Cyber Warfare

What is Cyber Warfare?

Cyber warfare is a cyberattack or series of cyberattacks launched against a country or state with the aim of gaining a strategic or military advantage. Acts of cyber war typically involve infiltrating or damaging networks, sabotaging infrastructure, and disrupting the operations of organizations and institutions vital to the target nation's interests.

The main purpose of cyber warfare is to weaken the country by undermining social cohesion, political stability, and military-industrial capacity.

Here are five major impacts of cyber warfare:

Power failures: Disruption to the national electrical grid can harm the economy and affect public opinion.
Cybersecurity breaches: Hacking attacks may corrupt software systems or compromise sensitive government networks.
Data leaks: Large-scale data breaches can impact a range of personally identifiable information, such as medical records or banking details.
Military or industrial sabotage: Direct attacks on a country's national security or economic infrastructure degrade military or industrial capabilities.
Communications disruption: Telephone, mobile, email, or other digital communications can be shut down, intercepted, or otherwise tampered with.

7 Types of Cyber Warfare Attacks:

1. Espionage
2. Sabotage
3. Denial-of-Service Attack
4. Electrical Power Grid
5. Propaganda
6. Economic Disruption
7. Surprise Cyberattack

How cyberwarfare attacks are perpetrated:

How each attack is accomplished may change depending on the target, purpose and type of attack.

Examples of attack methods include the following:

- Viruses, phishing, computer worms and malware that can take down critical infrastructure.

- DDoS attacks that prevent legitimate users from accessing targeted computer networks or devices.
- Hacking and theft of critical data from institutions, governments and businesses.
- Spyware or cyber espionage that results in the theft of information that compromises national security and stability.
- Ransomware that holds control systems or data hostage.
- Propaganda or disinformation campaigns used to cause serious disruption or chaos.

Examples of Cyber warfare operations:

Ukraine and Russia – 2022:

Ukraine saw a large increase in cyber-attacks during Russia's invasion of Ukraine. Well-known groups, such as APT29 and APT28, for example, have been among the nation-state groups performing cyberwarfare attacks. These attacks include malware, data wipers, DDoS attacks and other attacks meant to target critical industrial infrastructure, data networks, and public and private sector organizations, as well as banks.

Iranian weapons systems – 2019:

In June 2019, the United States launched a cyber-attack against Iranian weapons systems that disabled the computer systems associated with controlling rocket and missile launchers.

China's Ministry of State Security – 2018:

In 2018, the U.S. Department of Justice charged two Chinese hackers associated with the Chinese government's Ministry of State Security with targeting intellectual property and confidential business information.

Sony Pictures – 2014:

Hackers associated with the government of North Korea were blamed for a cyber-attack on Sony Pictures after Sony released the film *The Interview*, which portrayed the North Korean leader Kim Jong Un in a negative light.