Chinese state-backed Cyber Attack Attempts

Why in news?

In the latest in a series of surveillance and hacking attempts, a Chinese state-backed hacker firm has been reported to be targeting Indian vaccine makers.

What were the earlier surveillance and hacking attempts?

- **Zhenhua & its targets** - A Shenzhen-based technology company was monitoring over 10,000 Indian individuals and organisations.
- This company, the Zhenhua Data Information Technology Co, has links with the Chinese government and the Chinese Communist Party.
- The attempt was part of the company's global database of "foreign targets".
- Its task is to -
    - collect information about relevant people from the web and social media platforms
    - track research papers, articles, patents, and recruitment positions
- The company also monitors the person's digital footprint across social media platforms and maintains an "information library".
- Those monitored in this database included -
    i. influential political and industrial figures
    ii. bureaucrats in key positions, judges, scientists and academicians, journalists, actors, sportspersons, religious figures, activists
    iii. hundreds accused of financial crime, corruption, terrorism and smuggling
- The collection of such data by Zhenhua does not violate any rules under the Information Technology Act of 2000 in India.
- This is because nearly all of this data is available in the public domain.
- However, Zhenhua's 24×7 watch had raised red flags with cybersecurity experts.
- They feel that the information collected could be put together for tactical manoeuvring.
- It could thereby target the individuals under surveillance or their institutions.
- **Red Echo & ShadowPad** - Recently, Massachusetts-based cybersecurity company Recorded Future published a report.
- It said that it had observed a "steep rise" in the use of resources like

malware by a Chinese group called Red Echo.
- It was used to target "a large swathe" of India's power sector.
- It said 10 distinct Indian power sector organisations were targeted.
- This included four Regional Load Despatch Centres (RLDCs) that are responsible for the smooth operation of the country's power grid by balancing the supply and demand of electricity.
- The group also targeted two Indian seaports.
- Red Echo used malware called ShadowPad, which involves the use of a backdoor to access servers.
- The Ministry of Power recently confirmed these attempts.
- It had said that "no data breach/data loss" had been detected due to the incidents.
- Also, none of POSOCO's functions had been impacted.
    - POSOCO '(Power System Operation Corporation Ltd) is the government enterprise in charge of facilitating transfer of electricity through load despatch centres.
- The government said it had taken action against the threats observed.

What is the recent Stone Panda & vaccines attempt?

- The attempts were highlighted by Goldman Sachs-backed cyber intelligence firm Cyfirma.
- The attempt was related with a Chinese hacker group known as Stone Panda.
- Stone Panda had "identified gaps and vulnerabilities in the IT infrastructure and supply chain software of Bharat Biotech and the Serum Institute of India (SII)."
    - These companies have developed Covaxin and Covishield, which are currently being used in India's Covid-19 vaccination campaign.
    - They are also in the process of testing additional Covid-19 vaccines that could add value to efforts around the world.
- Some Indian companies involved in Covid-19 vaccine development have also faced some issues.
- They have reportedly noticed nearly hundred-fold increase in cyberattack attempts over the last 6 months.
- These were primarily by foreign entities from countries like China and Russia.

What are the key reasons for the series of attempts?

- One major factor is the border clash between the two countries, Indian and China, in June 2020.
- As bilateral tensions continue to rise, there is likely to be continued increase in cyber operations by China-linked groups in line with national strategic

interests.
- China very clearly seems to be adopting and encouraging the use of cyber offensive tools and espionage.
- Even when it is not directly in charge of an offensive operation, it seems to be consistently encouraging actors to develop this capability.
- The attempts could also be part of a long-term strategy.

How is it worldwide?

- There was an increase in cyber offensive operations and incidents around the world in the second half of 2020.
- This especially targeted the healthcare and vaccine space.
- Such incidents were often attributed to actors linked with the Chinese and Russian governments.
- When vaccine companies are targeted, the motive could be competition.
- Notably, SII and Bharat Biotech have been getting global orders for their vaccines.
- Stone Panda's attack against SII and Bharat Biotech's IT systems was possibly to extract their intellectual property and gain a competitive advantage.

What are the drawbacks in India in dealing with it?

- India has not voluntarily made information about these attempts public.
- This lack of information could leave other companies and government bodies in the dark about their vulnerability to such attacks.
- What is needed is more data to be able to figure out what is going on, including specific data about what has happened in India.
- There is also little clarity on the government's chain of command where cybersecurity issues are concerned.
    - Different agencies deal with this issue.
    - This makes it difficult to understand who all to approach in the event of such cyber threats.
- The lack of information and lack of clarity as to the institutional authority impacts India's cyber security as a whole.

Source: The Indian Express