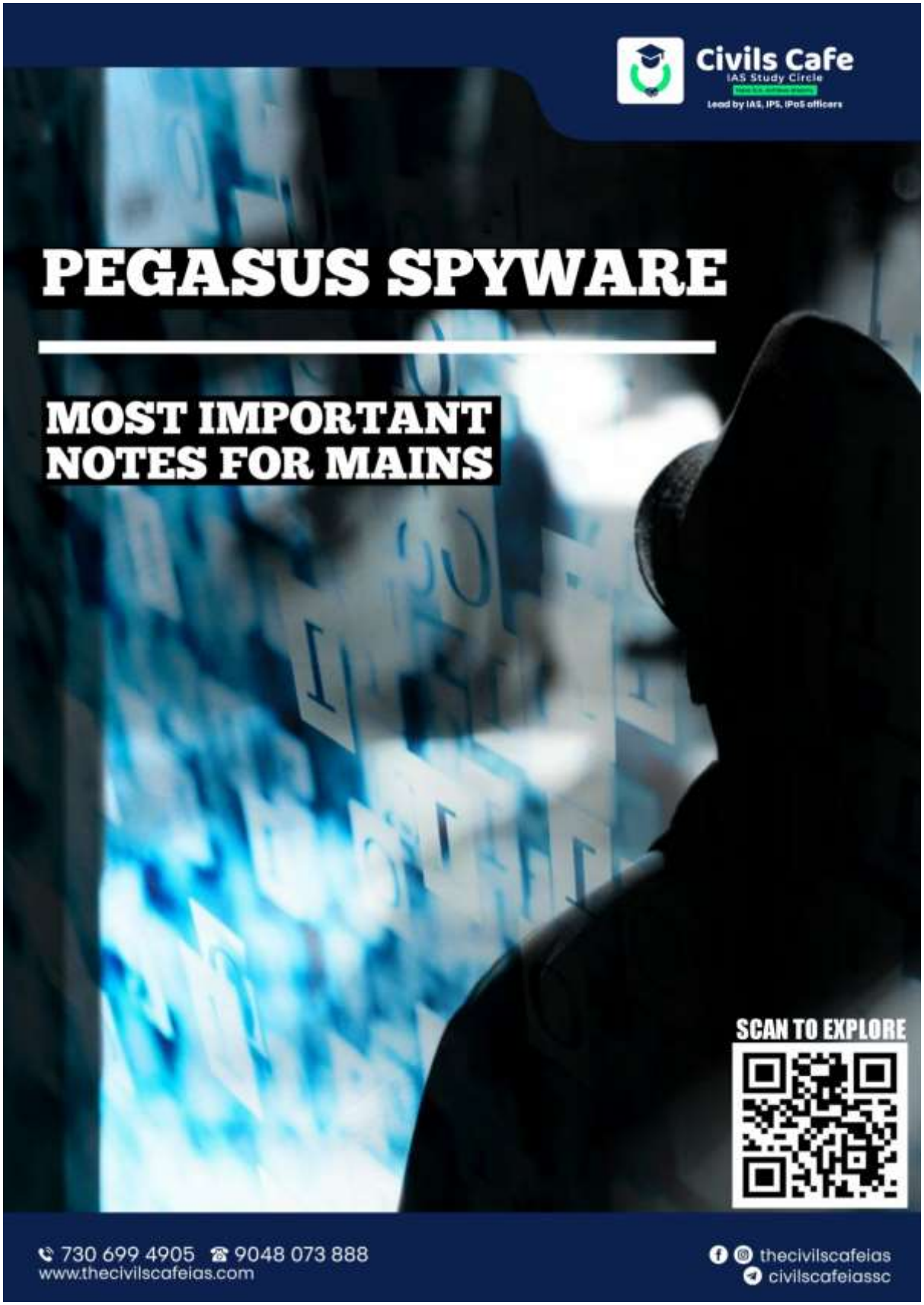
Civils Cafe
IAS Study Circle
Lead by IAS, IPS, IPoS officers
PEGASUS SPYWARE
MOST IMPORTANT
NOTES FOR MAINS
SCAN TO EXPLORE
730 699 4905 9048 073 888
www.thecivilscafeias.com
thecivilscafeias
civilscafeiassc

GS -3 INTERNAL SECURITY

CYBER SECURITY

Syllabus topic: Challenges to Internal Security through Communication Networks, Role of Media and Social Networking Sites in Internal Security Challenges, Basics of Cyber Security; Money-Laundering and its prevention.

PEGASUS SPYWARE ISSUE

In NEWS: A list of persons allegedly targeted by **Pegasus spyware** was released by a multi-organisational investigation involving news organisations, cybersecurity specialists, and Amnesty International. The list includes over 1,000 Indians, including at least 40 journalists, several members of Parliament

SURVEILLANCE

- **A surveillance state** is defined as a state which legally surveils all actions, locations, and friends of its citizens, in order to prevent crimes or in order to solve them faster.
- **Rationality behind surveillance**:
  - **Countering organised crime:** social media has become a tool for facilitating organised crime i.e., to commit and provoke extremism, money laundering, violence and crime.
  - **Neutralizing terrorist activities** Surveillance would help in countering possible terrorist activities by offering better information on potential terror attacks.
  - **Curbing fake news**: Fake news is a new challenge for law enforcement agencies as many lynching incidents reported in 2018 were triggered by fake news being circulated through Whatsapp and other social media sites.
- **Issues of surveillance**:
  - **Effect on Fundamental Rights**: The very existence of a surveillance system impacts the right to privacy and the exercise

of freedom of speech and personal liberty under **Articles 19 and 21** of the Constitution, respectively and also curtails **Articles 32 and 226** of the Constitution.

- ➢ **A lack of oversight:** A secretary of the home ministry has the authority to order the interception. The only legal safeguard against misuse is a review by a three-member review committee comprising the Cabinet secretary and two other top-level bureaucrats.
- ➢ **No independent accountability mechanism**, whether in the form of parliamentary or judicial oversight
- ➢ **A lack of transparency:** The problem is made worse by a complete lack of transparency. In 2013, the central government issued 7,500-9,000 orders per month for the interception of telephones.
- ➢ **Lack of safeguards:** An individual will almost never know that she/he is being surveilled due to the clandestine nature of the act, hence challenging it before a court is a near-impossibility.
- ➢ **Hampers free exchange of information**: It prevents people from reading and exchanging unorthodox, controversial, or provocative ideas.
- ➢ **Creates an atmosphere of distrust:** Surveillance threatens the safety of journalists, especially those whose work criticises the government, and the personal safety of their sources is compromised. It creates an **atmosphere of distrust.**

Judicial position on surveillance

- In **Kharak Singh Vs The State of Uttar Pradesh**, the Supreme Court struck down certain UP Police Regulations that allowed for home visits to "habitual criminals" or those who were likely to become habitual

criminals. The Constitution bench held that such surveillance was violative of Article 21 (right to life and liberty).

- **PUCL case 1996**: The Supreme Court held that the right to privacy would certainly include telephonic conversation in the privacy of one's home or office. Telephone tapping would, thus, infringe Article 21 of the Constitution of India unless it is permitted under the procedure established by law. Subsequently, the Centre codified the guidelines in 2007 under Rule 419A.
- In **R Rajgopal alias RR Gopal and another Vs State of Tamil Nadu (1994),** the Supreme Court held that the right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21.

- **Puttaswamy judgement:** The judicial debate on the status of the right to privacy was, however, settled in August 2017 when a nine-judge bench held that the right to privacy is a fundamental right. The court added that telephone tapping and internet hacking by the State, of personal data, is another area that falls within the realm of privacy.

❖ **PEGASUS SPYWARE ISSUE**

- ➢ **Spyware** is a category of software which aims to steal personal or organisational information.
- ➢ Once a Spyware is installed it starts sending the data from that computer in the background to some other place.
- ➢ What is **Pegasus**?
  - ■ It is a **spyware** created by **NSO Group**; an Israeli cybersecurity firm founded in 2010.
  - ■ The NSO Group's founders come from **Unit 8200** – Israel's elite defence force. It is also the Israel Defence Force's largest military unit and probably the foremost technical intelligence agency in the world.

- Pegasus spyware can **hack** any iOS or Android device and steal a variety of data from the infected device.
- Pegasus can be **deleted remotely**. It's very hard to detect and once it's deleted, **leaves few traces.**
- **Purpose:** Pegasus is designed for three main activities:
  - collection of historic data ona device without user knowledge
  - continuousmonitoring of activity and gathering of personal information and
  - transmission of this data to third parties.
- It helps spyware like Pegasus to gain control over a device **without human interaction** or human error.
- Most of these **attacks exploit software** that receives data even before it can determine whether what is coming in is trustworthy or not, like an email client.
- They are **hard to detect** given their nature and hence even harder to prevent.
- Pegasus utilises "**zero click exploits**" that do not require the victim to do anything. Instead, the spyware is designed to take advantage of bugs in popular apps such as iMessage and WhatsApp to infiltrate the system.
- Pegasus can also use **unsecured websites** to infiltrate a device. These are called **network injection attacks** and also happen without the victim's intervention.
- Pegasus seeks **root privileges** (Root privileges is a level of control over the phone that is beyond what a regular user has).
  - It enables Pegasus to establish communications with its controllers through an anonymised network of internet addresses and servers.

- It can then start transmitting any data stored on the phone to its command-and-control centres. This level of control also means Pegasus can turn on the phone's cameras and microphones to turn it into a spying device without the owner's knowledge.

❖ **Implication of Pegasus Spyware**:

➢ **National security implications**: The use of Pegasus poses a national security risk as it can snoop into national security apparatus.

➢ The issue also indicates that surveillance rules in India are not as per global standards. This **hinders India's ability to enter data sharing agreements,** which allow government agencies to access data stored overseas when required, with other countries.

➢ **Weakness of India's cyberwarfare capacity**: Beyond national security, the Pegasus revelations highlight a disturbing weakness in India's cyber warfare capacity. If it is indeed true that Indian government agencies had to purchase a foreign commercial cyber-weapon for their needs, then we have advertised a strategic vulnerability that is bound to be exploited unless rectified quickly.

➢ **Misuse of data insights**: Vendors of commercial cyber-weapons can get insights as to how their product is being used. This information can be misused by making it available to their governments.

❖ **Supreme Courts stand on Pegasus Spyware Issue**:

➢ The Supreme Court (SC) has appointed an independent expert technical committee to examine allegations that the government used an Israeli spyware, Pegasus, to snoop on its own citizens. Committee will be overseen by a former apex court judge, Justice R.V. Raveendran.

- ➢ The court has also asked the Raveendran committee to **make recommendations on a legal and policy framework to protect citizens against surveillance** and **enhance the cyber security** of the country.

❖ **Rationality of Supreme Court Forming Committee on Pegasus Issue**:

- ➢ Reports that the snooping exercise had widely impacted the **rights to privacy** and **freedom of speech** of ordinary citizens.
- ➢ No clear stand was taken by the Union of India regarding actions taken by it.
- ➢ Seriousness accorded to the allegations by foreign countries and involvement of foreign parties.
- ➢ Possibility that some foreign authority, agency or private entity is involved in placing citizens of this country under surveillance.
- ➢ Allegations that the Union or State Governments are parties to the rights' deprivations of the citizens.
- ➢ As per SC, surveillance, or even the knowledge that one could be spied upon, affects the way individuals exercise their rights. Therefore, it could not ignore allegations that Pegasus affected the **individual rights of the citizenry** as a whole.
- ➢ **Surveillance vs Privacy**:
  - The court has stated that spying on an individual, whether by the state or by an outside agency, amounts to an infraction of privacy. Surveillance is not illegal. But, any limitation on a fundamental right must be proportional and based on evidence
  - Court has thus effectively recognized that an act of surveillance must be tested on four grounds:

1) the action must be supported by legislation

2) the state must show the Court that the restriction made is aimed at a legitimate governmental end

3) the state must demonstrate that there are no less intrusive means available to it to achieve the same objective

4) the state must establish that there is a rational nexus between the limitation imposed and the aims underlying the measure.

❖ LAWS GOVERNING SURVEILLANCE IN INDIA

➢ Communication surveillance in India takes place primarily **under two laws — the Telegraph Act, 1885 and the Information Technology Act, 2000**.

Telegraph Act, 1885:

- It deals with interception of calls. **Section 5(2)** allows for the interception.
- The section states that the **Central Government or a State Government** or any **officer** specially authorised by them may order interception of any telegraph.
- He/she can direct that any message or class of messages shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order. The reasons for such an order **should be recorded in writing.**
- Such an order can be made in the interests of
    - the sovereignty and integrity of India,
    - the security of the State,
    - friendly relations with foreign states or

    - public order or for preventing incitement to the commission of an offence.
- Additionally, a **proviso** in **Section 5(2)** states that even this lawful interception cannot take place against journalists.
- **Public Union for Civil Liberties v Union of India (1996)**: The SC pointed out the lack of procedural safeguards in the provisions of the Telegraph Act and laid down certain guidelines for interceptions.
    - It called for setting up a review committee that can look into authorisations made under Section 5(2) of the Telegraph Act.
    - These guidelines formed the basis of introducing rule 419A in the Telegraph Rules in 2007 and later in the rules prescribed under the IT Act in 2009.
- **Rule 419A states** that a Central Home Secretary and State Home Secretary can issue interception orders on behalf of the centre and state governments, respectively.
- In unavoidable circumstances, Rule 419A adds, such orders may be made by an officer, not below the rank of a Joint Secretary.
- However, such an officer should be duly authorised by the Union Home Secretary or the state Home Secretary.

Information Technology Act, 2000:

- It was enacted to deal with surveillance of all electronic communication, following the Supreme Court's intervention in 1996.
- **The Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 were enacted to further the legal framework for electronic surveillance**.
- **Under Section 69** of the IT Act, all electronic transmission of data can be intercepted. Apart from the restrictions provided in Section 5(2) of

the Telegraph Act and Article 19(2) of the Constitution, the section adds another aspect that makes it broader.

- It broadens the scope of interventions as it allows interception, monitoring and decryption of digital information "for the investigation of an offence".
- Further, it **dispenses with the condition precedent set under the Telegraph Act that requires** "the occurrence of public emergency in the interest of public safety" which widens the ambit of powers under the law.

WAY FORWARD:

- The current legal framework on surveillance has a wide divergence amongst themselves as pointed out by **Justice A P Shah committee**.
  - They differ on "type of interception", "granularity of information that can be intercepted", the degree of assistance from service providers etc.
- Thus, there is **a need to test the wide reach of these laws in the court against the touchstone of fundamental rights**.
  - IT intermediary rules 2021 and the government's 2018 order are being already challenged in the SC.
  - The order authorised 10 security and intelligence agencies to intercept, monitor and decrypt any information generated, transmitted, received or stored in any computer resource.
- Further, **a comprehensive data protection law** to address the gaps in existing frameworks for surveillance should be enacted as recommended by the **B.N Srikrishna Committee.**
- Improve existing laws and procedures for surveillance. The Telegraph Act on phone wiretaps and Information Technology Act on interception of electronic devices suffer from the infirmity of civil bureaucracy signing off on each other's requests.

- Judicial oversight would enable a measure of independent checks and balances.