Cyber Warfare

Description

Theme:

- The All India Institute of Medical Sciences (AIIMS), Delhi, one of India's top medical institutions, came under a cyber attack on November 23, 2022, which corrupted all of its servers and resulted in the loss of all of its data, according to information released by the Ministry of Health and Family Welfare (MoHFW). Additionally, there may have been data theft. This cyber-attack is suspected to have originated in China.

What is Cyber Warfare?

- When a nation or a military organisation launches a cyber attack against another nation, that act is known as cyber warfare. This is a military operation whose aim is to spy on, damage, and steal crucial information from the other nation's computer systems and technologies.

Why Cyberwarfare?

- Countries use cyber warfare to gain a military advantage over their adversaries by disrupting or harming their military systems or infrastructure.
- Cyber warfare is a very effective method of spying on the enemy to gather intelligence on their military capabilities, political plans and other sensitive information.
- The cost of launching a cyber attack is very less compared to a full fledge military attack.
- It is very hard to track the source of a cyber attack. A cyber attack can be conducted from anywhere and without leaving a trace behind. This allows countries to carry out attacks without the risk of getting caught.
- Through a cyber attack, it is possible to do heavy damage to an adversary. A cyber attack on the power grid of a country can result in widespread blackouts, a cyber attack on the financial system of a country can result in disruption of financial transactions, and a cyber attack on the nuclear plant of a country can cause the meltdown of the plant and a potential

nuclear disaster.
- Information manipulation and spreading propaganda are other tactics in cyber warfare.

How can a country be prepared?

- Countries can increase their investment in acquiring new technologies and research and development for becoming more resilient to cyber-attacks.
- Countries need to put in place measures like Backup systems and alternative communication networks to ensure that their important infrastructures are more resistant to cyber-attacks.
- Countries should focus on providing regular training to their workforce so that they have the required skills to defend against cyber threats.
- Countries should collaborate with each other to share technologies, information and intelligence to defend against the common threat of cyber attacks.
- There is also a need for countries to develop their cyber forensics capabilities so that they can identify where the cyber attack originated from. This will help in holding accountable the culprit country on the world stage.

International Cooperation:

- Convention on Cybercrime: It is also known as the Budapest Convention and aims to reduce cybercrime by increasing cooperation between countries in investigation and prosecution.
- International Telecommunication Union (ITU): This is a specialized agency United Nations, which releases guidelines and recommendations on best practices for cyber security.
- Some of the regional initiatives like the ASEAN Cyber Capacity Programme and European Union Cyber security Agency promote cooperation and support for cyber defence to its member countries as well as partner countries.
- Global Forum on Cyber Expertise: This is an international platform which promotes cooperation between different governments, the private sector and civil society for sharing expertise and information with each other to improve cyber defence.
- Cyber Security Tech Accord: It is a voluntary commitment by over 150 technology companies to work together to improve cyber security, by sharing information about cyber threats and sharing technology to build a resilient cyber defence.

Conclusion:

Cyber warfare is a significant challenge for many countries including India due to the increasing reliance on technology and the internet in all aspects of society. Cyber attacks pose a national threat and can have significant consequences for the military and civilian infrastructure, as well as the economy. It is important for India to be capable to defend itself against cyber attacks and carry out cyber operations if necessary. For this, India will need to develop its technical capabilities, increase investment in cultivating skilled personnel, and update its Cyber Security Policy, 2013 according to the new age technology and threats. By addressing these issues, India can ensure its national security and effectively utilize cyberspace in the event of a conflict.

Your Turn…

What's your take on this topic? Express your point of view through the comment section below. And subscribe to our blog to read answers to the trending GD topics.

Photo by Tima Miroshnichenko

Copyright @ Group Discussion Ideas.