DECEMBER 11, 2017

DEPARTMENT OF THE NAVY CYBER GLOSSARY: TERMS AND DEFINITIONS

DEVELOPED BY OPNAV N2N6 IN COLLABORATION WITH DON CIO AND USMC C4 CYBERSECURITY DIRECTORATES

Sources: Various, including Joint Pub 3-12 Cyberspace Operations

ABBREVIATIONS AND ACRONYMS

C10F – Commander, U.S. TENTH Fleet

CDRUSCYBERCOM - Commander, United States Cyber Command

CDRUSSTRATCOM - Commander, United States Strategic Command

CI - counterintelligence

CI/KR - critical infrastructure/key resources

CIO - chief information officer

CNCI - Comprehensive National Cybersecurity Initiative

CNE - computer network exploitation

CO - cyberspace operations

CS - cybersecurity

CSE - cyberspace support element

DCI - defense critical infrastructure

DCO - defensive cyberspace operations

DCO-RA - defensive cyberspace operations response actions

DISN – Defense Information Systems Network

DOD - Department of Defense

DODD - Department of Defense directive

DODI - Department of Defense instruction

DODIN - Department of Defense Information Networks

DSCA - defense support of civil authorities

EA - electronic attack

EMS - electromagnetic spectrum

EW - electronic warfare

FCC - Fleet Cyber Command

FOC – Full Operational Capability

ICT - information and communications technology

IM - information management

IO - information operations

IOC - Initial Operating Capability

IP - internet protocol

ISP - Internet Service Provider

ISR - intelligence, surveillance, and reconnaissance

IT - information technology

IW – Information Warfare

JCC - joint cyberspace center

JWICS - Joint Worldwide Intelligence Communications System

MILDEC - military deception

MISO - military information support operations

NCSD - National Cyber Security Division (DHS)

NIPRNET - Non-classified Internet Protocol Router Network

NMS-CO - National Military Strategy for Cyberspace Operations

OCO - offensive cyberspace operations

OPM - Office of Personnel Management

OSI - Open System Interconnection

PPD - Presidential policy directive

PTE - Persistent Training Environment

SATCOM - satellite communications

SIGINT - signals intelligence

SIPRNET – Secret Internet Protocol Router Network

STO - special technical operations

TCPED - tasking, collection, processing, exploitation, and dissemination

TFCA - Task Force Cyber Awakening

URL - uniform resource locater

USCYBERCOM - United States Cyber Command

USD(P) - Under Secretary of Defense for Policy

TERMS AND DEFINITIONS

Adware – is free software that is supported by advertisements. Common adware programs are toolbars that sit on your desktop or work in conjunction with your Web browser. They include features like advanced searching of the Web or your hard drive and better organization of your bookmarks and shortcuts. Adware can also be more advanced programs such as games or utilities. They are free to use, but require you to watch advertisements as long as the programs are open. (www.techterms.com)

Black Hat Hacker – a black hat hacker is an individual with extensive computer knowledge whose purpose is to breach or bypass internet security. Black hat hackers are also known as crackers or dark-side hackers. (http://www.pctools.com/security-news/blackhat-hacker/)

Blue Team – 1. The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).
2. A group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cybersecurity readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems (CNSSI 4009).

BotNet – a group of computers that are controlled from a single source and run related software programs and scripts – the term usually refers to multiple computers that have been infected with malicious software. (www.techterms.com)

Brute Force Attack – Refers to a programming style that does not include any shortcuts to improve performance, but instead relies on sheer computing power to try all possibilities until the solution to a problem is found. (www.webopedia.com)

Cyberspace Capability – a device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace. (see JP 3-12)

Cloud Computing – a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST SP 800-145)

Critical Infrastructure – System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (CNSSI 4009) (see JP 3-12)

Cyber Attack – The term "cyber attack" is often used by the media, the public, and even USG officials (incorrectly) to describe the full range of unauthorized/unlawful actions in cyberspace. Such actions can range from stealing a celebrity's personal photos or stealing credit card information to causing a website to crash, compromising sensitive information, or putting critical infrastructure at risk. Only National Authority should characterize a cyberspace operation as a cyberspace attack and this determination will be based on the scale and effects of the cyberspace operation and focus on the actual level of harm, or potential harm, and clearly expressed qualitative elements of the cyberspace operation. The term "attack" carries with it significant legal and national security implications. Uses of force, to include through cyberspace, violate international law, and an armed attack gives rise to a nation's right to self-defense. In the cyberspace context, the focus should be on the scale and effects of an adversary's cyberspace operation. *JP 3-12 defines cyberspace attack tactically as cyberspace actions which create various direct denial effects (i.e. degradation, disruption, or destruction) and manipulation that leads to denial.* From a strategic perspective, labeling an action as a cyberspace attack has greater implications, and could lead to the perception that the United States views the action as rising to the level of warranting military actions in self-defense (whether kinetic or non-kinetic). Thus far, no malicious cyber activity has risen to the level of a cyber attack. Many events we have seen so far, such as OMB, are espionage activities, which are not in violation of international law and are not uses of force and/or armed attacks. Given the significant legal and national security implications, Navy personnel should avoid using the term "cyber attack" to refer to any malicious activity in cyberspace unless the cyberspace event has been determined by National Authority to be a cyber attack warranting military actions in self-defense.

Cyberspace Attack - Cyberspace actions that create various direct denial effects (i.e. degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains. (JP 3-12)

Cyber incident – Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein. (CNSSI 4009)

Cyber-persona Layer –The cyber-persona layer, an individual's or groups' online identity (ies), holds important implications for joint forces in terms of positive target identification and affiliation, and activity attribution. (see JP 3-12)

CYBERSAFE – patterned after the SUBSAFE program. "CYBERSAFE" applies to a specific set of requirements for design, procurement, material controls, maintenance and operating procedures, along with the change in organizational culture and crew proficiency required to institute these requirements, applied to a selected subset of platform system elements or components for which a failure caused by a cyber-attack would result in loss of critical mission capability, mission critical equipment, and/or personal injury.

Cybersecurity – Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (NSPD-54/HSPD-23)

Cyberspace – The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. (NSPD-54/HSPD-23)

Cyberspace Operations – The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-0)

Cyberspace Superiority – The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary.

Cyber Tools – A program used for software development or system maintenance. Virtually any program or utility that helps programmers or users develop applications or maintain their computers can be called a tool. (http://www.pcmag.com/encyclopedia/term/52979/tool)

Darknet – Short for dark Internet, in file sharing terminology, a darknet is an Internet or private network, where information and content are shared by darknet participants anonymously. (http://www.webopedia.com/TERM/D/darknet.html)

Defensive Cyberspace Operation Response Action – Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems. Also called DCO-RA. (DoD JP 3-12)

Defensive Cyberspace Operations – Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Also called DCO. (DoD JP 3-12)

Defense Information Systems Network — The integrated network, centrally managed and configured by the Defense Information Systems Agency to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services for all Department of Defense activities. Also called DISN. (JP 6-0)

Degrade – To deny access (a function of amount) to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation must be specified. If a specific time is required, it can be specified. (see JP 3-12)

Deny – To degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time. Denial prevents adversary use of resources. (see JP 3-12)

DOD Cyber Strategy – http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

DOD Information Networks – The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Also called DODIN. (JP 1-02, JP 3-12)

DOD Information Network operations – Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. (JP 3-12)

Denial of Service– The prevention of authorized access to resources or the delaying of time- critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) Also called DoS. (NIST SP 800-27 Rev A)

Distributed Denial of Service – A denial of service technique that uses numerous hosts to perform the attack. Also called DDoS. (CNSSI 4009)

Doxing – the process of gathering information about a person or business using online public sources such as social media profiles, reverse phone lookup and search engines. Doxing typically leads to an anonymous person's identity being revealed**.** (www.webopedia.com)

Disrupt – To completely but temporarily deny (a function of time) access to, or operation of, a target for a period of time. (see JP 3-12)

Disruption - An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). (NIST SP 800-34 REV 1)

Encryption – The cryptographic transformation of data to produce ciphertext. (ISO/IEC 7498-2)

Exfiltrate – Data exfiltration, also called data extrusion, is the unauthorized transfer of data from a computer. (http://whatis.techtarget.com/definition/data-exfiltration-data-extrusion)

Exfiltration - The unauthorized transfer of information from an information system. (NIST SP 800-53 Rev 4)

Hash – is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. (http://www.webopedia.com/TERM/H/hashing.html)

Hashing - The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. (NIST SP 800-72)

Hacktivist – Formed by combining "hack" with "activism," hacktivism is the act of hacking into a Web site or computer system in order to communicate a politically or socially motivated message. For the hacktivist, it is an Internet-enabled way to practice civil disobedience and protest. (www.webopedia.com)

Information Assurance – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non- repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. Also called IA. (CNSSI 4009)

Insider Threat – The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities. (CNSSI 4009)

Internet of Things (IoT) – The term Internet of things refers to devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet. "Internet of things: privacy and security in a connected world," (United States Federal Trade Commission, January 2015)

Logical Network Layer – constitutes an abstraction of the physical network layer, depicting how nodes in the physical dimension of the information environment logically relate to one another to form entities in cyberspace. It is the first point where the connection to the physical dimension of the information environment is lost. (see JP 3-12)

Malware – "malicious software" is considered an annoying or harmful type of software intended to secretly access a device without the user's knowledge. Types of malware include spyware, adware, phishing, viruses, trojan horses, worms, rootkits, ransomware and browser hijackers. (https://www.avast.com/c-malware)

Malware – See malicious code and malicious logic. (CNSSI 4009)

Malicious Code – Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. (NIST SP 800-53 Rev 4)

Malicious Logic – Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. (IETF RFC 4949 Ver 2)

Manipulate – To control or change the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives. (see JP 3-12)

Mission Assurance – A process to protect or ensure the continued function and resilience of capabilities and assets - including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains - critical to the performance of DoD MEFs in any operating environment or condition.
(http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf)

Offensive Cyberspace Operations - Cyberspace operations intended to project power by the application of force in or through cyberspace. Also called OCO. (DoD JP 3-12)

Packet – a small amount of computer data sent over a network. Each packet contains the address of its origin and destination, and information that connects it to the related packets being sent.

Packet Sniffer – Software that observes and records network traffic. (CNSSI 4009)

Payload – A payload refers to the component of a computer virus that executes a malicious activity. (https://www.techopedia.com/definition/5381/payload)

Phishing – A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. (IETF RFC 4949 Ver 2)

Physical Network Layer – layer is the medium where the data travels. It is the first point of reference for determining jurisdiction and application of authorities. It is also the primary layer for geospatial intelligence, which can also contribute useful targeting data in cyberspace. (see JP 3-12)

Public Key Infrastructure (PKI) – The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates. (CNSSI 1300)

Public Facing Internet – Available to the general public
(http://www.pcmag.com/encyclopedia/term/66440/public-facing)

Red Team – A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team. (CNSSI 4009)

Rootkit – A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means. (CNSSI 4009)

SECRET Internet Protocol Router Network - The worldwide SECRET-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. Also called **SIPRNET.** (JP 1-02. SOURCE: JP 6-0)

Secure socket layer (SSL) – A protocol used for protecting private information during transmission via the Internet. Note: SSL works by using the service public key to encrypt a secret key that is used to encrypt the data that is transferred over the SSL session. Most web browsers support SSL and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:". The default port for SSL is 443. (CNSSI 4009)

Significant Consequences – Loss of life, significant responsive actions against the United States, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States. (PPD 20)

Significant Cyber Incident – A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people (see PPD-41).

Script Kiddie – is a person, normally someone who is not technologically sophisticated, who randomly seeks out a specific weakness over the Internet in order to gain root access to a system. (www.webopedia.com)

Social Engineering – An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. (NIST SP 800-61 Rev 2)

Spear Phishing – A colloquial term that can be used to describe any highly targeted phishing attack. (CNSSI 4009)

Spoofing – 1. Faking the sending address of a transmission to gain illegal entry into a secure system. 2. The deliberate inducement of a user or resource to take incorrect action.
Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. (CNSSI 4009)

System Administrator – Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures. (CNSSI 4009)

Trojan Horse – A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (CNSSI 4009)

Virtual private network (VPN) – Protected information system link utilizing tunneling, security controls (see information assurance (IA)), and endpoint address translation giving the impression of a dedicated line. (CNSSI 4009)

Whaling – A specific kind of phishing that targets high-ranking members of organizations. (CNSSI 4009)

White/Ethical Hacking – A white hat hacker is a computer security specialist who breaks into protected systems and networks to test and asses their security. White hat hackers use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them. (https://www.techopedia.com/definition/10349/white-hat-hacker)

Worm – A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. (CNSSI 4009)

Zero Day – A previously unknown vulnerability that leaves users with no time to mitigate before potential or actual exploitation. As FireEye defines it: "A zero-day vulnerability, at its core, is a flaw. It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. In fact, a zero-day exploit leaves NO opportunity for detection ... at first." (https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html)

Zero Day Attack - An attack that exploits a previously unknown hardware, firmware, or software vulnerability. (CNSSI 4009)