Cyberterrorism essay

Media, Advertising

Cyberterrorism is a phrase used to describe 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. Cyberterrorism can also be defined much more generally, for example, as " The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives. " This broad definition was created by Kevin G.

Coleman of the Technolytics Institute. [1] The term was coined by Barry C. Collin. [2] OverviewAs the Internet becomes more pervasive in all areas of human endeavor, individuals or groups can use the anonymity afforded by cyberspace to threaten citizens, specific groups (i. e. with membership based on ethnicity or belief), communities and entire countries, without the inherent threat of capture, injury, or death to the attacker that being physically present would bring.

As the Internet continues to expand, and computer systems continue to be assigned more responsibility while becoming more and more complex and interdependent, sabotage or terrorism via cyberspace may become a more serious threat. edit] Basic definition Cyberterrorism is the leveraging of a target's computers and information , particularly via the Internet, to cause physical, real-world harm or severe disruption of infrastructure. Cyberterrorism is defined as “ The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives. ” This definition was created by Kevin G. Coleman of the Technolytics Institute. [1] ..

. subsumed over time to encompass such things as simply defacing a web site or server, or attacking non-critical systems, resulting in the term becoming less useful… There are some that say cyberterrorism does not exist and is really a matter of hacking or information warfare.

They disagree with labeling it terrorism because of the unlikelihood of the creation of fear, significant physical harm, or death in a population using electronic means, considering current attack and protective technologies. The National Conference of State Legislatures (NCSL), a bipartisan organization of legislators and their staff created to help policymakers of all 50 states address vital issues such as those affecting the economy or homeland security by providing them with a forum for exchanging ideas, sharing research and obtaining technical assistance [1] defines cyberterrorism as follows: the use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, Denial-of-service attacks, or terroristic threats made via electronic communication. [2] Demitri Jesus Olmo.

[edit] Background information Public interest in cyberterrorism began in the late 1980s. As the year 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 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. Authors such as Winn Schwartau and John Arquilla are reported to have had considerable financial success selling books which described what were purported to be plausible scenarios of mayhem caused by cyberterrorism. Many critics claim that these books were unrealistic in their assessments of whether the attacks described (such as nuclear meltdowns and chemical plant explosions) were possible.

A common thread throughout what critics perceive as cyberterror-hype is that of non-falsifiability; that is, when the predicted disasters fail to occur, it only goes to show how lucky we’ve been so far, rather than impugning the theory. edit] Effects Cyberterrorism can have a serious large-scale influence on significant numbers of people. It can weaken countries’ economy greatly, thereby stripping it of its resources and making it more vulnerable to military attack. Cyberterror can also affect internet-based businesses. Like brick and mortar retailers and service providers, most websites that produce income (whether by advertising, monetary exchange for goods or paid services) could stand to lose money in the event of downtime created by cyber criminals. As internet-businesses have increasing economic importance to countries, what is normally cybercrime becomes more political and therefore “ terror” related. [edit] Examples One example of cyberterrorists at work was when terrorists in Romania illegally gained access to the computers controlling the life support systems at an Antarctic research station, endangering the 58 scientists involved.

However, the culprits were stopped before damage actually occurred. Mostly non-political acts of sabotage have caused financial and other damage, as in a case where a disgruntled employee caused the release of untreated sewage into water in Maroochy Shire, Australia. [3] Computer viruses have degraded or shut down some non-essential systems in nuclear power plants, but this is not believed to have been a deliberate attack. More recently, in May 2007 Estonia was subjected to a mass cyber-attack in the wake of the removal of a Russian World War II war memorial from downtown Tallinn.

The attack was a distributed denial-of-service attack in which selected sites were bombarded with traffic in order to force them offline; nearly all Estonian government ministry networks as well as two major Estonian bank networks were knocked offline; in addition, the political party website of Estonia's current Prime Minister Andrus Ansip featured a counterfeit letter of apology from Ansip for removing the memorial statue. Despite speculation that the attack had been coordinated by the Russian government, Estonia's defense minister admitted he had no conclusive evidence linking cyber attacks to Russian authorities. Russia called accusations of its involvement " unfounded," and neither NATO nor European Commission experts were able to find any conclusive proof of official Russian government participation.

[3] In January 2008 a man from Estonia was convicted for launching the attacks against the Estonian Reform Party website and fined. [4][5] Even more recently, in October 2007, the website of Ukrainian president Viktor Yushchenko was attacked by hackers. A radical Russian nationalist youth group, the Eurasian Youth Movement, claimed responsibility. [6]Since the world of computers is ever-growing and still largely unexplored, countries new to the cyber-world produce young computer scientists usually interested in " having fun".

Countries like China, Greece, India, Israel, and South Korea have all been in the spotlight before by the U. S. Media for attacks on information systems related to the CIA and NSA. Though these attacks are usually the result of curious young computer programmers, the United States has more than legitimate concerns about national security when such critical information systems fall under attack. In the past five years, the United States has taken a larger interest in protecting its critical information systems.

It has issued contracts for high-leveled research in electronic security to nations such as Greece and Israel, to help protect against more serious and dangerous attacks. In 1999 hackers attacked NATO computers. The computers flooded them with email and hit them with a denial of service (DoS). The hackers were protesting against the NATO bombings in Kosovo. Businesses, public organizations and academic institutions were bombarded with highly politicized emails containing viruses from other European countries.