Building Cyber Resilience

What is the issue?

- Many high-profile cyberattacks in the recent period has exposed vulnerabilities in the critical infrastructure of even advanced nations.
- This has reinforced the need for improved defences against actual, and potential, cyberattacks by all countries across continents.

What were the recent cyber attacks on the U.S.?

- Towards the end of 2020, a major cyberattack, headlined 'SolarWinds,' had rocked the U.S., believed to have been sponsored from Russia.
- Following this, thousands of U.S. organisations were hacked in early 2021, by a Chinese group Hafnium.
- In quick succession, thereafter, the U.S. has witnessed three more major attacks.
- One was the ransomware attack by Russia/East Europe-based cybercriminals, styled DarkSide, on Colonial Pipeline.
- Another Russia-backed group, Nobellium, next launched a phishing attack on 3,000 e-mail accounts targeting USAID and several other organisations.
- Very recently, JBS SA, the U.S. subsidiary of a Brazilian meat processing company, faced ransomware attack.

What is the changing trend in this regard?

- Cyber attacks are often referred to as the fifth domain/dimension of warfare.
- Most nations are focusing on erecting cyber defences to protect military and strategic targets.
- The obsession of military cyber planners has been to erect defences against software vulnerabilities referred to as 'Zero-day.'
- [This has the capability to cripple a system and could lie undetected for a long time.
- A popular Zero-day software of this kind to date is Stuxnet, which almost crippled Iran's uranium enrichment programme few years back.]
- But, the above mentioned attacks were all primarily on civilian targets.
- Today, a whole new market currently exists for Zero day software outside the military domain.
- Governments and nations much prepare themselves for these new

challenges, which are sure to stretch their capability and resources.
- One related problem is that the distinction between military and civilian targets is increasingly getting erased.
- The consequences of this could be indefinite.
- [E.g. the 2012 cyberattack on Aramco, employing the Shamoon virus, which wiped out the memories of 30,000 computers of the company
- This has ever since been one reason for the very frosty relations between different countries in West Asia and the Gulf region.]
- In the civilian domain, ransomware and phishing, including spear phishing, are the two key modes of cyber warfare today.

What is the impact?

- Ransomware attacks have skyrocketed, with demands and payments going into multi-millions of dollars.
- India figures prominently in this list, being one of the most affected.
- Of late, the recovery cost from the impact of a ransomware attack in India, for example, has tripled.
- Mid-sized companies, in particular, face a catastrophic situation, if attacked, and may even have to cease operations.
- Banking and financial services were most prone to ransomware attacks till date.
- Oil, electricity grids, and lately, health care, have begun to figure prominently.

- **Healthcare sector -** As the COVID-19 pandemic is raging, cyberattacks on health-care systems gains significance.
- Compromised 'health information' of individuals is proving to be a vital commodity for use by cybercriminals.
- The available data aggravates the risk not only to individuals but also to entire communities.

How significant is data protection?

- The data life cycle can broadly be classified into:
    1. data at rest (when it is being created and stored)
    2. data in motion (when it is being transmitted across insecure and uncontrolled networks)
    3. data in use (when it is being consumed)

- Constant exposure lends itself to ever increasing data thefts and abuse.
- Reportedly, more than 3 quintillion bytes of data is created everyday (some put it at over 2.5 quintillion).
- And cybercriminals are becoming more sophisticated, engaging in stealing

sensitive data in targeted computers before launching a ransomware attack.

- So, cybersecurity essentially hinges on data protection.

What are the safety mechanisms available?

- Cybersecurity professionals are now engaged in building a 'Zero Trust Based Environment.'
- This is nothing but zero trust on end point devices, zero trust on identity, and zero trust on the network to protect all sensitive data.
- There are few niche companies today, which have developed/developing newer technologies to create a Zero Trust Based environment, employing:
    i. software defined solutions for agile perimeter security
    ii. secure gateways, cloud access security
    iii. privileged access management
    iv. threat intelligence platforms
    v. static and dynamic data masking, etc.
- There is thus a need to create awareness on the availability of such firms, to ward-off cyberattacks and safeguard data.

What is the way forward?

- Cybersecurity will likely be "the pressing issue of this decade."
- So, building deep technology in cyberspace is essential.
- New technologies such as artificial intelligence, Machine learning and quantum computing, also present new opportunities.
- Carrying out regular vulnerability assessments and creating necessary awareness of the growing cyber threat is essential.

Source: The Hindu

SHANKAR IAS PARLIAMENT
Information is Empowering