Tackling cyber threats

sanskritiias.com/current-affairs/tackling-cyber-threats

(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:

> Cyber attacks may be a relatively new phenomenon, but in a short time frame have come to be assessed as dangerous as terrorism because of ever-evolving nature of security risks.

Traditional response:

- Despite an increase in cyber threats, the world witnessed no change in the method of response as the years 2020 and 2021 have proved to be extremely difficult from the perspective of cyber attacks but no changes in methodology have been seen.
- In 2021, cyber attacks that attracted the maximum attention were SolarWinds and Colonial Pipeline in the U.S., but these were merely the tip of a much bigger iceberg among the string of attacks that plagued the world.
- Estimates of the cost to the world in 2021 from cyber attacks are still being computed, but if the cost of cyber crimes in 2020 (believed to be more than $1 trillion) is any guide, it is likely to range between $3trillion-$4 trillion.
- What is not disputed any longer is that soon cyber crime damage costs would become more profitable than the global trade of all major illegal drugs combined.

Vulnerable sectors:

- The general consensus is that the cyber threat is likely to be among the concerns for both companies and governments across the globe.
- In the Information age, data is gold and credential threats and the threat of data breaches, phishing, and ransomware attacks, apart from major IT outages, are expected to be among the main concerns.
- A little publicised fact is that the vast majority of cyber attacks are directed at small and medium sized businesses, and it is likely that this trend will grow.
- According to experts, among the most targeted sectors in the coming period are likely to be: health care, education and research, communications and governments.

Devastating reality:

- Far more than merely apportioning costs linked to cyber crime is the reality that no organisation can possibly claim to be completely immune from cyber attacks.
- While preventive and reactive cyber security strategies are needed which are essential to mitigate cyber risks but they are proving to be highly illusive in an increasingly hyper-connected world.
- For instance, despite all talk about managing and protecting data, the reality is that ransomware is increasing in intensity and is tending to become a near destructive threat, because there are many available soft targets.
- Apart from loss of data, what is also becoming evident is that ransomware criminals are becoming more sophisticated, and are using ransomware to cripple large enterprises and even governments.

Huge security impact:

- The huge security impact of working from home, dictated largely by the prevailing novel coronavirus pandemic, must again not be underestimated as it is likely to further accelerate the pace of cyber attacks.
- According to experts, a tendency seen more recently to put everything on the Cloud could backfire, causing many security holes, challenges, misconfigurations and outages.
- Furthermore, even as Identity and Multifactor Authentication (MFA) take centre stage, the gloomy prognostication of experts is that Advanced Persistent Threats (APT) attacks are set to increase, with criminal networks working overtime and the Dark web allowing criminals to access even sensitive corporate networks.

Proper solutions needed:

- Despite the plethora of such evidence, cyber security experts appear to be floundering in finding proper solutions to the ever widening cyber threat.
- There is a great deal of talk among cyber security experts about emerging cyber security technologies and protocols intended to protect systems, networks and devices, but little clarity whether what is available can ensure protection from all-encompassing cyber attacks.
- Constant references to the Zero Trust Model and Micro Segmentation as a means to limit cyber attacks, can be self-limiting.
- Zero Trust does put the onus on strict identity verification ‘allowing only authorized and authenticated users to access data applications’, but it is not certain how successful this and other applications will prove to be in the face of the current wave of cyber attacks.

Unique challenges:

- Cyber technology presents certain unique challenges which need particularised answers.
- A detailed study of the series of low- and medium-level proactive cyber attacks that have occurred during the past decade is clearly warranted.
- It could reinforce the belief that when it comes to deterrence in cyber space, what is required is not a piece of ‘grand strategy’: low and medium tech, low and medium risk targeted operations could be just as effective.
- What many companies and even others fail to realise is that inadequate corporate protection and defence could have huge external costs for national security, as was evident in the SolarWinds attack.

Decentralised resilience:

- Nations and institutions, instead of waiting for the ‘Big Bang cyber attack’, should actively prepare for a rash of cyber attacks mainly directed at available data.
- While solving the technical side is ‘one part of the solution, networks and data structures need at the same time to prioritise resilience through decentralised and dense networks, hybrid cloud structures, redundant applications and backup processes’.
- This implies ‘planning and training for network failures so that individuals could adapt and continue to provide service even in the midst of an offensive cyber campaign’.

Conclusion:

Prioritise building trust in systems by creating backup plans including ‘strategic decisions about what should be online or digital and what needs to stay analog or physical, and building capacity within networks to survive’ even if one node is attacked.