**Cyber crime** refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. **Net crime** refers to criminal exploitation of the [internet](http://en.wikipedia.org/wiki/Internet). Dr. Debarati Halder and Dr. K. Jaishankar (2011) **defines** Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation’s security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding [cracking](http://en.wikipedia.org/wiki/Hacker_(computer_security)), [copyright infringement](http://en.wikipedia.org/wiki/Copyright_infringement), [child pornography](http://en.wikipedia.org/wiki/Child_pornography), and [child grooming](http://en.wikipedia.org/wiki/Child_grooming). There are also problems of [privacy](http://en.wikipedia.org/wiki/Privacy) when [confidential](http://en.wikipedia.org/wiki/Confidential) information is lost or intercepted, lawfully or otherwise.

An Australian nationwide survey conducted in 2006 found that two in three convicted cyber-criminals were between the ages of 15 and 26.

Internationally, both governmental and non-state actors engage in cybercrimes, including [espionage](http://en.wikipedia.org/wiki/Espionage), [financial theft](http://en.wikipedia.org/wiki/Theft), and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as [cyber warfare](http://en.wikipedia.org/wiki/Cyber_warfare). The international legal system is attempting to hold actors accountable for their actions through the [International Criminal Court](http://en.wikipedia.org/wiki/International_Criminal_Court).

Computer crime encompasses a broad range of activities. Generally, however, it may be divided into two categories: (1) crimes that target computers directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

Crimes that primarily target computer networks or devices include:

* [Computer viruses](http://en.wikipedia.org/wiki/Computer_viruses)
* [Denial-of-service attacks](http://en.wikipedia.org/wiki/Denial-of-service_attacks)
* [Malware](http://en.wikipedia.org/wiki/Malware) (malicious code)

Crimes that use computer networks or devices to advance other ends include:

* [Cyber stalking](http://en.wikipedia.org/wiki/Cyberstalking)
* [Fraud](http://en.wikipedia.org/wiki/Fraud) and [identity theft](http://en.wikipedia.org/wiki/Identity_theft)
* [Information warfare](http://en.wikipedia.org/wiki/Information_warfare)
* [Phishing scams](http://en.wikipedia.org/wiki/Phishing)

[Spam](http://en.wikipedia.org/wiki/E-mail_spam)

The unsolicited sending of bulk [email](http://en.wikipedia.org/wiki/Email) for commercial purposes, is un-lawful [in some jurisdictions](http://en.wikipedia.org/wiki/E-mail_spam_legislation_by_country). While anti-spam laws are relatively new, limits on unsolicited electronic communications have existed for some time.

**Fraud**

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

* Altering in an unauthorized way. This requires little technical expertise and is not an uncommon form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;
* Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions: this is difficult to detect;
* Altering or deleting stored data;
* Altering or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes.

Other forms of fraud may be facilitated using computer systems, including [bank fraud](http://en.wikipedia.org/wiki/Bank_fraud), [identity theft](http://en.wikipedia.org/wiki/Identity_theft), [extortion](http://en.wikipedia.org/wiki/Extortion), and [theft of classified information](http://en.wikipedia.org/wiki/Classified_information).

A variety of [Internet scams](http://en.wikipedia.org/wiki/Internet_fraud) target direct to consumers.

**Drug trafficking**

Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted [e-mail](http://en.wikipedia.org/wiki/E-mail) and other Internet Technology. Some [drug traffickers](http://en.wikipedia.org/wiki/Drug_trafficker) arrange deals at [internet cafes](http://en.wikipedia.org/wiki/Internet_cafe), use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms.

The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away.

**Cyber terrorism**

*Main article:*[*Cyber terrorism*](http://en.wikipedia.org/wiki/Cyber_terrorism)

Government officials and [Information Technology](http://en.wikipedia.org/wiki/Information_Technology) security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern among federal officials that such intrusions are part of an organized effort by [cyber terrorists](http://en.wikipedia.org/wiki/Cyberterrorist), foreign intelligence services, or other groups to map potential security holes in critical systems. A cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching computer-based attack against computers, network, and the information stored on them.

Cyber terrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered cyber terrorism. As well there are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

Cyber extortion is a form of cyber terrorism in which a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks. According to the Federal Bureau of Investigation, cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a [distributed denial-of-service attack](http://en.wikipedia.org/wiki/Distributed_denial-of-service_attack).

**Hacker**

In the [computer security](http://en.wikipedia.org/wiki/Computer_security) context, a **hacker** is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge.[[1]](http://en.wikipedia.org/wiki/Hacker_(computer_security)#cite_note-crackdown-1) The subculture that has evolved around hackers is often referred to as the computer underground and is now a known [community](http://en.wikipedia.org/wiki/Community). While other uses of the word hacker exist that are not related to computer security, such as referring to someone with an advanced understanding of computers and computer networks, they are rarely used in mainstream context. They are subject to the long standing [hacker definition controversy](http://en.wikipedia.org/wiki/Hacker_definition_controversy) about the true meaning of the term [hacker](http://en.wikipedia.org/wiki/Hacker_(term)). In this controversy, the term hacker is reclaimed by [computer programmers](http://en.wikipedia.org/wiki/Hacker_(programmer_subculture)) who argue that someone breaking into computers is better called a **cracker**, not making a difference between computer criminals ([black hats](http://en.wikipedia.org/wiki/Black_hat_hacking)) and computer security experts ([white hats](http://en.wikipedia.org/wiki/White_hats)).Some white hat hackers claim that they also deserve the title hacker, and that only black hats should be called crackers.