CYBERWARF
ARE

Definition

The generally accepted definition of cyberwarfare is the use of cyber attacks against a nation-state, causing it significant harm, up to and including physical warfare, disruption of vital computer systems and loss of life.

However, there has been some debate among experts regarding what acts specifically qualify as cyberwarfare. While the United States Department of Defense (DOD) states that the use of computers and the internet to conduct warfare in cyberspace is a threat to national security, why certain activities qualify as warfare, while others are simply cybercrime, is unclear.

Although cyberwarfare generally refers to cyber attacks perpetrated by one nation-state on another, it can also describe attacks by terrorist groups or hacker groups aimed at furthering the goals of particular nations. While there are a number of examples of suspected cyberwarfare attacks in recent history, there has been no formal, agreed-upon definition for a cyber act of war, which experts generally agree would be a cyber attack that directly leads to loss of life.

What kinds of cyber weapons are used in warfare?

Examples of acts that might qualify as cyberwarfare include the following:

- viruses, phishing, computer worms and malware that can take down critica infrastructure;
- distributed denial-of-service (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; and
- propaganda or disinformation campaigns used to cause serious disruption or chaos.

What are the goals of cyberwarfare?

According to the Cybersecurity and Infrastructure Security Agency, the goal of cyberwarfare is to "weaken, disrupt or destroy" another nation. To achieve their goals, cyberwarfare programs target a wide spectrum of objectives that might harm national interests. These threats range from propaganda to espionage and serious disruption with extensive infrastructure disruption and loss of life to the citizens of the nation under attack.

Cyberwarfare is similar to cyber espionage, and the two terms are sometimes confused. The biggest difference is that the primary goal of a cyberwarfare attack is to disrupt the activities of a nation-state, while the primary goal of a cyber espionage attack is for the attacker to remain hidden for as long as possible in order to gather intelligence. The two

Historical examples of cyberwarfare attacks

Bronze Soldier -- 2007

In 2007, the Estonian government moved a Bronze Soldier, a painful symbol of Soviet oppression, from the center of Tallinn, the capital of Estonia, to a military cemetery on the outskirts of the city.

In the following months, Estonia was hit by several major cyber attacks. This resulted in many Estonian banks, media outlets and government sites being taken offline due to unprecedented levels of traffic.

The Stuxnet worm -- 2010

The Stuxnet worm was used to attack Iran's nuclear program in what is considered one of the most sophisticated malware attacks in history. The malware targeted Iranian supervisory control and data acquisition systems and was spread with infected Universal Serial Bus devices.

Edward Snowden -- 2013

Edward Snowden, a former Central Intelligence Agency consultant, leaked details of the U.S. National Security Agency's cyber surveillance system. He attributed this act to ethical concerns about the programs he was involved with

Thank you!