Short Glossary

(from **The Art of War of Cybersecurity**, by Thomas Reynolds, © 2007,
Glossary online version as modified 20.July.2010, © 2010)

Disclaimer: YMMV about these explanations, which should not be taken as any more than rough definitions. They are included merely as a convenient, quick alternative to looking in paper or online reference sources for some of the technical terms I mention in my *Art of War* Guide. I do not claim that they should be considered any better than any others. In particular, I have not written them with the same attention to careful distinction as I have tried to give to writing the main part of this book and the Appendix.

Further, since readers who would want to use this glossary might be persons who are not specially familiar with computing or networking, and since there are not very many entries, I have arranged them in general conceptual order, rather than alphabetic order.

For readers who may want a suggestion about a useful reference source, at the present time (mid 2010) the online Wikipedia and Wiktionary (www.wikipedia.org, www.wiktionary.org) are one place to start, kind of like a gossipy neighbor, not always perfectly reliable but often enough having useful information or knowing where to find it.

* * *

YMMV: Your Mileage May Vary. A generic way of saying no claim is being made that the associated information is correct for all cases or for all persons. A common abbreviation in things written about computing, adopted from a legal escape clause phrase in automobile performance advertisements.

RFC: Request For Comment. A modern electronic computer is by itself hugely complex, and getting a bunch of them to work together adds greatly more complexity. In the development of computer networking, very many quite new processes had to be devised and agreed upon by all the people doing the development. People involved in working on a task would produce a statement of what they had figured out so far, and issue the statement as a request for comments about their ideas. This method is still followed. When a set of ideas is felt to be good enough to put into use, the last RFC on the topic is treated as a definitive statement of rules for how its topic is to work. The present authoritative repository of RFCs is maintained by the Internet Engineering Task Force, accessible at www.ietf.org/.

host: Any unit computer (form factor—such as desktop, laptop, handheld, etc, even embedded system microcontroller—is irrelevant), including ones being used as self-sufficient personal computers, servers, clients, etc.

sysadmin: Abbreviation for system(s) administrator, a person responsible for the effective functioning of a system of hosts. An idea of the details of this activity can be gotten from the book **Unix System Administration Handbook** by Evi Nemeth, Garth Snyder, Scott Seebass, and Trent R. Hein.

network, *subnet*, *internet*: Some hosts which are interconnected in such a way that they are able to communicate with each other. "Network" is the most generic term; "subnet" implies the existence of a larger network of which the subnet is a part, or at least of some separate network with which hosts in the subnet can communicate; "internet" generally refers to the existence of a number of networks among which intercommunication is possible, capitalized, it usually means the global Internet. (Although "World Wide Web" is sometimes used interchangeably with "Internet", the "Web" actually is the totality of interlinked information or services available on Internet hosts.)

NIC: Network Interface Card. The hardware via which a host connects to a network, also known as "network adapter". In modern equipment often not actually a card; includes built-in ethernet ports and wireless radios, removable cards and USB units, and so on.

address: An identifier for a host or some other kinds of equipment on a network, supposed to distinguish each uniquely from all others on the network. In TCP/IP networking, the basis of the Internet, an IP (internet protocol) address consists of punctuated numerical digits.

traffic: Communications over a network.

packet: Basic unit of network communication. Typically composed of a content or "payload" section, to which is prefixed a header section containing information about the packet itself and its content, and to which may be postfixed a trailer section. The size and content of the different parts of a packet are supposed to follow certain rules, depending on what the packet is supposed to be used for.

log: A record of some activity, such as traffic log (record of network traffic), system log (record of host operating system activity), and so on.

router: A device which connects networks to each other, routing traffic it receives to the network or host to which the traffic is addressed.

firewall: A device through which network traffic must pass, which examines the traffic and lets it pass or not depending on some characteristic(s) of the traffic.

NAT: Network Address Translation. A procedure by which subnet hosts communicating with wider networks are identified, in their traffic on the wider network, as having IP address(es) different from their actual addresses on their subnet.

LAN, *WAN*: Local Area Network, Wide Area Network. Roughly, a local area network is a network which is controlled by one organization and from which there may be restricted access to any other network; a wide area network is two or more interconnected LANs treated for some purpose as a single network.

covert channel: Means of communication exploiting the fact that information can be communicated by any structured variation of anything, as long as the variation can be translated into linguistic meaning at both ends of the communication. Typically much less efficient than ordinary linguistic communication, but also much less recognizable since not familiar to or expected by ordinary observers. (Electronic digital communication in general is itself actually an example of this basic principle, as linguistic information is translated into structured sequences of voltage variations transmitted through an usual communications channel. A channel is covert in this context when it does not follow usual public protocols for digital communication, including cases where the covert communication is not even via digital means.) The idea of covert channel is extended to any variation from which an aware observer can infer meaning—such a variation may also be called an "information leak".

phone home: Software, by itself without user action, initiating communication with some other host(s) specified by the producer of the software. Examples range from software automatically checking for new updates or for other kinds of programs, to registering its location or use with some recordkeeping system, to surreptitiously transmitting private information from its host, to facilitating remote tampering with the software itself or with its host.

RAID: Redundant Array of Independent Disks/Drives. A set of information storage media acting together a lot like a single disk or drive, whether by information being split among them or by information being duplicated among them or by both.

EMR: ElectroMagnetic Radiation. Radio waves, light, and so on. Pretty much any movement of electrons, including the electrons that make electronic computing work, produces some kind of EMR.

RFID: Radio Frequency ID. Identifying things by information gathered via radio signaling from tags on or in the things. The size of RFID tags has been decreasing and the information capacity increasing since they were first introduced. Recently (early 2007) a flat quadrangular RFID tag with width smaller than the thickness of a single human hair was announced.

GPS: Global Positioning System. The geo-locational system in which individual GPS units determine their location by referring to signals broadcast from some earth-orbiting satellites. Like all electronic devices, capabilities have been increasing and sizes have been decreasing.