# Glossary

**Application encryption:** Cryptographic functions built into the communications protocols for a specific application, like e-mail. Examples include PEM, PGP, and SHTTP.

**Authentication:** The ability to ensure that the given information is produced by the entity whose name it carries and that it was not forged or modified.

**Availability:** It means that data is accessible and services are operational, despite possible disruptive events such as power-supply cuts, natural disasters, accidents, or attacks. This is particularly vital in contexts where communication network failures can cause breakdowns in other critical networks, such as air transport or the power supply.

**Buffer overflow:** This means techniques by which large inputs are given to software to induce it to do things it normally does not.

**Carnivore:** This is an FBI system that is used to analyze the e-mail packets of suspected criminals.

**Certificate, public key:** This is a specially formatted block of data that contains a public key and the name of its owner. The certificate carries the digital signature of a certification authority to authenticate it.

**Collateral damage:** This is damage from an attack to other than the intended targets.

**Communication:** This is any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network, except to the extent that the information can be related to the identifiable subscriber or user receiving the information.

**Computer forensics:** This includes methods for analyzing computers and networks to determine what happened to them during a cyber attack, with the hope of repairing the damage and preventing future similar attacks.

**Confidentiality:** It is the protection of communications or stored data against interception and reading by unauthorized persons. It is particularly needed for the transmission of sensitive data and is one of the requirements for addressing privacy concerns of users of communication networks. Systems and networks must enforce this control at all levels.

**Covert channel:** This is a concealed communications channel.

**Critical infrastructure protection:** This means security of those physical and cyber-based systems that are essential to the minimum operations of the economy and government by ensuring protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.

**Cryptography:** The practice and study of encryption and decryption—encoding data so that it can only be decoded by specific individuals. A system for encrypting and decrypting data is a cryptosystem.

**Cyber attack:** This refers to offensive acts against computer systems or networks.

**Cyber war:** This is attacks on computer systems and networks by means of software and data.

**Cyber weapon:** Software designed to attack computers and data.

**Denial of service:** This refers to an attack that overwhelms a cyberspace resource with requests so as to prevent authorized persons from using the resource.

**Department of Homeland Security (DHS):** The Homeland Security Act of 2002, which created the Department of Homeland Security (DHS), brought together 22 diverse organizations to help prevent terrorist attacks in the United States, reduce the vulnerability of the United States to terrorist attacks, and minimize damage and assist in recovery from attacks that do occur.

**Digital watermarks:** Much like a watermark on a letterhead, a digital watermark is used to assist in identifying ownership of a document or other file. It includes embedded unique strings of data that do not alter the sensory perception of the image file, music file, or other data file.

**Echelon:** This is a putative system of analysis of international communications. The details of the system are difficult to obtain because many government officials often deny or ignore reports regarding the existence of Echelon.

**Electronic communications network:** This is a transmission systems and, where applicable, switching or routing equipment and other resources that permit the conveyance of signals by wire, by radio, by optical, or by other electromagnetic means, including satellite networks; fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks; electric cable systems; and, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting and cable television networks, irrespective of the type of information conveyed.

**Encryption:** This is a reversible method of encoding data, requiring a key to decrypt. Encryption can be used in conjunction with steganography to provide another level of secrecy.

**Encryption:** This is a systematic and reversible way of making a message unintelligible by using secret keys.

**Escalation of privileges:** This is exploiting security weaknesses to increase one's abilities on a computer system.

**Financial services information sharing and analysis centers (FS-ISAC):** The FS-ISAC, established in response to PDD-63, is a not-for-profit organization formed to serve the needs of the financial services industry for the dissemination of physical and cyber security, threat, vulnerability, incident, and solution information.

**Hacker:** This refers to an amateur attacker of computers or sites on the Internet.

**Hacktivism:** This refers to politically motivated attacks on publicly accessible Web pages/resources or e-mail servers.

**Information sharing and analysis centers:** Presidential Decision Directive 63 (PDD-63) in 1998 resulted in creation of information sharing and analysis centers to allow critical sectors to share information and work together to help better protect the economy.

**Information warfare:** This means the use and management of information in pursuit of a competitive advantage over an opponent.

**Integrity:** It is the confirmation that data that has been sent, received, or stored are complete and unchanged, that is not altered by inappropriate treatment or a malevolent event . This is particularly important in relation to authentication for the conclusion of contracts or where data accuracy is critical (medical data, industrial design, etc.).

**Jus in bello:** These are international laws for conducting warfare.

**Location data:** This is any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

**Pacifism:** An ethical position opposed to warfare and violence.

**Patch:** This means a modification of software to fix vulnerabilities that a cyber attack could exploit.

**Phishing:** This type of e-mail tries to steal secrets by directing users to a counterfeit Web site.

**Presidential Decision Directive (PDD) 63:** In 1998, the Clinton Administration issued Presidential Decision Directive 63 (PDD-63), to meet the demands of national security interests in cyberspace and to help protect the critical infrastructure of the United States.

**Private key:** Key used in public key cryptography that belongs to an individual entity and must be kept secret.

**Public key system:** A public key system is one which uses two keys, a public key known to everyone and a private key that only the recipient of message uses.

**Rootkit:** This replacement code for the operating system of a computer is placed on a compromised system by an attacker to ensure that their malicious activities will be hidden and to simplify future access to the system by them.

**RSA:** A popular, highly secure algorithm for encrypting information using public and private keys, obscurely named for the initials of its creators (Massachusetts Institute of Technology (MIT) professors Ron Rivest, Adi Shamir, and Leonard Adleman).

**Secure sockets layer (SSL):** Cryptography protocol applied to data at the socket interface. It is often bundled with applications and widely used to protect World Wide Web traffic.

**Social engineering:** This refers to methods to trick or manipulate people into providing sensitive information or performing a task.

**SpamMimic:** A Web site located at http://www.spammimic.com can be used to send a message that appears to be spam when in reality the message is just a cover for sending secret content. The use of spam as a cover will likely increase the workload of FBI systems, such as Carnivore and Echelon.

**Steganalysis:** This is the process of detecting hidden data in other files. Steganalysis is typically done by searching for small deviations in the expected pattern of a file.

**Steganography:** In general, it is the process of hiding information or "covered writing." More specifically, in the digital environment, steganography involves hiding data or images within other files, so they appear unaltered to persons unaware of the secret content.

**Steganography:** This means concealed messages within others.

**Traffic data:** This is any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

**Virtual fingerprint:** This is a unique digital water-mark that can be used to uniquely identify a particular file.

**Zero-day attack:** This is a type of cyber attack that has not been used before.