Cyberwarfare is the use of digital attacks to attack a nation, causing comparable harm to actual warfare and/or disrupting the vital computer systems. There is significant debate among experts regarding the definition of cyberwarfare, and even if such a thing exists. One view is that the term "cyberwarfare" is a misnomer, since no offensive cyber actions to date could be described as "war". An alternative view is that "cyberwarfare" is a suitable label for cyber attacks which cause physical damage to people and objects in the real world.

While there is debate over how to define and use "cyberwarfare" as a term, many countries including the United States, United Kingdom, Russia, China, Israel, Iran, and North Korea have active cyber capabilities for offensive and defensive operations. As states explore the use of cyber operations and combine capabilities the likelihood of physical confrontation and violence playing out as a result of, or part of, a cyber operation is increased. However, meeting the scale and protracted nature of war is unlikely, thus ambiguity remains.

The first instance of kinetic military action used in response to a cyber-attack resulting in the loss of human life was observed on 5 May 2019, when the Israel Defense Forces targeted and destroyed a building associated with an on-going cyber-attack.

There is ongoing debate regarding how cyberwarfare should be defined and no absolute definition is widely agreed. While the majority of scholars, militaries and governments use definitions which refer to state and state-sponsored actors, Other definitions may include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations depending on the context of the work.

The former US National Coordinator for Security, Infrastructure Protection and Counter-terrorism, Richard A. Clarke, defines cyberwarfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." Own cyber-physical infrastructure may be weaponized and used by the adversary in case of a cyber conflict, thus turning such infrastructure into tactical weapons.

There is debate on whether the term "cyberwarfare" is accurate. Eugene Kaspersky, founder of Kaspersky Lab, concludes that "cyberterrorism" is a more accurate term than "cyberwar". He states that "with today's attacks, you are clueless about who did it or when they will strike again. It's not cyber-war, but cyberterrorism." Howard Schmidt, former Cyber Security Coordinator of the Obama Administration, said that "there is no cyberwar... I think that is a terrible metaphor and I think that is a terrible concept. There are no winners in that environment."

Some experts take issue with the possible consequences linked to the warfare analogy. Ron Deibert, of Canada's Citizen Lab, has warned of a "militarization of cyberspace", as militaristic responses may not be appropriate. Although, to date, even serious cyber attacks which have disrupted large parts

of a nations electrical grids (230,000 customers, Ukraine, 2015) or affected access to medical care, thus endangering life (NHS, WannaCry, 2017) have not led to military action.

Oxford academic Lucas Kello proposed a new term – "Unpeace" – to denote highly damaging cyber actions whose non-violent effects do not rise to the level of traditional war. Such actions are neither warlike nor peace like. Although they are non-violent, and thus not acts of war, their damaging effects on the economy and society may be greater than even some armed attacks. This term is closely related to the concept of the "grey zone" which has come to prominence in recent years, describing actions which fall below the traditional threshold of war.

The term "cyberwarfare" is distinct from the term "cyber war". "Cyberwarfare" does not imply scale, protraction or violence which are typically associated with the term "war". Cyber warfare includes techniques, tactics and procedures which may be involved in a cyber war. The term war inherently refers to a large scale action, typically over a protracted period of time and may include objectives seeking to utilize violence or the aim to kill. A cyber war could accurately describe a protracted period of back-and-forth cyber attacks (including in combination with traditional military action) between nations. To date, no such action is known to have occurred. Instead, tit-for-tat military-cyber actions are more commonplace. For example, in June 2019 the United States launched a cyber attack against Iranian weapons systems in retaliation to the shooting down of a US drone being in the Strait of Hormuz.

the use of digital attacks, as described by the concept of cyberwarfare, in this page can be a retaliatory response to the cyber attacks. In addition, countries can use cyber sanctions as a reaction to being the targets of the cyber attacks. Sometimes, it is not easy to detect the attacker; however, it might be the case that suspicions can focus on a certain country or group of countries. In these cases, unilateral and multilateral economic sanctions can be used instead of cyberwarfare. For example, economic sanctions related to cyber attacks have been frequently used by the United States government. There are two Executive Orders, EO 13694 in 2015 and EO 13757 in 2016, issued during the Obama administration specifically focused on the implementation of the cyber sanctions. Later on, these Executive Orders have been frequently used by the following US presidents. Furthermore, the Congress is an important actor when it comes to the cyber sanctions. For example, Iran Cyber Sanctions Act of 2016 is a bill that imposes sanctions on specific individuals responsible for the cyber attacks.

Cyber warfare can present a multitude of threats towards a nation. At the most basic level, cyber attacks can be used to support traditional warfare. For example, tampering with the operation of air defenses via cyber means in order to facilitate an air attack. Aside from these "hard" threats, cyber warfare can also contribute towards "soft" threats such as espionage and propaganda. Eugene Kaspersky, founder of Kaspersky Lab, equates large-scale cyber weapons, such as Flame and NetTraveler which his company discovered, to biological weapons, claiming that in an interconnected world, they have the potential to be equally destructive.

Traditional espionage is not an act of war, nor is cyber-espionage, and both are generally assumed to be ongoing between major powers. Despite this assumption, some incidents can cause serious tensions between nations, and are often described as "attacks". For example:

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

The "Titan Rain" probes of American defense contractors computer systems since 2003.

The Office of Personnel Management data breach, in the US, widely attributed to China.

The security firm Area 1 published details of a breach that compromised one of the European Union's diplomatic communication channels for three years.

Out of all cyber attacks, 25% of them are espionage based.

Computers and satellites that coordinate other activities are vulnerable components of a system and could lead to the disruption of equipment. 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. According to Clarke, the civilian realm is also at risk, noting that the security breaches have already gone beyond stolen credit card numbers, and that potential targets can also include the electric power grid, trains, or the stock market.

In mid-July 2010, security experts discovered a malicious software program called Stuxnet that had infiltrated factory computers and had spread to plants around the world. It is considered "the first attack on critical industrial infrastructure that sits at the foundation of modern economies," notes The New York Times.

Stuxnet, while extremely effective in delaying Iran's nuclear program for the development of nuclear weaponry, came at a high cost. For the first time, it became clear that not only could cyber weapons be defensive but they could be offensive. The large decentralization and scale of cyberspace makes it extremely difficult to direct from a policy perspective. Non-state actors can play as large a part in the cyberwar space as state actors, which leads to dangerous, sometimes disastrous, consequences. Small groups of highly skilled malware developers are able to as effectively impact global politics and cyber warfare as large governmental agencies. A major aspect of this ability lies in the willingness of these groups to share their exploits and developments on the web as a form of arms proliferation. This allows lesser hackers to become more proficient in creating the large scale attacks that once only a small handful were skillful enough to manage. In addition, thriving black markets for these kinds of cyber weapons are buying and selling these cyber capabilities to the highest bidder without regard for consequences.

In computing, 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 nameservers. DoS attacks often leverage internet-connected devices with vulnerable security measures to carry out these large-scale attacks. DoS attacks may not be limited to computer-based methods, as strategic physical attacks against infrastructure can be just as devastating. For example, cutting undersea communication cables may severely cripple some regions and countries with regards to their information warfare ability.

The federal government of the United States admits that the electric power grid is susceptible to cyberwarfare. The United States Department of Homeland Security works with industries to identify vulnerabilities and to help industries enhance the security of control system networks. The federal government is also working to ensure that security is built in as the next generation of "smart grid" networks are developed.[48] In April 2009, reports surfaced that China and Russia had infiltrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national security officials. The North American Electric Reliability Corporation (NERC) has issued a public notice that warns that the electrical grid is not adequately protected from cyber attack. China denies intruding into the U.S. electrical grid. One countermeasure would be to disconnect the power grid from the Internet and run the net with droop speed control only. Massive power outages caused by a cyber attack could disrupt the economy, distract from a simultaneous military attack, or create a national trauma.

Iranian hackers, possibly Iranian Cyber Army pushed a massive power outage for 12 hours in 44 of 81 provinces of Turkey, impacting 40 million people. Istanbul and Ankara were among the places suffering blackout.

Howard Schmidt, former Cyber-Security Coordinator of the US, commented on those possibilities:

It's possible that hackers have gotten into administrative computer systems of utility companies, but says those aren't linked to the equipment controlling the grid, at least not in developed countries. [Schmidt] has never heard that the grid itself has been hacked.

In June 2019, Russia said that its electrical grid has been under cyber-attack by the United States. The New York Times reported that American hackers from the United States Cyber Command planted malware potentially capable of disrupting the Russian electrical grid.

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. In 2018, Sir Nicholas Carter, Chief of the General Staff of the British Army stated that this kind of attack from actors such as Russia "is a form of system warfare that seeks to de-legitimize the political and social system on which our military strength is based".

Jowell and O'Donnell (2006) state that "propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist" (p. 7). The internet is a phenomenal means of communication. People can get their message across to a huge audience, and with this opens a window for evil. Terrorist organizations can use this medium to brainwash people. It has been suggested that restricted media coverage of terrorist attacks would in turn decrease the number of terrorist attacks that occur afterwards (Cowen 2006).

In 2017, the WannaCry and Petya (NotPetya) cyber attacks, masquerading as ransomware, caused large-scale disruptions in Ukraine as well as to the U.K.'s National Health Service, pharmaceutical giant Merck, Maersk shipping company and other organizations around the world. These attacks are also categorized as cybercrimes, specifically financial crime because they negatively affect a company or group.

The idea of a "cyber Pearl Harbor" has been debated by scholars, drawing an analogy to the historical act of war. Others have used "cyber 9/11" to draw attention to the nontraditional, asymmetric, or irregular aspect of cyber action against a state.

There are a number of reasons nations undertake offensive cyber operations. Sandro Gaycken [de], a cyber security expert and adviser to NATO, advocates that states take cyber warfare seriously as they are viewed as an attractive activity by many nations, in times of war and peace. Offensive cyber operations offer a large variety of cheap and risk-free options to weaken other countries and strengthen their own positions. Considered from a long-term, geostrategic perspective, cyber offensive operations can cripple whole economies, change political views, agitate conflicts within or among states, reduce their military efficiency and equalize the capacities of high-tech nations to that of low-tech nations, and use access to their critical infrastructures to blackmail them.

Potential targets in internet sabotage include all aspects of the Internet from the backbones of the web, to the internet service providers, to the varying types of data communication mediums and network equipment. This would include: web servers, enterprise information systems, client server systems, communication links, network equipment, and the desktops and laptops in businesses and homes. Electrical grids, financial networks, and telecommunication systems are also deemed vulnerable, especially due to current trends in computerization and automation.