Hybrid Data Warfare by China

Why in News

The Chinese company Zhenhua Data Information Technology Co. Limited is monitoring over 10,000 Indian individuals and organisations in its global database of foreign targets.

Key Points

- **Method:** Zhenhua monitors the **digital footprint** of its targets using **Artificial Intelligence** tools across social media platforms, maintains an **information library,** which includes content not just from news sources, forums, but also from papers, patents, bidding documents, even positions of recruitment.
- **Database:** The database of the company called **Overseas Key Information Database (OKIDB)** has entries from the USA, UK, Japan, Australia, Canada, Germany and the UAE as well.
- **Targets:** Its targets include individuals and institutions in politics, government, judiciary, art and sports, business, technology, media, and civil society.
- **Link to Chinese Government and Intelligence:** The Company counts the Chinese government, intelligentsia and military among its clients.
    - However, the Chinese government has **denied** having asked the company to collect or provide data, information and intelligence stored within other countries' territories for the Chinese government.
- **Implication:** This information can be used for strategic and intelligence services of China for **hybrid warfare.**

- **Legal Aspects:** The data monitoring by Zhenhua cannot be covered under the **Information Technology Rules, 2011, under the IT Act, 2000,** as it only covers personal data and not information available freely or accessible in the public domain.
    - These rules also do not impose any conditions on the use of personal data for direct marketing etc.
    - Though it emphasizes on data collection by consent which is not done by Zhenhua, the law is impossible to enforce in a foreign jurisdiction.
    - India is yet to have a **data protection law** for protecting the privacy of individuals and national security.
- **India-China Relations:** The recent **Indo-China conflict** due to clashes at the Line of Actual Control and later **banning of chinese apps by India** has led to exponential increase in tension between the two countries. In this scenario, the information assets of Zhenhua can give a **strategic leverage to China over India.**

Hybrid Warfare

- **About:** It refers to using non-military tools to achieve dominance or damage, subvert or influence. These tools include **information pollution, perception management and propaganda.**
- **Background :**
    - **By China:** In 1999, Unrestricted Warfare, a publication by China's People's Liberation Army, talked about hybrid warfare and the need for a shift in the arena of violence from military to political, economic and technological.
        There have been many recent reports on China's attempts to collect sensitive military, intelligence or economic information in the USA and Europe through social media.
    - **Lebanon:** Hybrid warfare was used in the **2006 Israel-Lebanon War** by the Hezbollah group.
        It employed a host of different tactics like guerilla warfare, innovative use of technology and effective information campaigning.
    - **Russia:** It was also used by **Russia against Ukraine** in the 2014 annexation of Crimea.
        It involved a combination of activities, including disinformation, economic manipulation, use of proxies and insurgencies, diplomatic pressure etc.

- **Threats:**
    - **Cyber Attacks:** This may include attacks on critical infrastructure like power grids, business systems, and defence systems. These may be used to **disrupt economic activities, undermine institutions, and discredit political leadership and the intelligentsia.**
    - **Undermining Democracy:** The foreign government may manipulate the data, spread propaganda and misinformation and influence democratic systems like elections through use of social media, websites, advertisements etc.
        The 2016 election of the USA and UK Brexit vote are suspected to have been influenced through such interference by Russia.
    - **Inciting Social Discord:** The information may be used to plant disharmony and communal tensions within a society which is eventually a threat to the unity of the country.

Way Forward

- The governments should establish a process to develop a national approach of **self-assessment and threat analysis.** Institutionalizing a process regarding threat and vulnerability information will enhance hybrid warfare early warning efforts, assist resiliency efforts, and may even have a deterrent effect.
- Hybrid threats are an international issue, so should be the response. National governments should coordinate a coherent approach amongst themselves to understand, detect and respond to hybrid warfare to their **collective interests. Multinational frameworks** should be developed to facilitate **cooperation and collaboration across borders.**

Source: IE