THE VICE CHAIRMAN OF THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20318-9999

MEMORANDUM FOR CHIEFS OF THE MILITARY SERVICES
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTORS OF THE JOINT STAFF DIRECTORATES

Subject: Joint Terminology for Cyberspace Operations

1. (U) On behalf of the Chairman, I am pleased to announce a further step in the development of cyberspace as a war-fighting domain—a standard joint cyber operations (CO) lexicon. Recent efforts in both Joint and inter-agency channels have highlighted the inadequacy of current terminology to describe our CO capabilities and missions. Though the language of Computer Network Operations, developed in the Information Operations context, has served us well, CO has matured to the point where it should be aligned with the other domains.

2. (U) The military has developed a common joint vocabulary to describe mission sets in terms of objective, limitations, and authorities involved. Terms such as "defensive counter-air" provide specific data about a mission: that it is defensive in intent—responding to an attack or imminent attack; that it targets the adversary's air capabilities; and that it involves the use of friendly air assets to counter the attack. In contrast, "computer network attack" can describe anything from corrupting a database to destroying an electrical power grid, to responding in self-defense against an attack on our own critical cyber assets. In short, cyber's unique vocabulary doesn't discretely describe the nuances of its mission sets, lend itself to established legal interpretations of authorities and limitations, or reflect the standardized vernacular of the other domains.

3. (U) For these reasons, I have tasked the Joint Staff to develop the attached lexicon to align CO vocabulary with standard joint terminology. This lexicon will be used as the starting point for normalizing terms in all cyber-related documents, instructions, CONOPS, and publications as they come up for review.

5. (U) My POC is LtCol McPhillips, USMC, J-3, Computer Network Operations Division; 703-571-1991, christopher.mcphillips@js.smil.mil.

JAMES E. CARTWRIGHT
General, United States Marine Corps
Vice Chairman
of the Joint Chiefs of Staff

Atch: Cyberspace Operations Lexicon

Attachment 1

Cyberspace Operations Lexicon

The following definitions align key cyberspace operations (CO) concepts with doctrinally accepted terms and definitions used in the other joint operational domains. For explanatory purposes. in each case, the current **Information Operations (IO) doctrinal definition for some aspect of CO** is presented, followed by its **conventional analogue, if any**, and the **current terminology it would replace**. Where an existing JP 1-02 doctrinal definition is applicable as written or with very minor modifications, that definition is used with the modification, if any, noted.

Note 1: Because IO doctrine uses just three terms (CNA, CNE, and CND) to encompass all mission areas, each of those terms is replaced here by more than one standard joint term, reflecting the broad array of discrete missions that comprise CO as they are executed today.

Note 2: This lexicon does not attempt to include every cyber-related term, but rather is focused on those for which the current cyber terminology does not align with an analogous traditional military term. Thus many terms, especially those related to NetOps, are not captured here because they reflect missions that have no analogue in the other domains—those terms are unaffected by this lexicon, but remain important to any comprehensive understanding of cyberspace operations.

---

1. **Advance Force Operations** - An operation which precedes the main effort in an objective area in order to prepare the objective for the main assault by conducting such operations as reconnaissance, seizure of supporting positions—including key network systems or nodes—pre-emplacement or clearing of weapons--such as minesweeping, preliminary bombardment, underwater demolitions, or cyber accesses and/or weapon implants —and air support.

   *(**See: Advance Force Operations (DOD, NATO).** An operation which precedes the main effort in an objective area in order to prepare the objective for the main assault by conducting such operations as reconnaissance, seizure of supporting positions, minesweeping, preliminary bombardment, underwater demolitions, and air support.)*

   Replaces: CNE when used to describe cyberspace operations intended to support/facilitate a specific planned operation or set of operations via clandestine means, e.g., by delivery of software payloads that may facilitate preparation of the battlespace and/or provide effects in support of an operation

---

2. **Aim Point** (Derived from Air Warfare TTPs)**:** After compensation for such factors as course, speed, turbulence, target and /or terrain characteristics, target depth/elevation, and weapon characteristics, the point at which a weapon is aimed in order to achieve the desired effect at the target location. Multiple aim points may be assigned to a particular target location in order to multiply or complement the effects of a single weapon or propagate those effects to a target location not directly accessible to the

weapon. If the target can only be affected indirectly, a geographically separated aim point, such as a supporting facility or component, may be selected in order to achieve the desired effect at the target location.

Replaces: n/a

---

3. **Collateral Effect** – unintentional or incidental effects including, but not limited to, injury or damage to persons or objects that would not be lawful military targets under the circumstances ruling at the time. Includes effects on civilian or dual-use computers, networks, information, or infrastructure. Such effects are not unlawful as long as they are not excessive in light of the overall military advantage anticipated from the activity. In cyberspace operations, Collateral Effects are categorized as:

   - "High": Substantial adverse effects on persons or property that are not lawful targets from which there is a reasonable probability of loss of life, serious injury, or serious adverse effect on the affected nation's national security, economic security, public safety, or any combination of such effects.
   - "Medium": substantial adverse effects on persons or property that are not lawful targets.
   - "Low": Temporary, minimal or intermittent effects on persons or property that are not lawful targets.
   - "No": Only adversary persons and computers, computer-controlled networks, and/or information and information systems are adversely affected.

   *(**See: Collateral Damage (JP 1-02)** - unintentional or incidental injury or damage to persons or objects that would not be lawful military targets under the circumstances ruling at the time. Such damage is not unlawful as long as it is not excessive in light of the overall military advantage anticipated from the attack).*

   Replaces: n/a.

---

4. **Computer Network Attack (CNA) –** (DOD) A category of fires employed for offensive purposes in which actions are taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/ networks themselves. The ultimate intended effect is not necessarily on the targeted system itself, but may support a larger effort, such as information operations or counter-terrorism, e.g., altering or spoofing specific communications or gaining or denying access to adversary communications or logistics channels.

   *(**Note:** This definition modifies the current definition of CNA to 1) clearly identify it as a form of offensive fires, 2) differentiate CNA from counter-cyber ops which specifically target the adversary's use of the cyber domain, and 3) identify CNA as a key component in IO and related efforts.)*

   Replaces: Existing definition of CNA (see note above)

5. **Computer Network Exploitation (CNE) –** (DOD) Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data about target or adversary automated information systems or networks. See also computer network attack; computer network defense; computer network operations.

   *(**Note:** In order to support the effort to more finely parse intelligence and enabling activities in cyberspace, the definition above changes one word in the current definition of CNE from JP 1-02 "from target or adversary systems" becomes "about target or adversary systems." This change differentiates CNE from ISR conducted via cyber means (i.e., SIGINT.) Collateral Damage (JP 1-02)*

   Replaces: N/A –slightly modifies existing definition of CNE (see note above)

---

6. **Counter-cyber (CC)-** A mission that integrates offensive and defensive operations to attain and maintain a desired degree of cyberspace superiority. Counter-cyber missions are designed to disrupt, negate, and/or destroy adversarial cyberspace activities and capabilities, both before and after their employment.

   *(**See: Counterair** (JP 3-01) - A mission that integrates offensive and defensive operations to attain and maintain a desired degree of air superiority. Counterair missions are designed to destroy or negate enemy aircraft and missiles, both before and after launch. See also air superiority; mission; offensive counterair.*

   Replaces: "CND-RA," "active defense," and "dynamic network defense" where used to connote "offensive cyberspace operations to defend DoD networks"

---

7. **Countermeasures -** That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive or classified information or information systems.

   - Defensive Countermeasures includes actions to identify the source of hostile cyber activities; protection/ mitigation at the boundary (e.g., Intrusion Protection Systems (IPS), pre-emptive blocks, blacklisting); hunting within networks (actively searching for insiders and other adversaries or malware); passive and active intelligence (including law enforcement) employed to detect cyber threats; and/or actions to temporarily isolate a system engaged in hostile cyber activities.

   - Offensive countermeasures might include electronic jamming or other negation measures intended to disrupt an adversary's cyber capabilities during employment.

*(**See: Countermeasures (JP 1-02**): That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity. See also "Security Countermeasures" (JP 1-02): Those protective activities required designed to prevent espionage, sabotage, theft, or unauthorized use of classified or controlled information, systems, or material. **See also: "Technical Surveillance Countermeasures" (JP 1-02)**: Techniques and measures to detect and neutralize a wide variety of hostile penetration activities that are used to gain unauthorized access to sensitive and classified information). **See also: "Protection:"** (National Infrastructure Protection Plan 2009): Actions or measures taken to cover or shield from exposure, injury, or destruction. In the context of the NIPP, protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as... initiating **active or passive countermeasures**...) ,*

Replace: "CND-RA" where the response is purely technical, falls below use-of-force thresholds, or generically addresses activities pursuant to defensive countercyber.

---

8. **Critical Cyber System/Asset/Function** (Draft NCIRP Feb 2010): An information system Is considered to be vital if a physical or cyber incident affecting the confidentiality, integrity and availability of the system, asset or function would have significant negative impact on the national security, economic stability, public confidence, health or safety of the United States.

   Replaces: n/a

---

9. **Critical Infrastructure** (Draft NCIRP Feb 2010): Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

   Replaces: n/a

---

10. **Cyber attack:** A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.

    ***(See: Computer Network Attack (JP 1-02):** Actions taken through the use of computer networks to deny, degrade, disrupt or destroy information resident in computers and*

computer networks, or the computers and networks themselves. ***Note:*** *"cyber attack" is proposed in place of CNA not because the definition differs substantially, but because CNA is inextricably linked to a larger Computer Network Operations (CNO) paradigm/doctrine which differs in many substantive ways from that presented here—namely, that the connotations of CNA and CNE are much broader, and the definition of CND much narrower, than the set of related but more contextually and operationally nuanced definitions presented here.)*

Replaces: "CNA" and "offensive cyberspace operations" where the action meets use-of-force levels or is specifically intended to disrupt, deny, degrade, manipulate, and/or destroy adversary computer systems or data.

---

11. **Cyber Defense**: The integrated application of DoD or US Government cyberspace capabilities and processes to synchronize in real-time the ability to detect, analyze and mitigate threats and vulnerabilities, and outmaneuver adversaries, in order to defend designated networks, protect critical missions, and enable US freedom of action. Cyber Defense includes:

    - Proactive NetOps: (e.g., configuration control, information assurance (IA) measures, physical security and secure architecture design, intrusion detection, firewalls, signature updates, encryption of data at rest);
    - Defensive Counter Cyber (DCC): Includes: military deception via honeypots and other operations; and redirection, deactivation, or removal of malware engaged in a hostile act/imminent hostile act.
    - Defensive Countermeasures.

*(**See: Defense in Depth** (JP 1-02): Mutually supporting defense positions designed to absorb and progressively weaken attack, and to prevent observations of the whole position by the enemy. See also:* ***Computer Network Defense*** *(JP 1-02): Actions taken to protect, monitor, analyze, and detect and respond to unauthorized activity within DOD information systems or computer networks.* ***Note:*** *this doctrinal definition of CND is more restrictive than current and planned defensive cyberspace operations, as demonstrated in multiple national-level exercises, and USSTRATCOM's SECDEF-approved Implementation Plan for USCYBERCOMMAND. The replacement definition focuses on mission assurance, introduces the concept of maneuver by allowing for proactive measures and military deception, and allows the future designation of networks outside DoD (such as critical infrastructure) as systems falling under DOD's homeland defense role in cyberspace).*

Replace: "CND," "active defense," "Defense-in-Depth," and "Dynamic Network Defense" where the terms are meant to connote overarching defensive constructs.

---

12. **Cyber Incident** (Draft NCIRP Feb 2010): Level 2 or Level 1 Incident on the Cyber Risk Alert Level System. A Cyber Incident is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the Nation.

Replaces: n/a

---

13. **Cyber Operational Preparation of the Environment (C-OPE):** Non-intelligence enabling functions within cyberspace conducted to plan and prepare for potential follow-on military operations. C-OPE includes but is not limited to identifying data, system/network configurations, or physical structures connected to or associated with the network or system (to include software, ports, and assigned network address ranges or other identifiers) for the purposes of determining system vulnerabilities; and actions taken to assure future access and/or control of the system, network, or data during anticipated hostilities.

*(**See: OPE (JP 3-13**): Non-intelligence activities conducted to plan and prepare for potential follow-on military operations.)*

Replaces: CNE or CNA when used specifically as an enabling function for another military operation.

---

14. **Cyber-Security**: All organizational actions required to ensure freedom from danger and risk to the security of information in all its forms (electronic, physical), and the security of the systems and networks where information is stored, accessed, processed, and transmitted, including precautions taken to guard against crime, attack, sabotage, espionage, accidents, and failures. Cybersecurity risks may include those that damage stakeholder trust and confidence, affect customer retention and growth, violate customer and partner identity and privacy protections, disrupt the ability to conduct or fulfill business transactions, adversely affect health and cause loss of life, and adversely affect the operations of national critical infrastructures.

Replaces: n/a

---

15. **Cyberspace** (NMS-CO): Domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networkee systems and associated physical infrastructures.

Replaces: n/a

---

16. **Cyberspace Operations (CO)** (CM-0856-09 1 Sep 09): The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

Replaces: Computer Network Operations

---

17. **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, sea, and space forces at a given time and sphere of operations without prohibitive interference by an adversary.

*(**See: Air Superiority** (JP 1-02) That degree of dominance in the air battle of one force over another that permits the conduct of operations by the former, and by its related land, sea, and air forces in a given time and place without prohibitive interference by the opposing force.)*

Replaces: n/a

---

18. **Cyber Warfare (CW):** An armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defense, and cyber enabling actions.

*(**See: Undersea Warfare (JP 1-02**): Operations conducted to establish and maintain control of the underwater environment by denying an opposing force the effective use of the underwater systems and weapons. It includes offensive and defensive submarine, anti-submarine, and mine warfare operations.*

Replaces: Network Warfare (NW), Network Warfare operations.

---

19. **Defensive Counter-Cyber (DCC)** - All defensive countermeasures designed to detect, identify, intercept, and destroy or negate harmful activities attempting to penetrate or attack through cyberspace. DCC missions are designed to preserve friendly network integrity, availability, and security, and protect friendly cyber capabilities from attack, intrusion, or other malicious activity by pro-actively seeking, intercepting, and neutralizing adversarial cyber means which present such threats. DCC operations may include: military deception via honeypots and other operations; actions to adversely affect adversary and/or intermediary systems engaged in a hostile act/imminent hostile act; and redirection, deactivation, or removal of malware engaged in a hostile act/imminent hostile act.

*(**See: Defensive counterair (DCA) (JP 3-01)** - All defensive measures designed to detect, identify, intercept, and destroy or negate enemy forces attempting to penetrate or attack through friendly airspace.)*

Replaces: "CND-RA," "active defense," "dynamic network defense" where used to connote operations outside the DOD network perimeter to counter a hostile act or demonstrated hostile intent in cyberspace.

---

20. **Effects assessment (EA):** The timely and accurate evaluation of effects resulting from the application of lethal or non-lethal capabilities against a military objective. Effects assessment is composed of physical effect assessment, functional effect assessment, and target system assessment.

*(**See: Battle Damage Assessment (BDA)** (JP 1-02): The timely and accurate evaluation of effects resulting from the application of lethal or non-lethal force against a military objective. BDA is composed of physical effect assessment, functional effect assessment, and target system assessment. **Note**: BDA is a specific type of effects assessment for damage effects.)*

Replaces: n/a

---

21. **Flexible Deterrent Option (FDO)** (JP 1-02): A planning construct intended to facilitate early decision making by developing a wide range of interrelated responses that begin with deterrent-oriented actions carefully tailored to produce a desired effect. The flexible deterrent option is the means by which the various diplomatic, information, military, and economic deterrent measures available to the President are included in the joint operation planning process.

*(**Note**: Cyber operations, to include defensive counter-cyber options which if known by an adversary to have the likely effect of rendering his operation ineffective, and would thereby deter that operation, can be part of the FDO spectrum.)*

Replaces: **n/a**

---

22. **Hostile Act** – Force or other means used directly to attack the US, US forces, or other designated persons or property, to include critical cyber assets, systems or functions. It also includes force or other means to preclude or impede the mission and/or duties of US forces, including the recovery of US personnel or vital US Government property.

*(**See: Hostile Act (JP 3-28, and JP 1-02)** - An attack or other use of force against the US, US forces, or other designated persons or property. It also includes force used directly to preclude or impede the mission and/or duties of US forces, including the recovery of US personnel or vital US Government property.)*

Replaces: n/a

---

23. **Hostile Intent:** The threat of an imminent hostile act. Determination of hostile intent in cyberspace can also be based on the technical attributes of an activity which does not meet the hostile act threshold but has the capability, identified through defensive countercyber or forensic operations, to disrupt, deny, degrade, manipulate, and/or destroy critical cyber assets at the will of an adversary (such as a logic bomb or "sleeper" malware). Because an individual's systems may be used to commit a hostile act in cyberspace without their witting participation, the standard for attribution of hostile act/intent for defensive counter-cyber purposes is 'known system involvement,' and is not witting actor or geography-dependent."

*(**See: Hostile Intent** (JP 1-02): The threat of imminent use of force by a foreign force, terrorist(s), or organization against the United States and US national interests, US forces and, in certain circumstances, US nationals, their property, US commercial assets, and other designated non-US forces, foreign nationals, and their property. When hostile intent is present, the right exists to use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat. A determination that hostile intent exists and requires the use of proportional force in self-defense must be based on evidence that an attack is imminent. Evidence necessary to determine hostile intent will vary depending on the state of international and regional political tension, military preparations, intelligence, and indications and warning information.)*

Replaces: malware, Trojan, virus, and similar technical terms where they refer to operationally significant, targeted efforts to adversely affect DOD or other vital US systems.

---

24. **Information Assurance (IA)** (CJCSI 8500-1): Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating detection, protection, and reaction capabilities

Replaces: N/A

---

25. **Interdiction:** An action to divert, disrupt, delay, or destroy an adversary's military capability before it can be used effectively against friendly forces or systems, or to otherwise achieve objectives.

***(See: Interdiction (JP 3-03)**- An action to divert, disrupt, delay, or destroy the enemy's military surface capability before it can be used effectively against friendly forces, or to otherwise achieve objectives. **Note:** If "surface" is deleted from current Interdiction definition, Cyber interdiction becomes a subset of this type of operation.)*

Replace: "CND-RA" where preemptively removing or rendering ineffective malware targeted at DOD or vital national systems on the adversary system or in transit is intended.

26. **Intelligence, surveillance, and reconnaissance (ISR)** (JP 2-01) - An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.

Replaces "CNE" when used in defensive countercyber or in support of offensive (USC Title 10) operations in cyberspace. Where CNE is intended purely for the collection of foreign intelligence, it is cyber-enabled foreign intelligence (CEFI), or computer network exploitation (CNE). Where it is in support of planned or current kinetic operations, it is JIPOE (see below).

---

27. **Intrusion** (JP 1-02): Movement of a unit or force within another nation's specified operational area outside of territorial seas or territorial airspace, not specifically approved by that nation, for surveillance, intelligence gathering, or other operation in time of peace or tension.

(**See also: "Intrusion"** (NCIRP): Unauthorized act of bypassing the security mechanisms of a system.

Replaces: n/a

---

28. **Joint Intelligence Preparation of the Operational Environment (JIPOE)** - An analytical methodology employed to reduce uncertainties concerning the adversary, environment, and terrain, including cyberspace operations. Intelligence preparation of the battlespace is a continuing process. Also called *Intelligence Preparation of the Battlespace (IPB).*

*(**See: JIPOE (JP 2-0):** An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. JIPOE builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process.. Also called Intelligence Preparation of the Battlespace (IPB)).*

Replace: CNE when used to describe cyberspace operations intended to identify or map network topologies and cyber capabilities in order to support/facilitate a specific planned operation or set of operations.

29: **Mission Assurance Category (MAC)** (DODD 8500-1): Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly

the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

- **Mission Assurance Category I** (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

- **Mission Assurance Category II** (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness.

- **Mission Assurance Category III** (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities.

Replaces: n/a. Used to determine appropriate ROE in response to known or anticipated hostile acts or other threats.

---

30. **Mitigation** (US CERT CONOPS, NRF): Solutions that contain or resolve risks through analysis of threat activity and vulnerability data which provide timely and accurate responses to prevent attacks, reduce vulnerabilities and fix systems. Activities providing a critical foundation in the effort to reduce the loss of life and property from natural and/or manmade disasters by avoiding or lessening the impact of a disaster and providing value

Replaces: n/a

---

31. **National Military Strategy for Cyberspace Operations (NMS-CO):** The comprehensive strategy of the US Armed Forces to ensure US military superiority in cyberspace. The NMS-CO establishes a common understanding of cyberspace and sets forth a military strategic framework that orients and focuses DOD actions

in the areas of military, intelligence, and business operations in and through cyberspace.

Replaces: n/a

---

32. **Network Operations (NetOps)** (JP-1-02): Activities conducted to operate and defend the DOD's Global information Grid

Replaces: n/a

---

33. **Offensive Counter-Cyber (OCC):** Offensive operations to destroy, disrupt, or neutralize adversary cyberspace capabilities both before and after their use against friendly forces, but as close to their source as possible. The goal of OCA operations is to prevent the employment of adversary cyberspace capabilities prior to employment. This could mean preemptive action against an adversary.

*(**See: Offensive Counter-Air** (JP 1-02): Offensive operations to destroy, disrupt, or neutralize enemy aircraft, missiles, launch platforms, and their supporting structures and systems both before and after launch, but as close to their source as possible." The goal of OCA operations is to prevent the launch of enemy aircraft and missiles by destroying them and their overall supporting infrastructure prior to employment. This could mean preemptive action against an adversary.)*

Replaces: **CNA where it refers to a SECDEF-directed cyber attack, presumably in a period of hostilities, specifically aimed at damaging an adversary's ability to use its cyberspace capabilities against friendly forces.** It differs from the generic use of "cyber attack" in that the latter can be used to affect non-cyber systems, including but not limited to infrastructure, IADS, transportation and other networks, etc., and is not specifically tied to imminent or ongoing of hostilities.

---

34. **Offensive Cyberspace Operations (OCO):** Activities that, through the use of cyberspace, actively gather information from computers, information systems, or networks, or manipulate, disrupt, deny, degrade, or destroy targeted computers, information systems, or networks. This definition includes Cyber Operational Preparation of the Environment (C-OPE), Offensive Counter-Cyber (OCC), cyber attack, and related electronic attack and space control negation.

Replaces: n/a

---

35. **Sensitive Reconnaissance** (CJCSI-3250.01): Reconnaissance operations which, by virtue of their collective objectives, means of collection, or area of operation, involve significant military risk or political sensitivity.

Replaces: CNE when referring specifically to specific, high risk, politically sensitive cyber operations which require additional interagency deconfliction, coordination, or execution authorities.

---

36. **Special Reconnaissance (SR)** (JP 3-05, JP 1-02): Reconnaissance and surveillance actions conducted as a special operation in hostile, denied, or politically sensitive environments to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces. These actions provide an additive capability for commanders and supplement other conventional reconnaissance and surveillance actions.

    Replaces: Can replace CNE used specifically to denote cyberspace ops executed in highly sensitive areas or for highly sensitive purposes, using means or capabilities not normally employed by Service component forces; e.g., direct human action in gaining accesses or implanting tools, or specific target development in support of planned operations. Will generally apply to CO conducted by special forces or via other non-conventional means.

---

37. **Target location**: The specific location at which an effect is intended to manifest. If a cyber action will result in kinetic or kinetic-like effects (e.g., changing the function of a physical system, or file manipulation that results in a financial loss), the target location is the physical location of the effect, The target location may differ from the aim point(s) of the action—e.g., generating or blocking a command at a server or router to generate a desired effect (protection from malware, re-routing of packets, or an end-user being unable to access a site) at another node.

    (**Note:** Derived from Air Warfare TTPs. Target Location is the specific physical point at which the desired effect is intended to manifest. E.g., a bomb may have an aim point calculated to create a shockwave effect at a nearby target location, or to destroy a remote power or communications node feeding a command and control function at a distant target location)

    Replaces: n/a

---

38. **Weapon action** (JP 1-02): The effect-producing mechanisms or functions initiated by a weapon when triggered.

    *(**Note:** The weapon actions of a kinetic weapon are blast, heat, fragmentation, etc. The weapon actions of a cyber attack weapon might be writing a set of software commands or other information to a memory register, transmission of a radio frequency (RF) waveform, etc.)*

    Replaces: n/a

---

39. **Weapon categorization**: A binning of cyber weapon capabilities into categories, based on risk assessment and the release authority required for their use, that is used to determine authorization level for its use. Example categories might be:

- Category I – Combatant commander release
- Category II – Pre-approved for combatant commander use in specific OPLANs or under specific warning/weapon status ROE
- Category III – President/SECDEF release only

Replaces: n/a

---

40 **Weapon effect:** A direct or indirect objective (intended) result a weapon action, typically specified by a specific target scope, desired effect type (material, behavioral) and level, and start time and duration. A direct (or first-order) effect is an outcome created directly by the weapon's action. An indirect effect is an outcome that cascades from one or more direct or other indirect effects of the weapon's action (also known as second, third, n^{th} order effects, etc.). Because of the interconnected nature of cyberspace, indirect effects must be determined to the greatest extent possible and evaluated for acceptability before weapon use. These assessments will feed the Weapon Categorization process.

Replaces: n/a

---

41. **Warning Status (WS)**. Established by Combatant Commander to identify threat and support implementation of appropriate rules of engagement (ROE).* Standard WS levels are:

(1) White: Attack by hostile forces is improbable without adequate warning

(2) Yellow: Attack by hostile forces is probable

(3) Red: Attack by hostile forces is imminent or is in progress.

Replaces: INFOCON and use as significant component of CYBERCON conditions evaluation

---

42. **Weapons Control Status** (JP 1-02 (NATO)): the degree of fire control imposed by appropriate command authorities upon units with assigned, attached, or organic weapons. WCS is established and adjusted based on friendly and enemy dispositions, and may be modified for specific operations to prevent unintended effects or fratricide, or to facilitate rapid target engagement. WCS may differ from unit to unit depending on situation. For example, JTF commanders may have the authority to direct permissive WCS within their theater to protect their forces or aid in achieving wartime military objectives, yet may impose greater restrictions in areas where friendly forces are known to be operating. WCS is paired with warning status.[1]

The three WCS in descending order of restriction are:

(1) **WEAPONS HOLD/SAFE** (JP 1-02 NATO): A weapons control order imposing a status whereby weapon systems may only be engaged in self defense or in response to a formal order.

(2) **WEAPONS TIGHT** (JP 1-02 NATO): . A weapons control order imposing a status whereby weapon systems may engage only targets recognized under the ROE in effect as hostile.

(3) **WEAPONS FREE** (JP 1-02 NATO): A weapons control order imposing a status whereby weapon systems may engage any target not positively recognized as friendly.

*(**Note:** WCS, in conjunction w/ WS, is used to develop/effectively implement supplemental SROE[1])*

Replaces: n/a.

---

43. **Weapon system** (JP 1-02): A combination of one or more offensive capabilities with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. (Source: JP 1-02.)

*(**Note:** Offensive cyber capabilities, though they may be available "in the wild," or developed by a single individual, go through a process of effect determination, characterization, categorization, and crew training before they are considered "weaponized" and available for use by DOD operators).*

Replace: "tool" or "toolkit" where weaponized offensive (meets use of force criteria) capability is intended.

---

[1] WS and WCS are paired to provide awareness of and control of operations. For example, under peacetime circumstances WS and WCS will likely be "White-Hold;" during escalating hostilities they be set as "Yellow-Tight" or "Red-Tight;" during major conflict they may be "Red-Tight" or "Red-Free." Though WS is likely to be common across an AOR, WCS may vary according to local or temporal conditions.