Cyber Warfare: Red Echo

March 12, 2021
Maharashtra Power Minister Nitin Raut announced that a State Cyber Cell probe had found 14 Trojan horses in the servers of the Maharashtra State Electricity Transmission Company. These malwares had the potential to disrupt power distribution in the State. A US report claimed that a group linked to the Chinese government, which it called 'Red Echo', had targeted 10 vital nodes in India's power distribution system and two seaports.

In news: Red Echo, ShadowPad, and the targeting of India's power grid
Placing it in syllabus: Internal Security
Dimensions

- What is Cyber Warfare?
- Differnce from Cyber Terrorism
- Types of Threat
- Types of Warfare
- Challenges to India
- India's Preparedness
- Suggestions

Content:

What is Cyber Warfare?

- Cyber warfare has been defined by government security expert Richard A. Clarke, in his book Cyber War, as "**actions by a nation-state** to penetrate another nation's computers or networks for the purposes of causing damage or disruption."
- Cyberwarfare is any virtual conflict initiated as a **politically motivated attack** on an enemy's computer and information systems.

- Waged via the Internet, these attacks disable financial and organizational systems by stealing or altering classified data to undermine networks, websites and services.

Differnce from Cyber Terrorism

- Cyber terrorism denotes unlawful attacks and threats of attack against, computers, networks, and information stored therein to intimidate or coerce a government or its people for propagating hidden political or unlawful social and religious agendas.
- Cyber terrorism is simply the use of computers and the Internet connectivity between them in order to launch a terrorist attack.
- Cyberterrorism would be something done by a group of hackers done to inflict fear upon the victims (i.e.: stealing thousands of credit cards to influence the actions of a major banking corporation).
- A cyberterrorist is someone who uses the Internet or network to destroy or damage computers for political reasons or other reasons.
- The main point of difference is that CyberWar is waged by a nation's military/security establishment, whereas cyber terrorism can be by a individual or a small group(i.e. non-state actors)
- The cyberterrorist might target the nation's air traffic control system, electricity-generating companies, or telecommunications infrastructure. Cyberterrorism usually requires a team of highly skilled individuals, millions of dollars, and several years of planning.
- **Fear Factor**: The most common denominator of the majority of terrorist attacks is a terrorist wishes the creation of fear in individual groups, or societies.
- **Speculator factor:** Attacks are aimed at creating huge direct losses and/or resulting in a lot of negative publicity.

- **Vulnerability Factor**: Some of the most effective ways to demonstrate an organisation’s vulnerability is to cause a denial of service to the commercial server or something as simple as the defacement of an organization’s web pages,very often referred to as computer graffiti.

Types of Threat

Cyberwarfare involves the following attack methods:

Sabotage:

- Military and financial computer systems are at risk for the disruption of normal operations and equipment, such as communications, fuel, power and transportation infrastructures.
- Compromise of military systems, such as C4ISTAR components that are responsible for orders and communications could lead to their interception or malicious replacement.
- Power, water, fuel, communications, and transportation infrastructure all may be vulnerable to disruption.
- Example: Malicious program ‘Stuxnet’ infiltrated factory computers and had spread to plants around the world and was extremely effective in delaying Iran’s nuclear program for the development of nuclear weaponry

Cyber Espionage:

- These illegal exploitation methods are used to steal or acquire classified information from rival institutions or individuals for military, political or financial gain.
- The following are the examples:
  - Massive spying by the US on many countries, revealed by Edward Snowden.

    - After the NSA’s spying on Germany’s Chancellor Angela Merkel was revealed, the Chancellor compared the NSA with the Stasi.
    - The NSA recording nearly every cell phone conversation in the Bahamas, without the Bahamian government’s permission, and similar programs in Kenya, the Philippines, Mexico and Afghanistan

Denial-of-service attack (DoS attack)

- a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users.
- Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. DoS attacks often leverage internet-connected devices with vulnerable security measures to carry out these large-scale attacks

Cyber Propaganda

- Cyber propaganda is an effort to control information in whatever form it takes, and influence public opinion.
- It is a form of psychological warfare, except it uses social media, fake news websites and other digital means.

Challenges to India

- India is a target. The country’s core assets such as power grids and financial and transport networks are fast getting connected to the internet and more official data are getting stored online.
- Hostile neighbours and wily groups of global and local extremists are equipping themselves in no-holds-barred cyber warfare
- There have been numerous incidents of sensitive

government and military computers being attacked by unknown entities and information being stolen. The frequency and intensity of such episodes is increasing.

- There is enough evidence to suggest that this is the action of nation states either directly or through proxies.
- There have also been cases of offensive action such as reports of shutting down of power systems.
- Such attacks on critical infrastructure either singly or in multiples are of serious concern, especially with respect to national security.
- The National Cyber Security Policy (NCSP) mainly covers defensive and response measures and makes no mention of the need to develop offensive capacity

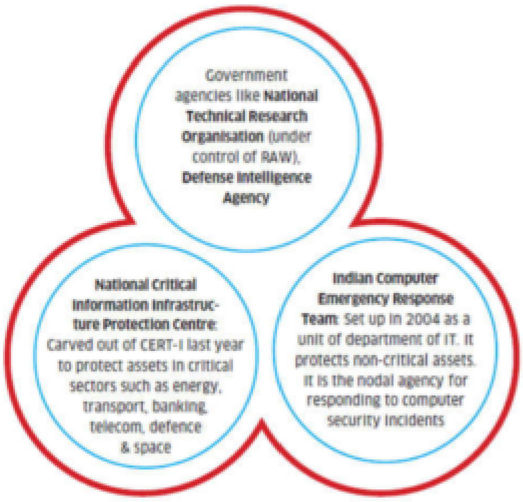
India’s Preparedness:

- India is tapping into a pool of young talent to fortify its anti-cyber war strength.
- The Ministry of Defence has recently upgraded the Defence Information Assurance and Research Agency to establish the **Defence Cyber Agency**, a tri-service command of the Indian armed forces to coordinate and control joint cyber operations, and craft India’s cyber doctrine.
- **The National Technical Research Organisation (NTRO)** was set up in 2004 and is a technical intelligence Agency under the National Security Advisor in the Prime Minister’s Office, India. It is highly specialised technical intelligence gathering
- **National Critical Information Infrastructure Protection Centre (NCIIPC)** takes all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all

stakeholders.

- The **Indian Computer Emergency Response Team (CERT-In)** is the nodal agency to deal with cyber security threats like hacking and phishing. It strengthens security-related defence of the Indian Internet domain.
- In 2015, the Prime Minister established the office of the **National Cyber Security Coordinator** who advises the Prime Minister on strategic cybersecurity issues.

AGENCIES FOCUSED ON CYBER OFFENCE/DEFENCE...



Government agencies like **National Technical Research Organisation** (under control of RAW), **Defense Intelligence Agency**

National Critical Information Infrastructure Protection Centre: Carved out of CERT-I last year to protect assets in critical sectors such as energy, transport, banking, telecom, defence & space

Indian Computer Emergency Response Team: Set up in 2004 as a unit of department of IT. It protects non-critical assets. It is the nodal agency for responding to computer security incidents

Suggestions

- India is also yet to clearly articulate a doctrine that holistically captures its approach to cyber conflict, either for conducting offensive cyber operations, or the extent and scope of countermeasures against cyber attacks.
- Clearer strategy and greater transparency are the need of the hour to improve India's cybersecurity posture.
- To better detect and counter threats from both state actors and their proxies as well as online criminals, improved coordination is needed between the government and the private sector, as well as within the government itself – and at the national and State levels.
- 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.

India needs to invest in the following:

- **Bleeding edge technology:** Bleeding edge refers to technology that has been released but is still not ready for the general public due to the fact that it has not been reliably tested. The term bleeding edge was formed as an allusion to the similar terms “leading edge” and “cutting edge”.
- **Big data analytics:** it is the process of collecting, organizing and analyzing large sets of data (big data) to discover useful information.
- **Air gapping:** Air gapping is a security measure that involves isolating a computer or network and preventing it from establishing an external connection. An air gapped computer is physically segregated and incapable of connecting wirelessly or physically with other computers or network devices.
- Offensive cyber operations and strengthened cyber security.

Mould your thought: What is cyber Warfare? How is it different from Cyber terrorism? Evaluate India’s preparedness for cyber attacks.

Approach to the answer:

- Introduction
- Define cyber Warfare
- Discuss the differences – Cyber Warfare vs Cyber terrorism
- Mention India’s preparedness measures
- Suggest steps to improve the situation
- Conclusion