According to the U.S. federal law known as the Anti-Cybersquatting Consumer Protection Act, cybersquatting is registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else. The term derives from squatting, the practice of inhabiting someone else's property without their permission.

Commercial domain names (technically, you reserve a second-level domain name) are obtained from one of several registries. However, these registries make no attempt to determine whether the domain name is one that rightfully ought to go to someone else. Consequently, a number of enterprising individuals and companies have applied for and reserved domain names, either new or expired, that they think someone else will want, either now or in the future.

Many cybersquatters reserve common English words, reasoning that sooner or later someone will want to use one for their Web site. Another target is mis-typed spellings of popular web sites. Cybersquatters will also regularly comb lists of recently expired domain names, hoping to sell back the domain name to a registrant who inadvertently let his domain name expire.

Since there is an initial and yearly fee for owning a domain name, some cybersquatters reserve a long list of names and defer paying for them until forced to preempt their use by others at no cost to themselves. The registry companies are working on this problem. Meanwhile, the Internet Corporation for Assigned Names and Numbers (ICANN), which licenses the domain name registrars, is working on a process for resolving domain name disagreements outside of the regular court system. Although trademark laws may offer some protection, it is often cheaper to buy the domain name from the cybersquatter than it is to sue for its use.

Cybersquatting (also known as domain squatting), according to the United States federal law known as the Anticybersquatting Consumer Protection Act, is registering, trafficking in, or using a domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else. The cybersquatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price.

The term is derived from "squattting", which is the act of occupying an abandoned or unoccupied space or building that the squatter does not own, rent or otherwise have permission to use. Cybersquatting, however, is a bit different in that the domain names that are being "squatted" are (sometimes but not always) being paid for through the registration process by the cybersquatters. Cybersquatters usually ask for prices far greater than that at which they purchased it. Some cybersquatters put up derogatory remarks about the person or company the domain is meant to represent in an effort to encourage the subject to buy the domain from them. Others post paid links via Google, Yahoo!, Ask.com and other paid advertising networks to the actual site that the user likely wanted, thus monetizing their squatting.

Another strategy is as follows: Internet domain name registrations are for a fixed period of time. If the owner of a domain name doesn't re-register the name with an internet registrar prior to the domain's expiration date, then the domain name can be purchased by anybody else after it expires. At this point the registration is considered lapsed. A cybersquatter may use automated software tools to register the lapsed name the instant it is lapsed. This strategy is one of a family of identity theft schemes including renewal snatching, extension exaggeration and alert angling.
Cybersquatting refers to using, trafficking in or registering a domain name with the intention of taking advantage of the popularity of another company’s trademark. These cybersquatters generally register these domains before the target company, thus forcing the latter to buy the domain from them at a higher price.

Cybersquatting comes from the term squatting, which describes the act of occupying a land, building or any other property without the knowledge or permission of the owner. In a sense, cybersquatting entails cybersquatters registering a company or a trademark for his domain name and forcing the company to buy the domain name by advertising it as the legitimate company site. In some cases, the domain name is used for posting derogatory remarks about the target company. The legitimate company’s only option is to buy the domain name at ridiculously high prices.

Cyberterrorism is the use of Internet-based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.

Cyberterrorism is a controversial term. Some authors choose a very narrow definition, relating to deployments, by known terrorist organizations, of disruption attacks against information systems for the primary purpose of creating alarm and panic. By this narrow definition, it is difficult to identify any instances of cyberterrorism.

There is much concern from government and media sources about potential damages that could be caused by cyberterrorism, and this has prompted official responses from government agencies.

History.

Public interest in cyberterrorism began in the late 1980s. As 2000 approached, the fear and uncertainty about the millennium bug heightened and interest in potential cyberterrorist attacks also increased. However, although the millennium bug was by no means a terrorist attack or plot against the world or the United States, it did act as a catalyst in sparking the fears of a possibly large-scale devastating cyber-attack. Commentators noted that many of the facts of such incidents seemed to change, often with exaggerated media reports.

The high profile terrorist attacks in the United States on September 11, 2001 and the ensuing War on Terror by the US led to further media coverage of the potential threats of cyberterrorism in the years following. Mainstream media coverage often discusses the possibility of a large attack making use of computer networks to sabotage critical infrastructures with the aim of putting human lives in jeopardy or causing disruption on a national scale either directly or by disruption of the national economy.