The world is hardly wired for cyber resilience

(Mains GS 3 : Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges & Basics of cyber security)

Context:

- A string of high-profile cyber attacks in recent months 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.

America under attack:

- Several high-profile cyber attacks were reported from the United States during the past several months.
- Towards the end of 2020, for instance, a major cyberattack headlined 'SolarWinds' and believed to have been sponsored from Russia had rocked the U.S.
- It involved data breaches across several wings of the U.S. government, including defence, energy and state.
- Before the U.S. could even recover from this breach, thousands of U.S. organisations were hacked in early 2021 in an unusually aggressive cyberattack, by a Chinese group Hafnium, which had exploited serious flaws in Microsoft's software, thus gaining remote control over affected systems.

Now more attacks on civilian targets:

- Cyber, which is often referred to as the fifth domain/dimension of warfare, is now largely being employed against civilian targets, bringing the war into our homes.
- Most nations have been concentrating till date mainly on erecting cyber defences to protect military and strategic targets, but this will now need to change.
- The obsession of military cyber planners has been to erect defences against software vulnerabilities referred to as 'Zero-day', that had the capability to cripple a system and could lie undetected for a long time.

- However, it is evident that a whole new market currently exists for Zero day software outside the military domain, and the world must prepare for this eventuality.

Priority must be given to civilian cyber security:

- Defending civilian targets and critical infrastructure, against cyberattacks such as ransomware and phishing, including spear phishing, apart from unknown Zero day software, is utmost important.
- Nations need to stretch the capability and resources somewhat in the manner that nations have been forced to find the resources and the methods to deal with the COVID-19 pandemic.
- One related problem is that the distinction between military and civilian targets is increasingly getting erased and the consequences of this could be indeterminate.
- For instance, the 2012 cyber attack on Aramco is still one reason for the very frosty relations between different countries in West Asia and the Gulf region.

Economic cost of Cyber warfare in India:

- In the civilian domain, two key manifestations of the 'cat and mouse game' of cyber warfare today, are ransomware and phishing, including spear phishing.
- Ransomware attacks have skyrocketed, with demands and payments going into multi-millions of dollars.
- India figures prominently in the list of one of the most affected country.
- Experts believe that the recovery cost from the impact of a ransomware attack in India has tripled and mid-sized companies today face a catastrophic situation.
- Thus, the need to be aware of the nature of the cyber threat to their businesses and take adequate precautionary measures, has become extremely vital.
- Banking and financial services were most prone to ransomware attacks till date, but oil, electricity grids, and lately, health care, have begun to figure prominently.

Zeroing in on health care:

- The number of cyberattacks on health-care systems are increasing at the time when pandemic is raging,which makes countries more worried.
- With data becoming a vital element in today's world, personal information has become a vital commodity.
- One of the more vulnerable areas where data tends to be linked to a specific individual is in health care.
- Compromised 'health information' is proving to be a vital commodity for use by cybercriminals.
- All indications are that cybercriminals are increasingly targeting a nation's health-care system and trying to gain access to patients' data.
- The available data aggravates the risk not only to the individual but also to entire communities.

Double jeopardy for the targeted victim:

- It would be a mistake to believe that we can hope for a respite from cyberattacks such as ransomware and phishing.
- Cybercriminals are becoming more sophisticated, and are now engaged in stealing sensitive data in targeted computers before launching a ransomware attack.
- This is resulting in a kind of 'double jeopardy' for the targeted victim.
- Today's cybercriminals, specially those specialising in ransomware and similar attacks, are different from the ordinary run-of-the-mill criminals.
- Many are known to practise 'reverse engineering' and employ 'penetration testers' to probe high secure networks.

Motivation for cyberattacks vary:

- Nowadays, the cyber landscape is poised to undergo more fundamental changes.
- Motivation for cyberattacks are highly varied as some do this for nation states where the motivation is geopolitical transformation for cybercriminals
- For many others motivation for cyberattacks is increased profits and for terror groups, the motivation remains chaos in the society with lower risk factor.
- However, it is 'insider threats' due to discontent with the management or for personal reasons that could well become an omnipotent reality.

Need for data protection:

- Cybersecurity essentially hinges on data protection as data becomes the world's most precious commodity.
- Reportedly, the world creates more than three quintillion bytes of data everyday with several billion devices interconnected to billions of end point devices exchanging petabytes of sensitive data, on the network.
- Thus, ensuring data protection could prove to be a rather thankless task which complicates the lives of Information and other security professionals.

Zero Trust Based Environment:

- Constant exposure of data lends itself to ever increasing data thefts and abuse.
- With mobile and cloud computing expanding rapidly, cybersecurity professionals are now engaged in building a 'Zero Trust Based Environment'
- Zero Trust Based Environment means zero trust on end point devices, zero trust on identity, and zero trust on the network to protect all sensitive data.
- However, there do exist quite a few niche companies today, which have developed newer technologies to create a Zero Trust Based environment
- These companies employ software defined solutions for agile perimeter security, secure gateways, cloud access security, privileged access management, threat intelligence platforms, static and dynamic data masking, etc.

- Business community, especially oil, finance, and health care are shown to be more aware than governments and are ready to utilise these technologies to ward-off a cyberattack and safeguard their data.

Preparation is needed:

- Building deep technology in cyber is very essential today.
- New technologies such as artificial intelligence, Machine learning and quantum computing, also present new opportunities.
- Nations that are adequately prepared and have made rapid progress in artificial intelligence and quantum computing have a clear advantage over states that lag behind in cyber security fields.

Conclusion:

- There must be pressure on all stakeholders to carry out regular vulnerability assessments and create necessary awareness of the growing cyber threat.
- IBM Chairman, Arvind Krishna, rightly said that cybersecurity will be “the pressing issue of this decade” and that “value lies in the data and people are going to come after that data”.