Taking a Byte out of Cyber Threats

Why in news?

Rather than wait for the 'Big Bang cyber attack', nations and institutions ought to be prepared for a rash of cyber strikes.

What major cyber attacks threatened the security of the world?

- The world was possibly made aware of the danger and threat posed by cyber weapons with the advent of the **Stuxnet Worm** in 2010, which resulted in large-scale damage to Iran's centrifuge capabilities.
- In 2012, a bank of computers belonging to the **Saudi Aramco Oil Company** were targeted, reportedly by Iranian operatives wiping out data on 30,000 computers.
- Iran was again believed to have been behind a targeted attack on the Qatari natural gas company, **RasGas**.
- The string of instances appear to have provoked the US to warn that the world had to prepare for a kind of 'cyber Pearl Harbour', highlighting a new era of potential vulnerabilities.

India was the second most cyber-attacked country in Asia-Pacific in 2020, a new study by technology major IBM has revealed.

What is the response of the countries to cyber attacks?

- Each succeeding year, despite an increase in cyber threats, witnessed no change in the method of response.
- 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.
- Estimates of the cost to the world in 2021 from cyber attacks are likely to range between 3trillion to 4 trillion dollars.
- Cyber crime damage costs would become more profitable than the global trade of all major illegal drugs combined.

Which sectors are vulnerable to cyberthreats?

- The cyber threat is likely to be a concern for both companies and governments across the globe.
- The main concerns are expected to be
    - credential threats
    - threat of data breaches

    - phishing
    - ransomware attacks
    - major IT outages
- Majority of cyber attacks are directed at small and medium sized businesses and it is likely that this trend will grow.
- The most targeted sectors in the coming period are likely to be
    - health care
    - education and research
    - communications
    - governments
- The emergence of 'Ransomware as a Service' (RaaS) - a business model for ransomware developers is more than an idle threat.
- The huge security impact of working from home due to the pandemic must not be underestimated as it is likely to further accelerate the pace of cyber attacks.
- A tendency which is seen recently to put everything on the Cloud could backfire causing many security holes, challenges, misconfigurations and outages.
- Even as Identity and Multifactor Authentication (MFA) take centre stage, the prediction is that Advanced Persistent Threats (APT) are set to increase, with criminal networks working overtime and the Dark web allowing criminals to access even sensitive corporate networks.

To know more about cybersecurity, click here

Why is it difficult to find proper solutions to the widening cyber threat?

- **Lack of clarity**- Though emerging cyber security technologies and protocols intend to protect systems, networks and devices, there is little clarity on whether it can ensure protection from all-encompassing cyber attacks.
- **Loss of time**- While the West focused on militarization of the cyber threat, and how best it could win with its superior capabilities, valuable time was lost.
- It led to misplaced ideas and erroneous generalisations, resulting in a decade of lost opportunity.
- **Huge costs**- What many companies 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.
- **Limitations of solutions**- Technology details insist on every enterprise to incorporate SASE (Secure Access Service Edge) to reduce the risk of cyber attacks.
- Additional solutions are being proposed such as CASB (Cloud Access Security Broker) and SWG (Secure Web Gateway) aimed at limiting the risks to users from web-based threats.
- Constant references to the Zero Trust Model and Micro Segmentation as a means to limit cyber attacks have limited scope.
- Zero Trust puts the onus on strict identity verification allowing only authorized and authenticated users to access data applications but it is not certain how successful will it be in the face of emerging cyber attacks.
- Cyber security experts should aim at being two steps ahead of cyber criminals but it is absent at present.

What is the way ahead?

- Emphasis should be given on prioritising the defence of data above everything else.

- Law enforcement agencies would need to play a vital role in providing effective defence against cyber attacks.
- While solving the technical side is one part of the solution, networks and data structures need to prioritise resilience through decentralised networks, hybrid cloud structures and backup processes.
- There is a need to prioritise building trust in systems and creating backup plans including strategic decisions and building capacity within networks to survive even if one node is attacked.
- Failure to build resilience at both the technical and human level will mean that the cycle of cyber attacks and the distrust they give rise to will continue to threaten the foundations of democratic society.

Reference

1. https://www.thehindu.com/todays-paper/tp-opinion/taking-a-byte-out-of-cyber-threats/article38415816.ece