Cybersecurity

Cyberspace

Cyberspace is made up of all the existing computer systems and networks, including offline systems whose common feature is the ability to manage them through passwords.

It consists of three parts. a) the internet where all interconnected computers are incorporated, including b) the world wide web, which is accessible only through URL, c) a cyber-archipelago which consists of all the computer systems that exist in theoretical isolation, in other words, those that do not connect to the internet and the web.

Cyberweapon

Malicious software is software that is designed to interfere with the functions of a computer. Not all forms of malware are weapons from the perspective of international relations.

In terms of national security we are not interested in the vast majority of malware.

Only the below mentioned deserves the title of cyberweapon:

Exploitative codes that cause damage that impacts national security, e.g. steal military and engineering secrets or other sensitive information about politicians during a pre-election period.

Cyberweapons can be used to destroy uranium-enrichment centrifuges, render inoperable the financial infrastructure, paralyse networks, seize valuable military and trade secrets, steal personal data, and damage the states' political, economic, and military security.

Cyber-attack

The term cyber-attack refers to the use of a code to interfere with the operation of a computer system for political or military purposes. Cyberattacks are characterized by the attacker's desire, fulfilment, and ability to disrupt computer operations or destroy material goods through cyberspace.

A cyber-attack can maliciously disable computers, steal data, or use a breached computer to launch other attacks.

The result is not necessarily limited to cyberspace. But in addition to rendering the computer system dysfunctional, it can degrade the social, economic or governmental functions that depend on its proper functioning.

Cyberattacks can be personalized or generalized, affecting the machines of a specific network or all the devices accessible via the internet, such as DDoS attacks.

Cyber-warfare

In case the results of a cyber attack produce significant physical damage or loss of life, then the action can be called an act of cyber-warfare. To date, no cyber-attack meets this criterion, so there has been no cyber-warfare so far.

Malware is a very effective tool for military success. Still, a cyber-attack may increase but not replace traditional military power. However, some military analysts stress their role, warning that cyberattacks could deactivate advanced weapons systems.

Cyber-warfare should not be confused with electronic warfare, which does not involve the use of code to change the operation of a machine but can cause significant damage, for example, through electromagnetic energy.

Cyber-security

Cyber-security consists of measures for the protection of cyberspace from hostile acts. It can also be perceived as a state of affairs, i.e. the absence of intrusions into computer systems and their proper operation.

Moreover, the concept includes measures for shielding cyberspace from threats originating from the technical level, i.e., the security and viability of non-cyber-based operations that rely, however, on the provider computer to which they are logically or logically connected.

To the extent that security measures are a field in which the army is involved or have a corresponding impact on military capabilities, it constitutes cyber-defence.

Cyber-security includes the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberspace and organization and user's assets.

Organization and user's assets encompass connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in cyberspace.

Sources:

The Virtual Weapon and International Order (New Haven: Yale University Press, 2017)

Maria Sotiropoulou (2020) Cybersecurity within the European Union: threats, challenges and preventing strategies

What is a Cyber Attack? - Check Point Software

Cybersecurity (itu.int)