IAS PARLIAMENT
Information is Empowering
A Shankar IAS Academy Initiative

Growing Threat of Cyber Warfare

What is the issue?

\n\n

\n

- Cyber-space has emerged as a potential arena for international confrontations.
\n
- Countries like China are already working on expanding their cyber capabilities and India too much start enhancing its cyber-defence capabilities.
\n

\n\n

How serious is cyber threat?

\n\n

\n

- The U.S. Defence Science Board, in a recent report had cautioned that the U.S. cyber defence capabilities were not up to the mark.
\n
- It additionally noted that the next decade is bound to witness massive additional deployment of cyber offence capabilities by many nations.
\n
- As these observations are coming from one of the most potent countries in cyber space currently, the enormity of the challenge is only implicit.
\n
- Significantly, India is consciously and speedily making a serious foray into digital space.
\n
- India's vulnerabilities are only bound to grow exponentially.
\n
- A 2017 study found that India ranked 4th in online security breaches.
\n
- India also accounted for over 5% of global threat detections.

\n

\n\n

What are the various cyber threats?

\n\n

\n
- Cyber threats can manifest in many ways.
\n
- The most visible are cyber crimes, cyber theft, cyber espionage, cyber intrusions etc.
\n
- These are relatively low-end threats.
\n
- Criminal hackers can certainly cause data breaches and even financial loss.
\n
- Countering such large scale threats is important.
\n
- The real danger lies in targeted cyber attacks coming from adversarial nation states that carry out strategically planned and sophisticated cyber attacks.
\n
- “Stuxnet Attack”, which damaged the Iranian nuclear centrifuge facility, is thought to be a cooridated operation of the governments of U.S. and Israel.
\n
- Cyber tools are slowly becoming a regular part of the arsenal of nations.
\n
- Hence, it is essentail to be aware of future cyber-wars and take precauitionary measures.
\n

\n\n

What is required?

\n\n

\n
- The three main components of any national strategy to counter cyber threats are defence, deterrence and exploitation.
\n
- **Defence -** For the defence of critical cyber infrastructure, National Critical Information Infrastructure Protection Centre (NCIIPC) was established.
\n
- While this is a positive, it now needs to partner individual ministries and private companies.

\n

- It should put procedures in place to honestly report breaches.

\n

- However, there are limits to defensive strategies in the cyber domain as the field is highly condusive for offensive capabilities.

\n

- Therefore, cyber deterrence and exploitation have become important, although they are complex and not completely understood now.

\n

\n\n

What are the challenges?

\n\n

\n

- Nuclear deterrence works because there is clarity on the destructive potential.

\n

- But this is not the case with cyber warfare.

\n

- Notably, cyber capabilities of an adversary is not all that apparent.

\n

- This is because unlike nuclear arsenal, there are no missiles to be counted.

\n

- Besides these, identifying the time of the start of the attack and tracking the origins of the attack are also complex tasks.

\n

- For these reasons, deterrence in cyber domain cannot operate in isolation.

\n

- It thus needs the support of economic and diplomatic domains as well.

\n

\n\n

What are the structures that need to be created?

\n\n

\n

- **Militaristic View -** The most serious cyber attacks are when an external state threatens the national security of India by exploiting the cyberspace.

\n

- The danger cannot be countered by an intelligence agency like the *NTRO* or a research organisation like the DRDO.

\n

- The lead agency to deal with this will have to be the defence services.

\n

- This has to gather intelligence, evaluate targets and prepare cyber attack plans.

\n

- Also, cyber operations cannot be a standalone activity.

\n

- It has to be integrated with land, sea and air operations, as a part of information warfare.

\n

- **Defence Cyber Agency -** India is one of the few countries which still do not have a dedicated cyber Command in its military.

\n

- While the setting up of a Defence Cyber Agency has been announced, the effort looks lacklustre and half hearted.

\n

- It is important for a dedicated cyber agency to have significant autonomy.

\n

- It should have an expanded mandate on its own to erect a strong cyber arsenal.

\n

\n\n

\n\n

Source: Indian Express

\n\n

\n\n

Quick Facts

\n\n

National Technical Research Organisation (NTRO)

\n\n

\n

- NTRO was set up in 2004.

\n

- It is a technical intelligence agency under the National Security Advisor (NSA).

\n

- It falls directly under the Prime Minister's Office.
  \n
- It also includes National Institute of Cryptology Research and Development (NICRD) within its ambit.
  \n
- It works for developing technological capabilities in various fields.
  \n
- It acts as a super-feeder agency for providing technical intelligence to other intelligence agencies on internal and external security.
  \n

\n\n

\n