The Need for a New National Security Policy

This article is based on **"The Outlines of A National Security Policy"** which was published in The Hindu on 21/10/2021. It talks about the inclusion of cybertechnology in warfare and the changing prospects of the National Security Policy for India in the technological era.

Cyber is often touted as the fifth dimension of warfare — in addition to land, sea, air and space. It increasingly appears that the cyber warfare is going to become a regular part of the arsenal of nations

As far as India is concerned, it ranks 3rd in terms of the highest number of internet users in the world after the USA and China, but still, its **cybersecurity architecture** is in a nascent approach.

The changing military doctrines, all across the world, favour the need to raise cyber commands reflecting a shift in strategies along with building deterrence in cyberspace.

Cyber Warfares and India

- **About:** It is the use of computer technology to disrupt the activities of a state or organization; deliberately attacking information systems for strategic or military purposes.

  Cyber warfare typically involves the use of **illegal exploitation methods on the internet**, corruption or **disruption of computer networks** and software, hacking, computer forensics and **espionage.**

- **Arguments in Favour of Cyber Warfares:** Tempered by responsible use and appropriate controls, cyberwarfare is a **safer and more flexible strategic alternative**, one critical step between sanctions and bombs.
    - **Minimises Human-life Loss:** Reducing loss of human lives **forms one of the core principles of ethics of war.**
        Cyberwars can be seen as an opportunity to decrease global violence and can **shift wars' focus away from human casualties.**
    - **Prevents Physical Territorial Invasions:** Fighting digitally offers a unique opportunity; the continuation of politics by other means, **without the physical invasion of a sovereign territory.**
- **Arguments Against Cyber Warfares:**
    - **Threat to International Security:** Cyber warfare **attacks on military infrastructure**, government and private communications systems, and financial markets pose a **rapidly growing but little understood threat** to international security and **could become a decisive weapon in future** conflicts among States.
    - **More Number of Countries to Engage in Wars:** Once cybertechnology enters as an important variable in nations' defence policies, the size of a country will cease to matter.
        Even **smaller countries empowered by cybertechnology will be equal to the larger countries** like the US, Russia, India or China, in their capability to cause unacceptable damage.
    - **Lowering Threshold of Entry into War:** Weapons in the 21st century will merely mean a cyber button on the desk of the nation's military/ the leader of the government.
        Geographical land, population, or GDP will be **irrelevant in war-making capacity** or deterrence.
    - **More Frequent Conflicts:** With cyber warfares becoming a norm, each nation will have to be **more prepared for bilateral conflicts that are based on cyber warfare** rather than in multilateral acts of conventional war or rely on military blocs for mobilisation.

- **Threats to India:**
  - **Past Experiences:** India has been the victim of cyber attacks multiple times in the past.
    - In 2009, a **suspected cyber espionage network dubbed GhostNet** was found to be targeting, amongst others, the Tibetan government in exile in India, and many Indian embassies.
    - The **power outage in Mumbai in 2020** is also suspected to be the result of an attack by a Chinese state-sponsored group.
  - **Threats from China:** The real danger to India lies in **targeted cyber attacks coming from adversarial nation** states.

    Countries like China can bring immense assets to bear in carrying out sophisticated cyber attacks.
  - **Lack of Cyberspace Infrastructure:** India is one of the few countries which **still does not have a dedicated cyber component in its military.**

    The setting up of a Defence Cyber Agency was announced but came out only as a typical half-hearted step characterising India's lack of strategic planning process.

Way Forward

- **Bringing Changes to the National Security Policy:**
  - **Clarifying the Objectives:** The National Security Policy in the 21st century **shall define what assets are required to be defended** and the identity of opponents who seek to overawe the people of a target nation by unfamiliar moves to cause disorientation of people.
  - **Setting Priorities:** The national security priorities will require new **departments for supporting several frontiers of innovation and technologies; hydrogen fuel cells**, desalination of seawater, **thorium** for **nuclear technology**, anti-computer viruses, and new immunity-creating medicines.
    - This focus on a new priority will **require compulsory science and mathematics education.**
    - Also, **every citizen will have to be made aware** of the new remote controlled military technology and be ready for it.
  - **Changing the Strategy:** The strategy required for the new national security policy will be to **anticipate the enemies** in many dimensions and by **demonstrative but limited pre-emptive strikes** by developing a strategy of deterrence of the enemy.

    For India, it will be China's cyber capability factor which is the new threat for which it has to devise a new strategy.
  - **New Agenda:** The agenda for the new strategy will be to focus on; **critical & emerging technologies**, connectivity & **infrastructure, cyber security** and maritime security.

- **Role of Policy Makers:** The government should **carve out a separate budget for cybersecurity.**
    - Creating a central body of **cyber warriors to counter state-sponsored hackers.**
        - India's talent base in software development should be harnessed by providing career opportunities.
    - Bootstrapping the cybersecurity capability programme in states through central funding.
- **Defence, Deterrence and Exploitation:** These are the three main components of any national strategy to counter cyber threats.
    - **Critical cyber infrastructure must be defended** and individual ministries and private companies must also put procedures in place to honestly report breaches.
    - **Deterrence in cyberspace** is a hugely complex issue. Nuclear deterrence is successful because there is clarity on the capability of adversaries but cyber warfare lacks any such clarity.
    - **Exploiting cyberspace to achieve national security objectives**. The preparation for this will have to start with the Indian military gathering intelligence, evaluating targets and preparing the specific tools for cyber attacks.

Conclusion

- Once cybertechnology becomes a key variable in the defence policies of a nation, land size or GDP size are irrelevant. Hence, clearer strategy and greater transparency are the need of the hour to improve India's cybersecurity posture.
- A clear public posture on cyber defence and warfare boosts citizen confidence, helps build trust among allies and clearly signals intent to potential adversaries, thus enabling a more stable and secure cyber ecosystem.

Drishti Mains Question

"Cyber is often touted as the fifth dimension of warfare — in addition to land, sea, air and space. However, if cyber warfares become a norm, each nation will have to prepare more for bilateral conflicts that are based on cyber warfare". Comment.