

Glossary of Key Terms

A

Access control list (ACL) | A list of rules that permit or deny access based on a network address and/or port.

Active defense | A network defense strategy that emphasizes the ability to respond as attacks occur at varying levels of intensity against the right attackers, and using shared intelligence.

Active response | A network defense strategy that uses attacks and probes in response to attacks to attempt to stop an attack.

Activists | Individuals or organizations that seek to change opinions or effect political change through peaceful, nonviolent means.

Administrative privileges | Rights provided to an administrator that give control over the system or network.

Advanced persistent threat (APT) | A sophisticated cyberwarfare threat group characterized by advanced technical tools and a persistent focus on compromising targets thought to be of strategic value.

Analysis and Production | The phase of the intelligence cycle where intelligence analysts transform collected information into intelligence that satisfies the intelligence requests made by decision makers.

Anonymous | A hacktivist organization composed of many individuals. Anonymous has no set leaders, although some members act as leaders for specific actions or subgroups.

Application-aware firewalls | Firewalls that are able to read and analyze application protocols then apply rules based on the content of packets using those protocols.

Application whitelisting | A technological solution that uses known, allowed programs to run on trusted systems. It also prohibits unknown programs not on the whitelist from running.

Asymmetric encryption | An encryption algorithm that requires both a private and a public key, allowing secure key distribution, authentication, and nonrepudiation when combined with cryptographic hashes.

Asymmetric warfare | Warfare fought between opponents with significantly different capabilities or strategies. Guerrilla wars and insurrections are both examples of asymmetric warfare.

Authenticity | Whether a message or data is genuine and can be proven to be from the person it claims to be from.

Authority | The principle of influence that says individuals will often defer to someone perceived to have power granted by law, due to his or her position within an organization or because of his or her social leadership.

Availability | Whether an information system is accessible and usable when needed. A system without the ability to ensure availability may be offline or inaccessible. Availability is part of the C-I-A triad.

B

Backups | Copies of data used to provide disaster recovery and to help ensure the ability to restore systems to working order.

Baiting | A social engineering attack where the attacker creates a flash drive that contains malicious code and leaves it in a parking lot, lobby, or other location where a target is likely to discover it.

Baseline configuration | A defined configuration to which systems are expected to conform. It is often used as part of a security design to ensure that systems comply with required settings and configurations.

Black-hat hackers | Hackers who use their skills with malicious intent, seeking to gain unauthorized access to systems for financial gain, to advance a political agenda, or for other purposes.

Blacklisting | The process of creating a list of prohibited sites, software, users, or other items.

Bot | A system that has been compromised by an attacker and is attached to a command-and-control server.

Botnet | A collection of bots under the control of the same attacker that may be leveraged for a common purpose, such as a distributed denial of service attack.

Buffer overflow | A category of exploits that attempt to write to areas of memory beyond that reserved for a particular purpose in the hope that the system will execute the overwritten areas as programs.

C

Careto | The name given to an advanced persistent threat of unknown origin that infected systems from 2007 through its discovery in 2014.

Certificate authority (CA) | The authority responsible for issuing certificates in a public key infrastructure.

Certification | A process used to verify that a system, application, or device meets a known standard. Certifying bodies use a known, documented process to ensure that certified items meet those standards.

Checksums | Mathematical calculations used to verify that data is intact.

C-I-A triad | An information security model describing the relationship between confidentiality, integrity, and availability in relation to the security of systems and data.

Ciphers | Algorithms for encrypting or decrypting data or messages.

Ciphertext | The resulting data when plaintext is encrypted.

Civilian infrastructure | The infrastructure and systems used for civilian purposes. At times, this can include infrastructure used by the military for nonmilitary purposes, such as Facebook or Twitter.

Classification | The process of assigning a file or object security or sensitivity levels, or the levels of security or sensitivity assigned to a file or object.

Clone phishing | A phishing attack that uses a modified copy of a legitimate message in the hopes of prompting the recipient to visit a link or open a file.

Cloud computing | Computing using resources hosted elsewhere, usually in a shared, virtual environment, which may exist in multiple data centers around the world.

Code | A series of substitutions for letters or words.

Code Red | A computer worm that affected more than 350,000 systems running Microsoft Internet Information Server in 2001.

Collection | The phase of the intelligence cycle during which intelligence professionals use assets at their disposal to gather essential elements of information.

Command, Control, Communications, Computers, and Intelligence (C4I) | A U.S. Department of Defense strategy for integration of technology command, control, and information management.

Commitment and consistency | The principle of influence that states that once someone has made a commitment to a particular course of action, his or her future actions will likely be consistent with that committed decision.

Common Criteria | An international standard (ISO/IEC 15408) for computer security certification and testing.

Communications intelligence (COMINT) | The collection of communications between individuals for intelligence purposes. COMINT may include the collection of telephone calls, e-mail messages, and web communications.

Computer network attack (CNA) | One of the core capabilities of offensive information operations and cyberwarfare, consisting of actions taken through the use of computer networks to deny, corrupt, or destroy an adversary's information and/or information systems.

Computer network defense (CND) | Activities designed to protect, monitor, analyze, detect, and respond to unauthorized activity in friendly information systems and networks.

Computer network exploitation (CNE) |

Cyberespionage capabilities of the military that include the ability to infiltrate computer systems and steal sensitive information.

Confidentiality | The ability to prevent disclosure of information or data to unauthorized individuals or users. A system without the ability to provide assurance of confidentiality is likely to expose data. Confidentiality is part of the C-I-A triad.

Configuration management systems | Systems that monitor and maintain the configuration of workstations or other devices to a defined standard.

Control | A nation-state's ability to prevent or allow actions by units or organizations.

Controlled Unclassified Information (CUI) | A program employed by the U.S. government to protect and label sensitive information that is not classified.

Conventional warfare | Warfare between two nation-states, typically following the traditional rules of warfare or treaties like the Geneva Conventions.

Corporations | For-profit businesses that are organized by individuals and officially registered by a government.

Cryptanalysis | The discipline of studying and defeating encryption technology to gain access to the plaintext of encrypted messages.

Cryptocurrency | Electronic currency that relies on cryptographic algorithms to provide proof of payment and proof of value. Bitcoin and Litecoin are examples of cryptocurrencies.

Cryptosystem | The set of algorithms required to perform a specific type of encryption and decryption.

Cyberattacks | Nonkinetic offensive operations that are intended to cause some form of physical or electronic damage.

Cyber domain | The domain of warfare that encompasses all cyberwarfare operations. The cyber domain complements the traditional domains of land, sea, air, and space.

Cyberespionage | Intrusions onto computer systems and networks designed to steal sensitive information that may be used for military, political, or economic gain.

Cyberhygiene | A term used by the U.S. Department of Defense to describe the overall health and maintenance of a computer system, including patching, vulnerability scanning, and other good system administration techniques.

Cyberintelligence | Intelligence activities related to cyberthreats, including identifying and analyzing their existence and capabilities.

Cyber Kill Chain | A model used to describe the process of engaging in a cyberwarfare attack, from conducting reconnaissance through acting on strategic objectives.

Cyberwarfare | Acts of war that include a wide range of activities using information systems as weapons against an opposing force.

Cyberwarriors | Combatants in cyberwar, either formally or informally trained.

D

Damage containment | The process of limiting the impact of a successful attack as part of computer network defense.

Darknet | A segment of network space that is unused, but monitored. Traffic sent to darknets can be presumed to be hostile, or at least unwanted because no legitimate systems exist there.

Data Execution Prevention (DEP) | A technology that prevents the execution of code stored in certain parts of memory to protect against malware exploitation of buffer overflows.

Data labeling | The addition of flags or tags to data that provide information about the data, such as its classification, handling requirements, date of creation, or declassification date.

Data Lifecycle Management (DLM) | The use of policy and procedures to manage data throughout its life cycle from creation to deletion.

Declassified | A description of data that has been removed from a classification system.

Decryption | The process of decoding ciphertext, typically using a secret key.

Demilitarized zone (DMZ) | A special-purpose network designed to contain and isolate systems that offer public-facing services from other systems on the network.

Device integrity | The ability to ensure that a device has not been modified by unauthorized users or attackers.

Digital certificates | Electronic documents that are used to connect a public key and an individual, system, or other organization's identity.

Dissemination | The phase of the intelligence cycle that includes the delivery of finished intelligence products to decision makers and the integration of intelligence information into user processes.

Distributed control systems (DCSs) | Systems that use a combination of sensors and feedback systems to control and adjust processes as they receive feedback.

Distributed denial of service (DDoS) | A network attack conducted by many machines using their combined resources to consume resources on the targeted system or systems.

Doctrine | Military planning documents that provide commanders with a shared philosophy and language for military operations.

Domain | A domain name is used to represent a system or group of systems on the Internet. For example, example.com is a domain name, and security.example.com would be a subdomain of the example.com domain.

Downgraded | Data that has been moved from a higher classification level to a lower classification level, but which has not been declassified.

Drive encryption | Encryption of a full disk or volume (partition) of a drive.

Duqu | A computer worm discovered in 2011 that is believed to be an advanced variant of the Stuxnet worm used for reconnaissance against industrial control systems.

E

Economy of Force | The principle of warfare that states commanders should use the minimum amount of force necessary to achieve secondary objectives.

Electronic intelligence (ELINT) | The collection of electronic signals generated by nonhuman communications for intelligence purposes. ELINT includes the electronic emissions generated by radar systems, aircraft, ships, missiles, and other communications systems.

Electronic warfare | Information operations that include all military actions designed to use electromagnetic or directed energy to either control the electromagnetic spectrum or attack the enemy.

Eligible Receiver | The code name for a military cyberwarfare exercise that took place in 1997, raising awareness of the U.S. vulnerability to cyberwarfare attacks.

Encryption | The process of encoding ciphertext using an algorithm and a secret key.

Essential elements of information (EIs) | The specific pieces of information that may be collected to help answer the priority intelligence requirement.

F

File encryption | Encryption of one or more files.

Financial intelligence (FININT) | The collection of information about financial transactions that may be exploited for intelligence purposes.

Firewalls | Network security devices that use a group of rules known as a ruleset to allow or deny traffic from passing through them.

Flame | A computer worm discovered in 2012 that is believed to be a later version of Stuxnet and Duqu used to target Iranian computer systems.

FOXACID | The code name for a program designed to compromise targeted computer systems by tricking them into visiting infected Web sites.

G

Geneva Conventions | The primary treaty basis for the internationally accepted laws of war.

Geospatial intelligence (GEOINT) | The collection of information gathered through the use of photography, maps, and other information about terrain.

Gray-hat hackers | Hackers who use their skills to advise companies of system vulnerabilities, but perform their actions without permission.

Guerrilla warfare | A type of asymmetric warfare; fought between opponents with significantly different capabilities or strategies.

H

Hacker | An individual who exploits computer security weaknesses for fame, financial gain, or other purposes.

Hactivism | Political activism conducted via hacking or by using cyberwarfare techniques.

Hactivist | A cyberactivist who uses hacking for political or social protest and activism. Members of Anonymous, one of the most active hactivist groups, have also ventured into cybercrime activities.

Hashes | Algorithms that generate a fixed-length output given variable-length input. The fixed-length output is unique for each given set of input data and cannot be reversed to determine the original input.

Heuristics | A behavior-based detection that focuses on how a program acts and what it does to determine if it is a threat.

Honeynets | Networks or groups of systems set up to allow attackers to attack a number of systems, which then capture information about the attacks for defenders to analyze.

Honeytrap | A fake or decoy system designed to allow attackers to successfully compromise it while providing information about the tools and techniques the attackers used.

Host intrusion prevention system (HIPS) | A software-based system that attempts to detect and prevent attacks before they can reach the system they are installed on.

Human intelligence (HUMINT) | The collection of information from interactions among people.

I

Imagery intelligence (IMINT) | The collection of photographic information by aircraft or satellites overflying an area of intelligence interest.

Indicators | Actions taken by friendly forces and publicly available information that reveal critical information to the enemy.

Industrial control system (ICS) | A term that covers DCS, SCADA, and PLC systems used to control and oversee industrial processes and systems.

Industrial espionage | Intelligence activities conducted for business purposes, rather than for national security reasons.

Information assurance | A discipline that covers the protection of information and the management of risks to that information.

Information operations | Actions taken to affect adversary information and information systems while defending your own information and information systems.

Information warfare | Information operations conducted during a time of crisis or conflict to achieve or promote specific objectives over a specific adversary.

Integrity | The ability to prevent unauthorized modification of data, settings, or other elements of a device or system. Integrity is part of the C-I-A triad.

Intelligence | The collection, analysis, and dissemination of information about the capabilities, plans, intentions, and operations of an adversary.

Intelligence cycle | A model used to describe the process of intelligence operations with five phases: Planning and Direction, Collection, Processing and Exploitation, Analysis and Production, and Dissemination.

Intelligence gathering | Information operations actions that include efforts to gather information about an adversary's capabilities, plans, and actions.

Intelligence requirements | General or specific subjects for which a decision maker has determined that there is a need for the collection of information or the production of intelligence.

International organized crime | Self-perpetuating associations of individuals who operate internationally for the purpose of obtaining power, influence, monetary, and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence.

Internet of Things | A term used to refer to the large number of networked devices that can now connect to the Internet.

Intrusion detection systems (IDSs) | Network- or host-based network protection systems that detect and report attacks.

Intrusion prevention systems (IPSs) | Network- or host-based network protection systems that detect and can prevent attacks from passing through them.

Irregular warfare | A form of warfare characterized as a violent struggle among state and nonstate actors for legitimacy and influence over the relevant population(s).

J

Jurisdiction | A nation-state's territory and areas where it is the sovereign power.

Jus ad bellum | Latin for "the right to war"; a set of criteria that defines when war is allowed.

Jus in bello | Latin for "laws of war"; laws of warfare like the Geneva Conventions.

K

Key | The part of an encryption algorithm that controls the output of the algorithm. Keys are kept secret, as they can be used to encrypt or decrypt information using the algorithm.

Key distribution | The method by which keys are securely provided to those who need them.

Key pair | A private and a public key that are used by an individual or other entity in asymmetric encryption.

Kill chain | A model describing the process followed during an attack, from identifying appropriate targets to assessing the damage after an attack.

Kinetic warfare | Traditional warfare that is active, such as bombing and killing opposing troops.

L

Legitimacy | The principle of joint operations that states military operations must take place within the confines of appropriate authority.

Liking | The principle of influence that says people are more apt to be influenced by people who they know and appreciate.

Local area networks (LANs) | Networks that connect systems within a limited or nearby area, such as a building or campus.

M

Malware | Malicious software, such as a virus, Trojan, or other software designed to attack or take over a computer or system.

Maneuver | The principle of warfare that states applying power in a flexible manner keeps the adversary off guard.

Mass | The principle of warfare that states military commanders should concentrate their combat forces at the decisive time and location.

Mean time between failure (MTBF) | A measure of the reliability of devices and drives; the average time until the device fails.

Measurement and signature intelligence (MASINT) | The collection of information gathered from unintended electromagnetic emissions generated by a target.

Mercenaries | Combatants who are involved in a conflict for personal gain, and who are not members of an involved party's military or other governmental functions.

Message digests | Cryptographic functions that protect the integrity of a message by allowing you to check that the message has not changed.

Metadata | Data about communications other than the actual content of the communication. For example, metadata for a telephone call may include the called number, calling number, and length of the call.

Military deception | Actions designed to mislead adversary forces about the operational capabilities, plans, and actions of friendly forces.

Mission assurance | The combination of risk management, system engineering, design, quality assurance, and management to ensure that systems and networks remain available and usable.

Mission Assurance Categories (MAC) | A U.S. Department of Defense mission assurance categorization scheme ranging from MAC I, which provides extremely high levels of integrity and availability, to MAC III, which matches common industry practices for integrity and availability of data and systems.

Moonlight Maze | The code name for a series of attacks, believed to be of Russian origin, that began targeting U.S. government systems in 1998.

N

Nation-states | Formally recognized countries or nations.

Network address translation (NAT) | A technology that allows one or more addresses to be used by a group of systems inside of a network without exposing their internal addresses to the outside world.

Network admissions control (NAC) | A system that requires systems to authenticate and/or provide proof that they meet required configuration standards before connecting to a network.

Network attacks | Attacks conducted across or via a network.

Network enclave | A separated portion of an internal network. Network enclaves are used to separate sections of the network based on usage, data, or the security requirements of systems or devices on that segment.

New York Times Co. v. United States | U.S. Supreme Court decision that legitimized the constitutional basis for publishing the *Pentagon Papers* under the press's First Amendment protections.

Nongovernmental organizations (NGOs) | Organizations that exist outside of the context of a government or a for-profit corporation.

Nonkinetic warfare | Cyber and electronic warfare.

Nonrepudiation | The ability in a communication to ensure that the sender cannot claim that he or she did not send a message.

Nonstate actors | Individuals or groups that seek to participate in cyberwarfare but do so independently, without the endorsement of a national government.

O

Objective | The principle of warfare that states every military action should have a clearly defined and articulated purpose.

Offensive | The principle of warfare that states military commanders must seize, retain, and exploit the initiative.

Open source intelligence (OSINT) | The collection of publicly available information to satisfy intelligence requirements.

Operation Aurora | A series of cyberattacks launched by Chinese sources against Google and other American companies in 2009.

Operational level | The level of warfare that links strategy and tactics through the planning and execution of operations.

Operations security (OPSEC) | Activities designed to deny an adversary access to information about friendly forces that would reveal capabilities, plans, or actions.

Opportunistic attack | An attack type that uses a brute-force approach against thousands or millions of targets in an attempt to find a handful of vulnerable systems.

Organ | Every nation-state agency, person, or entity that is part of the official government or associated bodies of a nation-state.

P

Packet filter firewalls | Firewalls that provide very basic filtering capabilities based on the network address, port, or protocol that traffic is coming from or going to.

Penetration testing | Security testing that involves attacking systems to attempt to gain access or control as part of a test.

Pentagon Papers | The collection of classified U.S. government documents related to the Vietnam War published by the *New York Times* in 1971 as part of a famous leak of embarrassing government records.

Perseverance | The principle of joint operations that states military commanders must take measures to ensure that the commitment exists to achieve the desired end state.

Phishing | A social engineering attack where the attacker sends the victim an electronic message (via e-mail, text, or other means) attempting to solicit sensitive information from the victim.

Pivot | Attackers use a technique known as pivoting when they compromise a system inside of a defensive layer. They attack other systems inside of the segment or security zone they are in, using those systems to attempt to gain more access in other zones or to access additional data and systems.

Plaintext | Unencrypted text or data.

Planning and Direction | The phase of the intelligence cycle that includes the identification of intelligence requirements, the development of an intelligence architecture, the design of a collection plan, and the issuance of collection requests.

Poison Ivy | A remote access trojan developed in 2005 and still in use today to remotely control systems infiltrated by hackers.

Port scanning | The process of scanning systems to determine what services they are offering on numbered ports.

Pretexting | A social engineering attack where the attacker creates a false set of circumstances and uses them to convince the target to take some form of action.

Priority intelligence requirements (PIRs) | The questions identified by decision makers as needing critical attention from intelligence operations.

Processing and Exploitation | The phase of the intelligence cycle during which data collected by intelligence assets in the Collection phase is transformed into information useful to intelligence analysts.

Programmable logic controllers (PLCs) | Special-purpose computers designed to handle specialized input and output systems.

Psychological operations (PSYOPs) | Military operations planned to convey selected information and indicators to foreign governments, organizations, groups, and individuals in order to influence their emotions, motives, objective reasoning, and behavior.

Public key encryption | A method of encryption that can provide all four critical requirements: confidentiality, message integrity, authentication, and nonrepudiation. *See* asymmetric encryption.

Public key infrastructure (PKI) | The software, hardware, policies, procedures, and staff needed to create, manage, distribute, and use digital certificates.

Q

Quantum cryptography | Cryptography that uses quantum mechanics to perform cryptographic tasks like encrypting and decrypting data or providing secure key exchange.

R

Ransomware | Malicious computer software that takes over a system, encrypting files with a secret key rendering them inaccessible to the legitimate user until he or she pays a ransom.

Reciprocity | A relationship between two people that involves the exchange of goods or services of approximately equal value.

Redacting | The removal of information from a document or data. Paper records are often redacted using a black marker, whereas digital documents often have words or sections replaced with blanks or black boxes.

Red Cell | The U.S. government's title for opposing forces in exercises, including specialized teams that attack networks and other cyberinfrastructure.

Red team | *See* Red Cell.

Redundancy | Providing multiple copies of data, multiple servers, or otherwise providing multiple versions of a system or data to ensure availability.

Registration authority (RA) | The organization or individual responsible for verifying the identities of entities requesting certificates in a PKI.

Remote access trojan (RAT) | Malicious software that allows continued access to a compromised system from a remote location.

Restraint | The principle of joint operations that states that, while conducting military operations, commanders should limit collateral damage and prevent the unnecessary use of force.

Routers | Network devices used to interconnect networks and direct traffic between them.

Rulesets | The list of rules that define what traffic is allowed through or stopped by a firewall or other network security device.

Ruse | A trick or act intended to fool an enemy during wartime.

S

Sanitizing | The removal of all data from a drive or other media.

Script kiddies | Hackers who do not discover vulnerabilities on their own but instead download exploit scripts written by others and run them against target systems without a real understanding of the technical details behind the attack.

Secure Sockets Layer (SSL) | The predecessor to TLS, a security protocol for the creation and use of an encrypted link between a client and a server.

Security | The principle of warfare that states commanders must never allow enemy forces to gain an advantage.

Security Information and Event Management (SIEM) | A network security system that gathers data about attacks as well as security information from logs and other data sources, then correlates that data for security practitioners.

Self-defending network | A network that modifies itself to protect against attacks as they occur.

Semi-targeted attack | An attack that seeks to infiltrate a specific organization or type of target but not a specific individual.

Senior Suter | The code name for a U.S. Air Force program designed to manipulate enemy air defense systems.

Side-channel attacks | In encryption, attacks that target the physical implementation of encryption, such as measuring the amount of power a cryptographic processor draws to determine what calculation it is performing.

Signals intelligence (SIGINT) | The collection of intelligence information through the interception of communications and other electronic signals.

Signature-based detection | A detection capability that uses details of a file or program to match it to a list of known files. Malware detection systems often use cryptographic hashing and other techniques to perform this function.

Simplicity | The principle of warfare that states military plans should be simple, clear, and concise to reduce confusion and misunderstanding.

Simulations | Exercises intended to simulate actual attacks to test processes and procedures.

Social engineering | The art of manipulating human behavior through social influence tactics in order to achieve a desired behavior.

Social proof | The principle of influence that says an individual in a social situation who is unsure how to act will likely follow the example of the crowd and behave in the same way as the people around him or her.

Software testing | Testing via either human or programmatic means that attempts to validate a program's function and to determine if it has any flaws.

Solar Sunrise | The code name for cyberattacks launched in 1998 by three teenagers against computer systems operated by the U.S. government.

Sovereignty | A nation's right to be the final authority over its territory, citizens, and resources.

Spear phishing | A phishing attack that is targeted at a specific individual and uses personal information to add legitimacy to the phishing message.

SQL Slammer | A computer worm that affected more than 75,000 systems running Microsoft SQL Server in 2003.

Stateful packet inspection firewalls | Firewalls that track the state of traffic between systems, allowing ongoing permitted traffic to pass through without additional inspection.

Strategic level | The level of warfare that involves national-level policies and military strategies across an entire theater of operations.

Stuxnet | The computer worm allegedly used by a joint U.S.-Israeli operation to destroy Iranian uranium enrichment centrifuges in 2010.

Supervisory control and data acquisition

(SCADA) | Systems used to monitor and control remote equipment.

Surprise | The principle of warfare that states that, when attacking, military forces should strike the enemy at an unexpected time or place.

Symmetric encryption | Encryption in which the same secret key is used for both decryption and encryption.

T

Tactical level | The level of warfare concerned with the employment and ordered arrangement of forces in relation to each other.

Tallinn Manual | An in-depth analysis of the current international law in the context of cyberwarfare created for the United Nations.

Terrorists | Individuals or organizations that seek to change opinions or effect political change through violent, unlawful means.

Tiger teams | Teams assigned to solve a specific problem. In security testing, a tiger team is assigned to identify and possibly fix flaws and vulnerabilities.

Titan Rain | The code name for the investigation into a series of computer intrusions launched against U.S. government systems from Chinese Web servers from 2003 through 2005.

Total warfare | Warfare fought without any restrictions or boundaries. Total warfare is fought entirely to win, and ignores normal conventions regarding targeting of civilians, use of some types of weapons, and other restrictions.

Traditional warfare | A form of warfare consisting of large-scale conflict between nations or groups of nations that is characterized as a violent struggle for domination between nation-states or coalitions and alliances of nation-states.

Transport Layer Security (TLS) | A security protocol for the creation and use of an encrypted link between a client and a server. TLS is most often associated with secure Web traffic.

Treachery | Harmful trickery used in wartime that can result in death or injury.

Trusted Platform Module (TPM) | A cryptographic processor that provides encryption capabilities as well as helping to prove a system's identity when decrypting a drive. Also commonly called a TPM chip.

U

Unconventional warfare | Warfare fought primarily on a psychological level, with the goal of changing how an enemy feels about the conflict. Unconventional warfare attempts to persuade the enemy to surrender or negotiate peace.

Unity of Command | The principle of warfare that states a single commander should be responsible for achieving each military objective.

U.S. Cyber Command (USCYBERCOM) | A major command of the U.S. military organized to operate in the cyber domain.

V

Virtualization | The creation of virtual, rather than physical, environments for servers and devices. Virtualization can allow multiple virtual servers or systems to run on the same hardware that would normally host a single system or device.

Virtual LAN (VLAN) | A virtual local area network, or logically separated network created through software-based tags on a network.

Virtual private network (VPN) | A network constructed through other networks that relies on encryption or encapsulation to keep its content separate.

Vulnerabilities | Flaws in a system, software, network, or device that can leave it vulnerable to attack or exploit.

Vulnerability scanning | A scanning process conducted against systems and devices to identify any vulnerabilities in their services or software.

W

War | Socially sanctioned violence to achieve a political purpose.

War games | Exercises intended to simulate actual attacks to test processes and procedures.

White-hat hackers | Benevolent security practitioners who use their hacking skills for good purposes, seeking to secure the information systems of their employers or consulting clients.

Whitelisting | The process of creating a list of allowed items, typically programs, Web sites, individuals, or other groups.

Wide area networks (WANs) | Networks that interconnect over a broad area, such as those across geographic regions.

Window of vulnerability | The time that exists between when a vulnerability is discovered and when the software vendor releases a patch to correct the vulnerability.

Worm | A piece of malicious software that is able to spread between computer systems without any human intervention.

Z

Zero-day attacks | Attacks that occur during the window of vulnerability when no patch is available to successfully defend against the attack.

Zero-day vulnerabilities | Vulnerabilities in a computer system or network that are unknown to anyone other than the attacker, making it extremely difficult to defend against.

