CYBER TERRORISM

- Cyber terrorism 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.
CYBER TERRORISM

**Cyber terrorism** 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 cyber terrorism.

There are others who say cyber terrorism 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.
CYBER TERRORISM

Cyber terrorism 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. The term was coined by Barry C. Collin.
CYBER TERRORISM

• As 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.
Effects of cyber terrorism

• Cyber terrorism 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.

• Cyber terror 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
Examples of Cyber-Terrorism

• 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.

• In January 2008 a man from Estonia was convicted for launching the attacks against the **Estonian Reform Party** website and fined.
Examples of Cyber-Terrorism

- 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.

- 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".
Examples of Cyber-Terrorism

• 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.
Examples of Cyber-Terrorism

• 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.
Countering Cyber Terrorism

• The US Department of Defense charged the United States Strategic Command with the duty of combating cyber terrorism. This is accomplished through the Joint Task Force-Global Network Operations (JTF-GNO). JTF-GNO is the operational component supporting USSTRATCOM in defense of the DoD's Global Information Grid. This is done by integrating GNO capabilities into the operations of all DoD computers, networks, and systems used by DoD combatant commands, services and agencies.