(U) THE CYBER WARFARE LEXICON

(U) A LANGUAGE TO SUPPORT THE DEVELOPMENT, TESTING, PLANNING, AND EMPLOYMENT OF CYBER WEAPONS AND OTHER MODERN WARFARE CAPABILITIES

Version 1.7.6
05 January 2009

Lexicon POC:
USSTRATCOM
JFCC-NW J5

(U) Table of Contents

(U) A CYBER WARFARE TESTING, PLANNING, AND WEAPONEERING LEXICON

"Language is only secondarily the means by which we communicate, it is primarily the means by which we think." Dee Hock

"A lexicon is simply a collection of terms that apply to a particular skill or field of study. The fuller the lexicon, the richer the communication. You can't talk about a subject if you don't have the words. And, some psychologists would argue, you can't even think about it. At least not very productively." www.notrain-nogain.org

"The seeming inability to express ideas clearly, loose use of words, and ill-considered invention of other terms have damaged the military lexicon to the point that it interferes with effective professional military discourse." Lieutenant General Paul Van Riper USMC

(U) Introduction

(U//FOUO) Since the 2006 signing of the National Military Strategy for Cyberspace Operations (NMS-CO), the emerging US cyber warfare community continues to mature and its capabilities increasingly compete for consideration when US forces plan operations. Computer network attack (CNA) and electronic attack (EA) technologies have progressed to the point where their use could be routinely considered in the context of existing and developing OPLANS. In order to effectively integrate and standardize use of these non-traditional weapons, the developers, testers, planners, targeteers, decision-makers, and battlefield operators require a comprehensive but flexible cyber lexicon that accounts for the unique aspects of cyber warfare while minimizing the requirement to learn new terms for each new technology of the future. Without a shared understanding of the accurate meanings of a significant number of frequently used terms, it will be difficult to make progress on the more complex and unresolved technical and operational issues for non-traditional weapons: actionable requirements, technical and operational assurance, effective mission planning techniques, and meaningful measures of effectiveness. In fact, the Secretary of Defense's Information Operations (IO) Roadmap listed its first benefit to the combatant commanders as "a common lexicon and approach to IO, including support to integrated information campaign planning." Although the focus of cyberspace operations is not the same as that of IO, they share some technologies and until now, no such lexicon (for IO, or any portion of IO) has been published.

(U//FOUO) Under Unified Command Plan (UCP) 2008, USSTRATCOM has overall responsibility for IO. This Lexicon was initiated and originally published by the STRATCOM J8-sponsored IO Joint Munitions Effectiveness Manual (JMEM) Working Group. As its scope and potential impact grew beyond the JMEM community, responsibility was transferred to the USSTRATCOM Joint Functional Component Command for Network Warfare (JFCC-NW) staff for further refinement and development. The publication of the NMS-CO established an obvious but ill-defined relationship between CO and IO. This Lexicon is an attempt to consolidate the core terminology of cyberspace operations, and to clarify somewhat the CO/IO relationship. However, many of the terms introduced or updated here are equally applicable throughout the testing, planning, and operational communities, regardless of the underlying technology, and suggest language that could even improve doctrine for traditional weapons and operations.

(U//FOUO) The obvious place to start looking for a baseline of terms is in existing doctrine and policy, including the Joint Publication series and the kinetic warfare lexicons. The various documents that constitute Joint doctrine and policy contain an extensive set of existing terms for describing the utilization and effects of kinetic weapons. Although there are some similarities and analogous terms that can be transferred from kinetic warfare, there are significant underlying differences between traditional operations and modern effects-based operations (EBO) that incorporate non-traditional weapons. These differences make it difficult to directly re-use some of the traditional kinetic lexicon. There are also a number of concepts unique to non-kinetic warfare that require definition and inclusion in the lexicon, and that suggest improved definitions for some traditional kinetic terms are also possible.

(U//FOUO) It is worth noting that terms associated with traditional weapons are based on the assumption of materiel or personnel as the target and damage as the effect. Materiel is defined as the "equipment, apparatus, and supplies used by an organization." Although this description could cover adversary computer networks, it would be quite a linguistic stretch to say that the information on those networks is also materiel. Since cyber targets are very often non-materiel, and since cyber weapons can create non-damage effects, it stands to reason that the language of traditional munitions will be inadequate if we try to force it to cover offensive and defensive cyber operations.

(U) Terms whose existing definitions are already properly scoped for both traditional and modern warfare are not included in this lexicon; only those terms that are undefined or inadequately defined in Joint Publication 1-02 (JP 1-02), the "DOD Dictionary." Although some terms may be cyber-specific, whenever possible, terms have been defined (or redefined) to meet the needs of the traditional kinetic community as well and therefore the terms presented here are considered suitable for use throughout Joint doctrine. In addition to deciding which terms to include, the other, even thornier problem of the lexicon writer is exactly how to define each term selected. Experience teaches that, for many reasons, people grow strong attachments to existing definitions, and this can preclude serious consideration of alternate definitions, no matter how logically they are crafted and presented.

(U) Additional common lexicon errors that this document seeks to correct are:

1. (U) Circularity - Self-referential definitions or a chain of cross-references that results in self-reference.
2. (U) Insularity – Definitions that focus exclusively on a limited domain and ignore the fact that the term already has another meaning in a different but related domain, or fail to consider how, with minor changes, the definition could be made much more broadly useful to a wider audience.
3. (U) Incompleteness - Definitions that lack value either because they don't represent a complete thought or they are so broad that they can mean the same thing as other definitions.
4. (U) Overly complete - Definitions are generally best when they have as few words as possible that communicate the exact meaning. Many authors (often trying to be helpful) feel compelled to add words that are not central to the meaning of the term and end up with in an incorrect definition.

(U) The cyber warfare community needs a precise language that both meets their unique requirements and allows them to interoperate in a world historically dominated by kinetic warfare. Mission planners must be able to discuss cyber weapons with their commanders, the intelligence analysts, the targeteers, and the operators, using terms that will be understood not just because they have been defined somewhere in doctrine, but also because they make sense. Giving the weapons planners a well-founded lexicon enables them to have far-reaching discussions about all manner of weapons and make important decisions with a significantly reduced likelihood of misunderstanding and operational error.

(U) In addition to this Introduction, the Lexicon includes a brief description of its context and two attachments. Attachment 1 is the Lexicon itself and is designed to be extracted for readers who just want to review the proposed terminology without the background. Attachment 2 contains a series of background discussions on topics central to the terms included in the Lexicon. These discussions include explanation and justification for the terms selected for inclusion and for their definitions.

(U) Cyber Lexicon Context

(U) A Mk 84 iron bomb will detonate with a known force regardless of the type of environment in which it is dropped (i.e. desert, forest, city, ship, etc.). Its ability to create this kinetic action is inherent in the bomb itself and it generally requires nothing of its environment to produce the "boom." All that remains is to ensure that it is fused correctly and delivered accurately. Another way to describe this attribute of the Mk 84 is to say that it has few "environmental dependencies." Perhaps, if it uses an altitude sensitive fuse, then we could say that it has an environmental dependency on the fact that barometric pressure increases in proportion to proximity to the Earth's center. An environmental dependency is a condition or feature of the operational environment that must be in-place and be 'as expected' in order for the weapon to take its designed action (which is not the same as the desired effect, but which we hope will subsequently create the desired effect).

(U//FOUO) In stark contrast to a typical kinetic weapon, cyber weapons often have significant and complex environmental expectations and dependencies. If a cyber weapon is used on an improperly characterized target network, data link, or operating system where its dependencies are not met, the weapon is unlikely to 'detonate,' or if it does, it will not generate the desired effect. Even worse, there may be consequences, such as the weapon revealing itself to the adversary. (Note that the fact that we are concerned with the self-illumination tendencies of cyber weapons is foreign to kinetic mission planning, where weapon illumination is almost always assumed.)

(U) Additionally, there are some terms used in kinetic operations that have never been defined, simply because it wasn't necessary. Because the DoD community has hundreds of years of shared experience using kinetic weapons, some things are mutually understood without definition. For instance, the term 'weapon' is not defined in JP 1-02. It has not been important because the dictionary definition and the long-held, shared understanding of the term were sufficient. In cyber warfare what constitutes a weapon is less obvious. The same might be said for the term 'effect' and other commonly used terms.

(U//FOUO) The detailed environmental dependencies of cyber warfare capabilities, and the relative complexity of non-kinetic operations in general, require a precise set of terms whose definitions are shared throughout DoD. Whenever they can be the same (or similar) to kinetic terms, they should be. Otherwise, sticking with kinetic terms just because they are familiar is neither logical nor conducive to increased understanding of non-kinetic weapons. And most importantly, it is not likely to foster operational success.

(U) Attachment 1: CYBER WARFARE LEXICON

Note: Most of the terms defined here are new, i.e. they are not currently defined in Joint doctrine or guidance. Definitions here of terms that are already found in current doctrine and guidance are proposed as updates or corrections to the existing incorrect or sub-optimal definitions. Some are already approved and some are suggested here in order to engender discussions on their appropriateness and applicability. Subsequent versions of the Lexicon may contain refined versions of these definitions and additional definitions suggested by the community.

(U//FOUO) cyberspace: a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (from 12 May 2008 SECDEF memo)

[(U//FOUO) *Previous version – cyberspace: A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. (from NMS-CO)*]

(U//FOUO) cyberspace operations (CO): All activities conducted in and through cyberspace in support of the military, intelligence, and business operations of the Department. (*based on NMS-CO description*)

(U//FOUO) cyberspace operations (CO): The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global information grid. (*from 29 Sep 2008 VJCS Memo, however it is inconsistent with NMS-CO and improperly limited*)

(U//FOUO) cyber warfare (CW): Creation of effects in and through cyberspace in support of a combatant commander's military objectives, to ensure friendly forces freedom of action in cyberspace while denying adversaries these same freedoms. Composed of cyber attack (CA), cyber defense (CD), and cyber exploitation (CE).

- (U//FOUO) cyber attack (CA): Cyber warfare actions intended to deny or manipulate information and/or infrastructure in cyberspace. Cyber attack is considered a form of fires.

- (U//FOUO) cyber defense (CD): Cyber warfare actions to protect, monitor, detect, analyze, and respond to any uses of cyberspace that deny friendly combat capability and unauthorized activity within the DOD global information grid (GIG).

- (U//FOUO) cyber exploitation (CE): Cyber warfare enabling operations and intelligence collection activities to search for, collect data from, identify, and locate targets in cyberspace for threat recognition, targeting, planning, and conduct of future operations.

(U//FOUO) cyber warfare capability: A capability (e.g. device, computer program, or technique), including any combination of software, firmware, and hardware, designed to create an effect in cyberspace, but that has not been weaponized. Not all cyber capabilities are weapons or potential weapons.

(U//FOUO) cyber weapon system: A combination of one or more weaponized offensive cyber capabilities with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. (*Note: adapted directly from JP 1-02 of weapon system.*)

(U//FOUO) cyber weaponization: The process of taking an offensive cyber capability from development to operationally ready by incorporating control methods, test and evaluation, safeguards, security classification guidance, interface/delivery method, certified and trained personnel, employment recorder, CONOP, TTP, life-cycle support, and launch platform.

(U//FOUO) cyber weapon characterization: The process of determining and documenting the effect producing mechanisms and assurance factors of cyber weapons. Characterization includes aspects of technical assurance evaluation, OT&E, risk/protection assessments, and other screening processes. Answers the question: "What do I need to know about this weapon before I can use it?" [Note: Cyber Weapon Characterization is one step in the Cyber Weaponization process.]

(U//FOUO) cyber weapon categorization: A binning of cyber weapon capabilities into categories, based on risk assessment and the release authority required for their use. Useful for answering the question: "Who can authorize use of this weapon?" Example categories might be:

- Category I – Combatant commander release
- Category II – Pre-approved for combatant commander use in specific OPLANs
- Category III – President/SECDEF release only

(U//FOUO) cyber weapon delivery mode: The method via which a cyber weapon (or a command to such a weapon) is delivered to the target. Delivery may be via direct implant or remote launch. Hardware cyber weapons often require direct implant. Remote launched cyber weapons and/or commands may be placed via wired and/or wireless paths.

(U//FOUO) cyber weapon flexibility: The extent to which the cyber weapon's design enables operator reconfiguration to account for changes in the target environment.

(U//FOUO) cyber weapon identification: The manner in which a cyber weapon is represented for inventory control purposes, based on the weapon's forensic attributes (e.g. for software: file name, file size, creation date, hash value, etc., for hardware: serial number, gram weight, stimulus response, x-ray image, unique markings, etc.).

(U) access: Sufficient level of exposure to or entry into a target to enable the intended effect.

(U) collateral effect: Unintentional or incidental effects, including injury or damage, to persons or objects that would not be lawful military targets in the circumstances ruling at the time.

(U) deny: To attack by degrading, disrupting, or destroying access to or operation of a targeted function by a specified level for a specified time. Denial is concerned with preventing adversary use of resources.

- (U) degrade: (a function of amount) To deny access to or operation of a targeted function to a level represented as a percentage of capacity. Desired level of degradation is normally specified.

- (U) disrupt: (a function of time) To completely but temporarily deny access to or operation of a targeted function for a period represented as a function of time. Disruption can be considered a special case of degradation where the degradation level selected is 100%.

- (U) destroy: To permanently, completely, and irreparably deny access to, or operation of, a target. Destruction is the denial effect where time and level are both maximized.

(U) dud: A munition that has not been armed or activated as intended or that failed to take an expected action after being armed or activated. (*Note: adapted directly from JP 1-02 of dud.*)

(U) effects assessment (EA): The timely and accurate evaluation of effects resulting from the application of lethal or non-lethal force against a military objective. Effect assessment can be applied to the employment of all types of weapon systems (air, ground, naval, special forces, and cyber weapon systems) throughout the range of military operations. Effects assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Effects assessment is composed of physical effect assessment, functional effect assessment, and target system assessment. Note: Battle Damage Assessment (BDA) is a specific type of effects assessment for damage effects. " *(This is a direct adaptation from the JP 1-02 definition of BDA.)*

(U//FOUO) intended cyber effect: A sorting of cyber capabilities into broad operational categories based on the outcomes they were designed to create. These categories are used to guide capability selection decisions. Answers the question: "What kind of capability is this?" Specifically:

- denial – degrade, disrupt, or destroy access to, operation, quality of service, or availability of target resources, processes, and/or data.
- manipulation – manipulate, distort, or falsify trusted information on a target.
- command and control – provide operator control of deployed cyber capabilities.
- information/data collection – obtain targeting information about targets or target environments.
- access – establish unauthorized access to a target.
- enabling – provide resources or create conditions that support the use of other capabilities.

(U) kinetic: Of or pertaining to a weapon that uses, or effects created by, forces of dynamic motion and/or energy upon material bodies. Includes traditional explosive weapons/effects as well as capabilities that can create kinetic RF effects, such as continuous wave jammers, lasers, directed energy, and pulsed RF weapons.

- (U) non-kinetic: Of or pertaining to a weapon that does not use, or effects not created by, forces of dynamic motion and/or energy upon material bodies.

(U) lethal: Of or pertaining to a weapon or effect intended to cause death or permanent injuries to personnel.

- (U) non-lethal: Of or pertaining to a weapon or effect not intended to cause death or permanent injuries to personnel. Nonlethal effects may be reversible and are not required to have zero probability of causing fatalities, permanent injuries, or destruction of property.

(U//FOUO) manipulate: To attack by controlling or changing a target's functions in a manner that supports the commander's objectives; includes deception, decoying, conditioning, spoofing, falsification, etc. Manipulation is concerned with using an adversary's resources for friendly purposes and is distinct from influence operations (e.g. PSYOP, etc.).

(U) misfire: The failure of a weapon to take its designed action; failure of a primer, propelling charge, transmitter, emitter, computer software, or other munitions component to properly function, wholly or in part. (*Note: adapted directly from JP 1-02 of misfire.*)

(U) probability of effect (PE): The chance of a specific functional or behavioral impact on a target given a weapon action.

(U) target state: The condition of a target described with respect to a military objective or set of objectives.

(U) targeted vulnerability: An exploitable weakness in the target required by a specific weapon.

- objective vulnerability: A vulnerability whose exploitation directly accomplishes part or all of an actual military objective.
- access vulnerability: A vulnerability whose exploitation allows access to an objective vulnerability.

(U) weapon action: The effect-producing mechanisms or functions initiated by a weapon when triggered. The weapon actions of a kinetic weapon are blast, heat, fragmentation, etc. The weapon actions of a cyber attack weapon might be writing to a memory register or transmission of a radio frequency (RF) waveform.

(U) weapon effect: A direct or indirect objective (intended) outcome of a weapon action. In warfare, the actions of a weapon are intended to create effects, typically against the functional capabilities of a material target or to the behavior of individuals. Effect-based tasking is specified by a specific target scope, desired effect level, and start time and duration.

- direct effect: An outcome that is created directly by the weapon's action. Also known as a first order effect.

- indirect effect: An outcome that cascades from one or more direct effects or other indirect effects of the weapon's action. Also known as second, third, Nth order effects, etc.

(U//FOUO) cyber weapon vulnerability: An exploitable weakness inherent in the design of a cyber weapon. Weaknesses are often in one of the following risk areas:

- detectability risk – The risk that a weapon will be unable to elude discovery or suspicion of its existence. This includes the adverse illumination risk of hardware weapons.
- attribution risk – The risk that the discoverer of a weapon or its effect will be able to identify the source and/or originator of the attack or the source of the weapon used in the attack.
- co-optability risk – The risk that, once discovered, the weapon or its fires will be able to be recruited, used, or reused without authorization.
- security vulnerability risk – The risk that, once discovered, an unauthorized user could uncover a security vulnerability in the weapon that allows access to resources of the weapon or its launch platform. This includes the risk of an adversary establishing covert channels over a weapon's C2 link.
- misuse risk – The risk that the weapon can be configured such that an authorized user could unintentionally use it improperly, insecurely, unsafely, etc.
- policy, law, & regulation (PLR) risk – The risk that the weapon could be configured such that an authorized user could intentionally use it in violation of existing policy, laws, and regulations.

(U) Attachment 2: Discussions on Cyberspace Operations

(U) Discussion 1 – The Evolution from Tool to Weapon (System)

(U//FOUO) The term 'tool' as applied to CNA capabilities, came into widespread use in the early 1990's when various non-Service organizations began to increase their support to the cyber warfare mission, and was a reflection of the sensitivities about any connection between the term weapon outside of Title 10 authorities. To a degree, it also represents the hesitation on the part of some to consider that offensive cyber capabilities might be 'real' weapons. However, in accordance with Joint doctrine, there are only six Joint functions: C2, Intel, Fires, Maneuver, Protection, and Sustainment. Therefore any form of offensive cyber warfare is unquestionably a form of fires and (again from Joint doctrine) fires come from weapons. Since the military Services have always built and fielded weapons and weapon systems, such distinctions were less important outside the Washington DC Beltway. But, since 'weapon' is a term not defined by JP 1-02, when the Office of the Undersecretary of Defense for Intelligence (USD(I)) began to work with the Services to define the process of weaponizing CNA, the JP 1-02 definition of 'weapon system' was the starting point. According to that definition, a weapon system does not exist until there also exists related equipment, trained personnel, material support, service, and a means of delivery and employment.

(U//FOUO) This begs the question, what is a weapon vs. a weapon system? Does it even matter? The distinction is moot in the kinetic world, since Defense acquisition documents tend to use the terms weapon and weapon system interchangeably. Even the simplest kinetic weapon (e.g. a firearm) is the product of lengthy and expensive design, development, and testing. And DoD acquisition policy requires that new weapons be fielded with all related training, maintenance and other life-cycle support, and a delivery mechanism. This means that the very first M-16 rifle ever made, while a 'weapon' in the dictionary sense of the word, was not deployed until it was operationally tested, had a training program, spare parts inventory, etc. After that, each new M-16 was part of a 'weapon system' and could be crated and shipped to the front lines directly from the assembly line.

(U//FOUO) However, new kinetic weapons are relatively rare. Relative, that is, to CNA weapons for instance, the average gestation of which is comparatively brief. Given the ease with which a new CNA weapon can emerge, there will frequently be temptation to skip the cost and schedule of a weaponization process. It may also interrupt what is intended to be a short lifespan: from development to operation to abandonment in a matter of only months or weeks. And except for some cyber weapons that may include hardware, there is no assembly line to support. For these reasons, it will be extraordinarily difficult to apply the same level of personnel training, material support, and life-cycle support to each and every offensive cyber capability that completes development.

(U//FOUO) Nevertheless, unless and until cyber weapon systems are given a pass on the weaponization process, the existing requirements still apply. Since there is no widely used DoD-level definition of a 'weapon' that distinguishes it from 'weapon system,' this Lexicon assumes that defining cyber warfare capability, and cyber weapon system is sufficient and no separate definition of Cyber Weapon is offered. A **cyber warfare capability** is therefore any cyber warfare device (software and/or hardware) that has completed development but that, for whatever reason, has not completed the weaponization process. This includes capabilities whose CONOP may not reach the level of attack (e.g. an enabling device that, used by itself, is not considered to be weapon). A **cyber weapon system** is a cyber warfare capability that has completed the weaponization process.

(U//FOUO) A limitation of the current weaponization process is that it obviously applies to software and hardware weapons, but it is less clear how it would apply to cyber techniques. A technique is a cyber capability that involves keystrokes, but where no hardware or software is introduced into the target system. This is analogous to sending a soldier to attack a target with no weapons other than his hands, his mind, and whatever he finds laying around the target environment. Normally, we might expect that anything he found would be fair game for employment. But what if he discovered an adversary's biological weapon? Could he use it? What if he began punching non-combatant bystanders with his bare hands? Is he authorized to take such measures? In these cases, the answer is almost certainly "no." However, we trust the soldier who we select for such missions to be well trained in rules of engagement (ROE) and well behaved. But, part of that trust is inherent in the fact that any kinetic weapons that he finds and is able to employ (including his fists) have straightforward environmental dependencies and logical consequences, and their relationship to the ROE will be readily apparent to him.

(U//FOUO) As far-fetched as that scenario may seem, that is exactly the situation in which a cyber warrior is likely to find herself. If last minute changes in the target render the approved weapon inert, an operator might need to use cyber techniques to complete an assigned mission, particularly one that has been approved for effect or objective (as opposed to approved for a particular weapon(s) or target). Do all such techniques require complete weaponization, legal review, and categorization before she can enter them at the system command prompt? Or, do we rely on her training and certification process and allow her to use her best judgment and to improvise as she goes along? What if the techniques she chooses to use are themselves somehow attributable based on style or the commands selected? Can she only use techniques previously approved for this specific target? Sub-optimal choices by the operator might not only thwart her attempts to complete the mission, but could lead to various undesirable consequences, including alerting the adversary of our intent and compromise of our weapons and techniques. These types of operations make the notion of having a certified and trained operator critical to the designation of a weapon system.

(U//FOUO) Answers to these and other similar questions are crucial to deciding more basic issues like "What is a cyber weapon system?", "When does it become a weapon?", and "When can it be used?" The most authoritative description of a cyber weaponization process to date is a USD(I) sponsored initiative to delineate the fundamental features of a CNA weapon system, which established a working definition that a CNA weapon system must have all of the following, as applicable:

- control methods (positive command and control by the operator),
- test and evaluation (functional testing and technical assurance evaluation),
- safeguards (protection of weapon and equities),
- security classification guidance,
- a delivery method,
- certified and trained personnel (specifically trained for the weapon),
- a mission log / data recorder (e.g. "black box" type record of weapon use),
- a CONOP,
- tactics, techniques, and procedures (TTP),
- life-cycle support, and
- an identified launch platform.

Until modified or superceded, this list comprises the current weaponization "best practices" for CNA weapons and, by extension, is an acceptable start for a cyber warfare weaponization process as well.

(U) Discussion 2 – Weapon Outcomes: A Differentiation

(U) Weapon planning discussions often include mention of 2ndorder effects and/or 2nd order consequences. Although many people use these terms interchangeably, for the purposes of planning and analysis, distinguishing between effect and consequence as two different types of weapon outcomes may provide a more useful language for military operations and might reduce the chance for operational error.

(U//FOUO) Note that while this discussion pertains to the specific effects and consequences of weapon application, the actions that precipitate effects and consequences do not have to come from weapons. The maneuver of military forces, the distribution of PSYOP materials, and the hoisting of an American flag over a captured adversary headquarters are all actions that can have effects and consequences. The same logic and definitions will still apply.

(U) Because the language of Joint Pub 3-60 and other targeting doctrine ties effects directly to objectives, and based on an understanding of the still dominant military construct of effects based operations (EBO), in addition to the existing definition, **effects** could also be thought of as those outcomes that the commander specifically intends to create, either directly or indirectly, through the use of selected capabilities or weapons. Effects can cascade and some weapons may be selected specifically for their ability to initiate a cascade of effects.

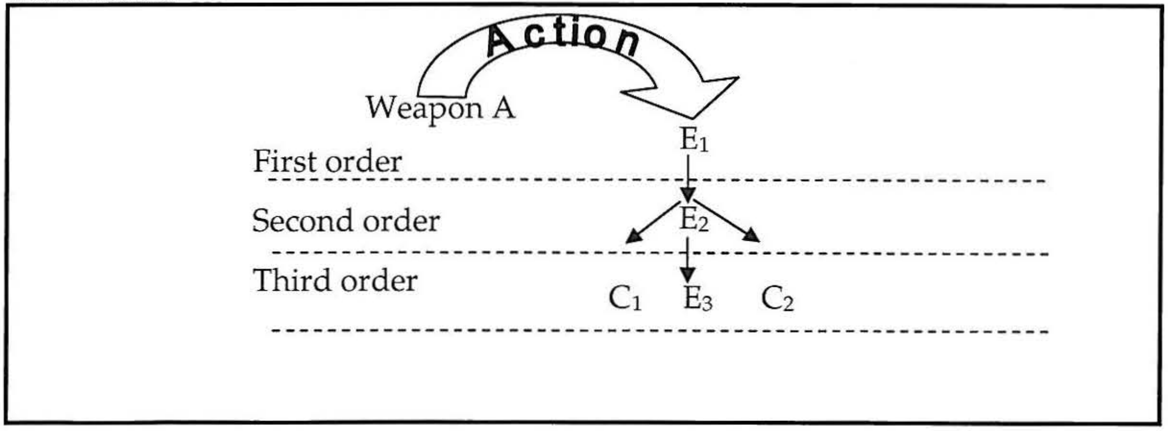
(U) Joint doctrine defines effect as the physical and/or behavioral *state* of a system that results from an action or set of actions. This definition is very high level (covering all actions, not just weapon actions), but also sub-optimal for weaponeering purposes because it does not reference objectives and because it equates effect directly with target state. As detailed in Discussion 3, at the tactical level, weapon effect and target state are very closely related but not equivalent.

(U//FOUO) Every weapon, when triggered, takes an **action** (although some actions may be delayed). The action is intended to have an effect. For an iron bomb, that action is a kinetic explosion and the effect is normally target damage. For a cyber weapon, the action may be the execution of some software and the effects, some form of denial or manipulation. The weapon action may also have outcomes that are not expected and are not required to achieve the objective.

(U) The term *consequences* is suggested here (only for discussion) as a way to describe unintended outcomes, which are normally unrelated to the commander's objectives, although they can be either positive or negative. Unintended outcomes (even positive ones) are usually undesirable because their impact cannot be incorporated into planning. [Note: The argument might be made that consequences could be considered intended if the commander has *a priori* knowledge of non-objective outcomes and continues with the plan anyway. An example might be predicted collateral damage; however the commander's foreknowledge means such damage is more appropriately categorized as a 'collateral effect' rather than a *consequence,* since its impact can be planned for.]

(U) The primary discriminators for labeling outcomes are the commander's military objective and the commander's specific intent with respect to that target. Note that JP 1-02 has a serviceable definition of the term 'objective' so it is not further defined in this Lexicon. Naturally, the principal objective in any military campaign is capitulation of the adversary. Every other objective selected, including cyber objectives, should be subordinate to and supportive of that goal. Because of the complex nature of cyber warfare and the fact that it often insulates its warriors from physical conflict, it is possible for cyber operators to lose track of the physical effects and consequences that may precipitate from their operations. This is particularly true since some of these outcomes may be unapparent to the operator… and in fact may be unknowable by the operator.

Illustration:



(U) In the Illustration, Weapon A creates Effect 1. Effect 1 cascades Effect 2. Effect 2 cascades Effect 3 and generates unplanned *consequences* 1 and 2. Effect 1 is a direct effect of the weapon's action. Effect 2 is a second order effect and Effect 3 is a third order effect. Effects 2 and 3 are also known as indirect effects. Consequence 1 and 2 are third order consequences.

(U) In this example, if Effect 3 is the commander's objective, then Effects 1 and 2 were necessary precursors to achieving the desired Effect. Consequences 1 and 2 are byproducts of the operation and the planning staff did not foresee their occurrence.

(U//FOUO) Because the actions taken by CNA and other similar cyber weapons are virtual, their direct (i.e. first order) effects are virtual effects and not kinetic effects. However, kinetic outcomes (effects) from some cyber weapons can occur as soon as the second order.

(U//FOUO) Not only can effects cascade, they can combine. Application of two separate weapons may create two different first order effects that are designed to interact and cause a second order effect that may not have been achievable with either weapon alone.

(U) While the relationship between the outcome and the commander's objective may be a primary factor for labeling outcomes, another important factor is the status of the target that was affected. 'Collateral damage,' is defined by JP 3-60 as "Unintentional or incidental injury or damage to persons or objects that would not be lawful military targets in the circumstances ruling at the time...". Therefore, following the logic of this discussion so far, outcomes that happen to unlawful targets would be **collateral effects.**

(U) Discussion 3 – Target State

(U//FOUO) Current Joint doctrine does not provide a definition for 'target state,' only 'end state,' which is defined as "the set of required conditions that defines achievement of the commander's objectives." Obviously such conditions could apply to the target or anything else in the operational environment. In order to address the state of the target itself, in a manner that assists mission planners, it is helpful to consider the target (even a human target) as a finite state machine whose states are defined relative to the military objective(s). For instance, a typical cyberspace target could be viewed as a state machine able to exist in any one of five states relative to achieving a commander's primary objective:

- Unconfirmed: Unknown if there is an access path to target.
- Confirmed/Nominal: Access path to target established.
- Unprivileged access: Unprivileged access to target established.
- Privileged access/At risk: Privileged access to target established.
- Goal/Other condition: Target has been placed in the desired or other intermediate condition.

(U//FOUO) It may sometimes be necessary to describe the target as being in states relative to other important factors such as awareness of the attack, level of preparedness/defense, etc. For instance, the target is either aware or not aware of our access, and the target may have fully, partially, or not implemented various defense mechanisms.

(U//FOUO) Having access to such language allows planners and weaponeers to subdivide missions into a logical sequence, assigning different weapons to different tasks, tracking the interaction of weapons, reporting the status of the mission in various phases, and segregating the risk and effectiveness measures of each phase, which may have some level of independence.

(U//FOUO) Therefore, the term '**target state**,' as applied to weapon planning, corresponds to the condition of the target with respect to a military objective. The use of a specific capability or weapon may have an effect on a target, which places (or helps to place) the target in a particular state. Typically, the state of a target is described using fairly abstract terms (i.e. operational, non-operational, compromised, etc.). Having the target in this state, although it may not be the ultimate objective desired by the commander, is intended to be a step towards the desired outcome.

(U//FOUO) As an example, consider the use of a 'buffer overflow' capability to achieve 'root' level (privileged) access on a computer operating system in order to disable an adversary's computer program. A buffer overflow is, by definition, a capability for unauthorized access. Use of the buffer overflow creates an initial effect (access to unauthorized portion of memory) and, by including in the buffer overflow capability other carefully crafted code, it can also enable another effect (e.g. gaining root access) and place the target in a different state. The previous state of the target was "nominal" or "uncompromised." The new state of the target is "compromised." Note that having unauthorized or even root level access was not the commander's objective, but it enables the achievement of that objective. In this case, the effects of the capability were general unauthorized access and opening of a root shell. An additional effect is a state change in the target machine.

Weapon Action	Weapon Effect	Weapon Consequence	Target State
None	None	None	Nominal
Execute code	Unauthorized Access	None	At Risk
Execute more code	Root Shell Established	None	Compromised

(U//FOUO) Now consider the case where the target system administrator has implemented, unknown to our operator, a mechanism to log and report all creations of a root shell. An alert adversary system operator sees the report and notes our activity. This outcome is an unplanned consequence of using the capability. It also changes the target state to one that is now aware of our activity.

Weapon Action	Weapon Effect	Weapon Consequence	Target State
None	None	None	Nominal
Execute code	Unauthorized Access	None	At Risk
Execute more code	Root Shell Established	Target System Operator notification	Compromised and Aware of compromise

(U) Therefore, effect and state are closely related but not equivalent. Perhaps the easiest way to think of the relationship between these terms is that an effect is the transition between states. This correlates precisely with the new JTCG/ME definition of desired effect: *the physical, functional or behavioral change in the state of the enemy that a commander desires to achieve from a lethal or non-lethal attack.*

(U) Discussion 4 – Toward a Common Usage of the Four D's

(U) The terms deny, destroy, degrade, and disrupt have been in common colloquial use throughout the IO community for many years. They have not, however, been formally defined in DoD level doctrine (i.e. they do not appear in JP 1-02 in relation to IO. "Denial measure" and "destroyed" are both defined specifically in relation to kinetic weapons). Various informal (i.e. in the text of JP 3-14) and Service-level definitions have appeared, however these are either inaccurate, imprecise, contradictory, and/or circular. They are also defined, sub optimally, in the Joint Forces Staff College Joint IO Planning Guide from 2002.

(U) For instance:

- Some previously proposed DoD-level definitions defined *degrade* as "permanent partial or total impairment." However, in common usage, the term *degrade* does not imply a time component and degrade rarely means total impairment. The same proposal included a definition of *disrupt* as "temporary impairment" (i.e. not permanent), but fails to give any indication of amount or level. Therefore, these proposed definitions leave the terms *disrupt* and *degrade* overlaping in a manner that is undefined.
- Another recent Service definition of *deny* is "to withhold information about (Blue) force capabilities and intentions from adversaries." This definition forces *deny* to have only an OPSEC meaning and does not correspond with any other common DOD or Service use of the term.
- The Joint IO Planning Guide also errs by attempting to fit the four D's into the four corners of a 'quad chart' that uses time and amount as center axes, thereby forcing *degrade* and *disrupt* to take on non-standard and unintuitive meanings.

This level of imprecision and lack of standardization, if transferred to mission planning, could easily lead to misunderstanding and perhaps even to operational error.

(U) Just as in kinetic warfare, effects of non-traditional weapons can be referred to with respect to three primary variables:

- Scope – the extent or range of desired effect described vis-à-vis specific functional capabilities and/or individuals considered to be the target or target set.
- Level – the amount of the effect. Effects are either partial, represented by a percentage of total capacity or described specifically, or complete (i.e. total).
- Time – the desired start time and duration of the effect. Effects are either temporary or long-term (i.e. permanent or effectively permanent).

These variables (or parameters), combined with a specific target, are the basis for describing most useful military effects.

(U) This simple construct leads to the correct hierarchical effects definition based on the overarching function of denial, where "to deny" is to cause reduction, restriction, or refusal of target operations (irrespective of time or amount). This acknowledges that degrade, disrupt, and destroy are all different forms of denial. Disrupt introduces the time aspect of denial (i.e. less that permanent) and degrade introduces the amount or level of denial (i.e. less than total). Destroy is the special case that includes the maximum time and maximum amount of denial.

(U) To illustrate by use of kinetic example, consider the tactical order to *deny* the use of a bridge to an adversary:

- This could be done temporarily by *disrupting* traffic flow by attacking and disabling bridge traffic to block the bridge.
- This could be done partially by *degrading* the bridge structure so that it will only support light vehicles and foot traffic.
- This could be done by *destroying* the bridge.

Each of these is an effective form of denial, depending upon the commander's objective. These definitions also allow useful combination of effects, whereby a target may be both disrupted and degraded (e.g. "the flow of traffic on the bridge is to be stopped for three hours and thereafter limited to vehicles under 2 tons"). Since the goals of most cyber campaigns are also effects-based, the precision description of a cyber mission requires an ability to describe those effects in unambiguous terms. (Note that our operational objective might also be accomplished via a deceptive form of manipulation, i.e. by placing a sign on either end of the bridge claiming that the bridge had been mined.)

(U) Quantitatively, denial (D) can be expressed as a function of scope *(s)*, level *(l)*, and time *(t)*, i.e. $D_{(s,l,t)}$. Defining effects in this manner makes it clear to the planning staff that each of the parameters of the function must be considered and specified as necessary as indicated by, or derived from, commander's objective. As the level *(l)* or amount approaches 100% and time *(t)* approaches infinity, destruction is achieved. Time can be just a duration (implying it should begin ASAP), a start time with a duration, or a start and stop time. Since destruction is an effects-based concept that will vary by mission, mission planners must decide both the amount and duration required to achieve destruction. Note that this is no different than the kinetic example, since even destruction of a bridge is not permanent, it is only "effectively permanent," based on the timeframe of the campaign and the time and resources required to rebuild it.

(U//FOUO) Some examples of cyber mission tasking stated using this construct:

- Degrade throughput on all channels of a microwave communications tower at specified GPS address by 75% beginning at 0630 for 3 hours.

- Disrupt Internet service at a named cybercafe from 2130 until 2145 for the next 3 days.
- Destroy the 80GB hard drive at IP address 207.10.132.15 tonight after 2300 but before 0430.

Note that each Denial effect has a scope, amount, and time either stated specifically or unambiguously implied. (Also note that only the third effect can be considered 'damage.')

(U) Discussion 5 – Function vs. Effect

(U//FOUO) It is natural to assume that cyber weapons can be easily sorted or classified by the effects they can create. If this were true, then it would be a simple matter of selecting a weapon that claimed to produce effect A for an OPLAN that required effect A. However, as described in Discussion 1, many cyber weapons, considered in isolation, have significant environmental dependencies, and any claims of action or effect mean little unless they are accompanied by a thorough analysis of these dependencies and unless they are considered in concert with a detailed analysis of a specific operational environment.

(U//FOUO) An additional liability of selecting a weapon based solely on its claimed effect is the possibility of an implied warranty of effect. When an iron bomb fails to explode, there is a significant likelihood that a manufacturer's defect is to blame. However, if a combatant commander's planner selects a 'disrupt' cyber weapon and it fails to disrupt because the weapon's environmental assumptions were not verified to be present on the target, we cannot blame the weapon developer for such a failure.

(U//FOUO) Because of the difficulty of guaranteeing effects, cyber mission planning also requires that cyber weapons be documented by the technical functions they implement. This functional description should be straightforward and easy to determine, assuming we have access to a 'functional claims' document or other similar developer documentation. Since the technical functions implemented in the weapon are (or are supposed to be) derived from some type of requirements, the developer's functional claims for their weapon should clearly map back to those requirements and carry forward into the developer's testing process. For most types of weapons, verification of this functional mapping should take place during the Weapons Characterization process, and documentation of these functions is important for enabling the mission planners to do weapon/target pairing.

(U//FOUO) Describing the effect(s) of using a cyber weapon is not nearly so straight-forward as determining its functions, since its effects depend not only on whether or not the developer's environmental assumptions and expectations have been properly characterized and satisfied by the operational environment, but also how well the target itself has been characterized. For example, a cyber 'disrupt' weapon may be selected for the intended effect of "tying-up adversary network," but the technical function it implements is "degradation through packet flooding," and the environmental assumption may be a maximum data bus speed and a maximum input/output processor throughput on the target.

(U//FOUO) This does not mean that cyber weapons shouldn't be classified by intended effect. On the contrary, sorting weapons by their intended effects (see Discussion 6) is an important distinction for cyber warfare planners. The key is not to let weapons employment decisions be made by effects claims alone. The intended effects and the technical functions implemented should be used together to ensure thorough planning, sufficient investigation of the target environment, and to offer the greatest chance of mission success.

(U) Discussion 6 – Sorting Cyber Warfare Capabilities

(U//FOUO) The terms *characterization*, *classification*, and *categorization* have sometimes been confused and freely interchanged when discussing the organization, preparation, and selection of cyber warfare capabilities. Because of the wide number of different cyber capabilities, their extensive environmental dependencies, and the special release authorities involved, each of these terms has come to have a distinct meaning in the cyber warfare context.

(U//FOUO) Weapons **characterization** is defined by the JTCG/ME as:

> *"Quantification of damage producing mechanisms and reliability of munitions."*

Substituting the term effect for damage (see Discussion 7), it is clear that characterization involves examining the features of the weapon that create the effect and the features that affect its reliability. Of course, software weapons don't share all of the same reliability factors as kinetic weapons. Software is either designed correctly or it is not. Software reliability is primarily connected with design flaws and environmental incompatibilities, not breakage, rust, deterioration, or a jammed launcher caused by lack of maintenance.

(U//FOUO) A substantial part of the necessary weapons characterization for CNA capabilities is done by the preparation for and execution of the technical assurance evaluation (ref. DODDIR 3600.03). This evaluation requires evidence that the weapon's claimed functions have been implemented correctly ("damage producing mechanisms") and evidence that all requisite assurance factors have been considered and documented ("reliability of munitions"). Some additional characterization factors are uncovered by OPEVAL procedures and other post-technical assurance events. This same type of assurance evaluation is possible for most types of cyber warfare capabilities.

(U//FOUO) The sorting of cyber warfare capabilities into broad operational classes based on intended outcomes is necessary for mission planning discussions (see Discussion 5). This is a type of weapons classification, however, since the term 'classification' is too easily confused with security classification, the term '**Intended Cyber Effects**' is used instead. Intended outcomes such as Denial, Manipulation, Exploit, Access, Enabling, etc. are useful ways to sort capabilities for the initial stages of the weapon selection process.

(U//FOUO) Based on language in the original SECDEF IO Roadmap, **categorization** has come to mean the sorting of weapons based on various risk factors for the purpose of determining releaseability. The IO Roadmap suggests three Categories: Category I for combatant commander release; Category II for inclusion in an existing OPLAN; and Category III for President/SECDEF release.

(U) Discussion 7 – Is Damage the Only Effect?

(U) In its JTCG/ME Publication 1-8 (Requirements for ... Vulnerability Data), the JMEM Program Office lists over 40 different kinds of damage-related combat kills for kinetic weapons. In order to establish credibility with combatant commanders and their staffs, the cyber warfare community should consider the meaning of these (and other) traditional terms to determine if the logic of the term can be applied in a straightforward manner to non-traditional weapons or the meaning can be adapted to include the cyber applications of the term. However, the singular focus on damage as the only effect makes this reutilization of terms difficult.

(U) All of the existing kill terms are based on the concept of damage, but damage is not often the best way to describe the objective effect of a non-kinetic mission. In addition, many of the kill term definitions include specific target types, such as aircraft, submarines, hardened structures, industrial process facilities, etc. In order to apply such terms directly to cyber warfare, a determination should be made about whether or not it's useful to retain such narrowly defined expressions of effects. And even before considering JMEM specific terms, other more widely used weapons effectiveness language should be reviewed to determine its ability to support EBO. Starting at the very top of the list is the near universally recognized term battle damage assessment (BDA).

(U) The question is often heard in the cyber warfare community, "How will we determine BDA for cyber capabilities?" Perhaps a better first question would be: "What are we actually assessing?" The term '*battle damage* assessment' implies that the outcome of a military operation must be damage and that the context of the operation was a 'battle.' JP I-02 defines battle damage assessment as:

> (U) "*The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment.* "

(U) Aside from the focus on damage, the overall intent of the definition seems plausible for non-traditional weapons. A slight modification to a term like '*tactical effect* assessment,' or simply '*effect* assessment,' makes more sense in the non-kinetic weapons context, and even in the broader '*effects* based operations' context, and because it is used to calculate 'measures of *effect*iveness.'

(U) Defined this way, the term retains whatever utility it had for kinetic planning and is now also applicable to cyber planning as well. It is interesting to note that traditionally, BDA is expected to be only an estimate. It remains to be seen if an estimate of effect will be sufficient for cyber planning and re-strike analysis.

(U//FOUO) Also germane to this discussion is the notion that the intelligence community (IC) is primarily responsible for kinetic BDA, since the sources and analysis of the IC are required to construct BDA and those resources are clearly separate from the resources used to conduct the strike. Therefore, the mandate for coordination between intel and ops has been embedded within the definition itself. For cyber warfare, this intel/ops distinction is more difficult to make. In the network domain, the resources used for intelligence collection, strike, and target analysis are often all the same. This should however, make the intel/ops coordination easier rather than harder and it would not require further modification to the definition.

(U) Based on these concerns, an updated definition of Effects Assessment (EA) or Tactical Effects Assessment (TEA) might look something like this:

> (U) *"The timely and accurate evaluation of effects resulting from the application of lethal or non-lethal force against a military objective. Effect assessment (EA) can be applied to the employment of all types of weapon systems (air, ground, naval, special forces, cyber, and special effects) throughout the range of military operations. Effects assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Effects assessment is composed of physical effect assessment, functional effect assessment, and target system assessment. Battle damage assessment (BDA) is a specific type of effects assessment for damage effects."*

(U) Two other definitions implemented within the kinetic JMEM community are Fractional Damage and Probability of Damage, with the following definitions:

- (U) **Fractional Damage** (FD) - *the average fractional damage (kills/incapacitations) achieved on an area target after being attacked by N volleys or passes. This can be thought of as the average fraction of the targets elements killed/incapacitated. FD1 is the same but for one volley/pass.*

- (U) **Probability of Damage** (PD) - *The probability (chance) of damage (kill, incapacitation or interdiction) to a unitary (single) target, a target site or a linear target after being attacked by N volleys or passes. PD1 is the same but for one volley/pass.*

(U) The alternative term to be used within IO JMEM is:

- (U) **Probability of Effect** (PE) – *The probability (chance) of effect (functional or behavioral impact) to a target(s) given an action. (If damage is the desired functional impact, then PD and PE are equivalent.)*

(U) Discussion 8 – Re-Design vs. Re-Configure

(U//FOUO) One of the oldest axioms of combat is that the initial OPLAN never survives first contact with the enemy. The impact of this truth on cyber warfare occurs when an operator encounters changes or other difficulty on target and tries to compensate by modifying the weapon 'on the fly.' The presumption that this can and should be an acceptable state of affairs assumes either extraordinary technical skill on the part of the operator or an extraordinarily tightly coupled operational relationship between the shooter and the developer. Broad acceptance of either of these scenarios will likely prevent the transformation of cyber warfare into a core military capability. First, the training challenge represented by the requirement for an operator to be able to modify an arbitrary cyber weapon is probably insurmountable. Second, the connectivity challenge of linking the operator with the developer under all circumstances is equally daunting. And third, the difficulty of meeting the requirement for post-modification regression testing and updating of the technical assurance evaluation may mean that these steps are skipped, thereby increasing the risk of using the modified weapon.

(U//FOUO) When this 'fix on the fly' strategy is used, it is usually because the design of the weapon did not allow sufficient (or any) operator reconfigurations as may have been required by target changes. Part of the duty of cyber weapon developers is to understand the potential target environments, and the impact of environmental changes, on the operation of their weapon. Clearly not all contingencies can be planned for, but a thorough analysis of likely challenges and their impact on the weapon should be considered, and reconfigurability sufficient to overcome these obstacles must be a part of the design trade-offs. To the extent that the weapon is designed to be reconfigured in use by the operator, its testing and evaluation will include this capability, and any such reconfigurations will not require the skills of a developer or the need for retest/reevaluation.

(U//FOUO) Obviously, a weapon of unlimited flexibility would be too expensive and impractical. Therefore, design trade-offs must be made. One consideration is the resulting size of the code. A design requirement for a software weapon to be as small as possible will argue against increasing its size to include reconfiguration features. This would not preclude, however, providing multiple versions of a capability in advance, each with code variations based on likely variations to be found on target. Another consideration is the nature of the reconfiguration mechanism. For instance, requiring an operator to recompile a software weapon in order to accomplish its reconfiguration is problematic. Issues of which compiler is used, who owns the license, and how that compiler changes the attribution and other characteristics of the weapon will all complicate the process and reduce the likelihood of a completely successful reconfiguration.

(U//FOUO) This reconfigurability characteristic of a weapon is directly related to its environmental expectations and assumptions. The more flexible the weapon, the fewer environmental dependencies it will carry. Therefore, we define the term **Cyber Weapon Flexibility** as the extent to which the weapon's design enables reconfiguration by the operator to account for changes in the target environment.

(U) Discussion 9 – What Kind of Warfare Is It?

(U//FOUO) A majority of capabilities that will initially make up the family of cyber warfare weapons will come from the disciplines of CNA and EA. Due to the rapid expansion and coincident integration of computers, digital communications, and other cyber-related technology, the current JP 1-02 definitions of EA and CNA no longer provide sufficient distinction to effectively label an increasing number of weapons as either EA or CNA. EA and CNA are both forms of 'information technology attack' or 'data attack,' however, based on employment authority decisions, there is currently a requirement to be able to clearly distinguish between them.

(U//FOUO) The EA definition includes methods (electromagnetic energy, directed energy, or anti-radiation), targets (personnel, facilities, or equipment), and effects (disrupt, deny, degrade, or destroy). The CNA definition includes only targets (information, computers, networks) and effects (disrupt, deny, degrade, destroy). Not only is the CNA definition less complete, the targets and effects portions of both definitions include considerable overlap. This allows labeling of weapons that use RF to degrade or destroy (i.e. deny) digital information bearing equipment as either EA or CNA.

(U//FOUO) An additional related issue is associated with the designation of 'fires.' In JP 1-02, EA is designated as a form of fires and CNA is not. However, the definition of fires is simply the "effects of lethal and non-lethal weapons," which clearly includes CNA.

(U//FOUO) EA and CNA can both target information systems, or, in accordance with the JP 3-13 definition of IO, "automated decision-making." Traditionally, EA has targeted radars, data links, and other forms of command, control, and communications systems by entering through the RF data stream (data in motion). However, most of these target types are transitioning from analog to digital technology. CNA can target these same systems as well as computers and computer networks by modifying the static data (instruction sets, databases, etc.) and/or data in motion, using both wired and wireless (RF) access. Given this overlap, no absolutely distinctive high-level definitions of EA and CNA appear possible without restricting either EA or CNA from certain specific operations already being done.

(U//FOUO) Existing definitions attempt to distinguish between the two by describing examples of each, but the examples used have been overcome by technology and are now of little value. This identity conflict has already begun to impact the operational community and will continue to do so until both types of capabilities are either clearly distinguished or are simply merged under the construct of cyber warfare. This Lexicon suggests the latter.

(U//FOUO) The NMS-CO and the emergence of the cyber warfare construct present the opportunity to discontinue the EA/CNA distinction at the planning and operational level. Based on the inexorable march of technology and the melding of these technologies, the best long-term solution is the merger of CNO, EW, and any other related cyber disciplines into the combined area of cyber warfare, where CNA and EA would simply co-exist on a continuum of offensive cyber warfare capabilities. (Note that the only exception to this new construct would be the directed energy forms of EA that are not specifically designed to target information systems. However, these non-traditional kinetic weapons are already grouped together under the munitions effectiveness category of directed energy/non-lethal (formerly Special Effects (FX)) weapons.)

(U//FOUO) In addition to CNO and much of EW, there are aspects of non-kinetic space control–negation (SC-N) that fit this same model. Merging these warfare areas into Cyber Warfare suggests the terms Cyber Attack (CA) to combine CNA and EA, Cyber Exploit (CE) to combine CNE and ES, and Cyber Defense (CD) to combine CND and EP. Note that since EA has traditionally combined both kinetic and non-kinetic approaches to attack, the term CA would maintain this flexibility. Since creation of effects in cyberspace can be done using either kinetic or non-kinetic capabilities, if a specific technique is required (or is to be excluded), this must be specified. (See Discussion 15.)

(U) Discussion 10 – Delivery Considerations

(U) The JTCG/ME defines delivery accuracy as the measure of a weapon system's capability to place munitions on target, and further describes it as the factor that characterizes the operational employment efficiency of a weapon. An underlying assumption of delivery accuracy analysis is that the location of the target is established and the challenge is on-target delivery of the weapon to that location. Delivery accuracy analysis is broken down into two major categories of weapons: guided and unguided.

- (U) An unguided weapon is one that, after release, relies entirely upon the laws of physics to reach its target. (Unguided weapons may be stabilized but stabilization is not a target-related input.)

- (U) A guided weapon has some method to receive and execute post-release course corrections in order to achieve greater delivery accuracy. The purpose of guiding weapons is to increase the accuracy and therefore the effectiveness of the weapon (the side benefits of increased accuracy are reduced unintended/collateral effects and reduced operating costs via fewer weapons expended per effect).

(U//FOUO) These definitions do not correspond directly to types of offensive cyber weapons, nor does the overall premise that employment efficiency is an important targeteering factor. Kinetic weapons are generally expensive and have mass and consequently represent a limited resource. Therefore, it is important for kinetic targeteers to use only the number of weapons required to achieve the commander's objective. Cyber weapons are information weapons whose direct effects are non-kinetic and whose delivery happens over wired and/or wireless information paths. As it turns out, this wired/wireless distinction is also a primary factor impacting the delivery accuracy of cyber weapons. Since cyber weapons deliver information or some other information-related effect to the target and not high explosive or high energy, as long as we have electrical power, we will not 'run out' of a (software) cyber weapon. Ironically, our essentially unlimited ability to re-fire cyber weapons is of little value since, if we fired it once and did not achieve the intended effect, firing it one thousand more times generally will not increase our odds of success. Therefore, we must think of the requirements for weaponeering a cyber target based on the delivery accuracy of cyber weapons from a different perspective.

(U//FOUO) There are some offensive cyber operations that rely on a combination of wireless and wired delivery. In such cases, the mission planning must treat each segment separately. And note that the whole concept of guided/unguided applies only to remotely launched cyber weapons. If a network target has already been accessed and subverted and our operators have unrestricted access, an implanted weapon can be considered like a mine or an improvised explosive device (IED) where there are no longer any delivery considerations for the weapon, but only survivability and transferring of commands and updates (i.e. C^2).

(U//FOUO) Although RF (wireless) signals can be directional, they cannot be guided in the sense that some kinetic weapons can be steered. The minimum criteria for selecting a wireless target is an RF frequency and, even though the frequency selected for the attack will limit the potential targets to those that receive on that frequency, this is not selective enough to be considered a form of guidance. Even techniques used to increase effectiveness and reduce collateral consequences of wireless capabilities (e.g. adjusting the signal strength, adding specific modulations, and using directional antennas) do not necessarily provide assurance of reaching only the correct target. Therefore, to whatever extent the cyber attack is wireless, it has a sort of 'unguided' component.

(U//FOUO) In contrast, all wired cyber attacks must be guided to some degree because the protocols used to route network traffic require that a guidance scheme be followed. Network targets are selected by network address (and usually, port number). However, network attacks, although 'guided,' can still be indiscriminate due to the nature of network addressing formats. For instance, a ping flood attack can be directed at a single IP address or broadcast to a whole Class B IP domain with thousands of recipients.

(U//FOUO) Another unique feature of cyber weapons is their susceptibility to environmental conditions (i.e. 'cyberspace atmospherics'), both real and virtual. Unguided kinetic weapons are affected by few environmental conditions, mainly gravity, wind, and rarely, precipitation. Cyber weapons that rely on wireless delivery are subject to more complex atmospherics that impact RF signals (ducting, bounce/skip, absorption, multi-path, etc.). Wireless weapons can be completely subverted by poor environmental analysis and planning.

(U//FOUO) Weapons that rely on wired delivery are subject to the 'atmospheric' conditions of the network. Complex networks (like the Internet) have continuously varying environmental conditions that can impact our ability to deliver a network weapon. Network segments go up and down for maintenance or repairs, segments become crowded, segments can be purposely interfered with, and new segments are constantly being created. Therefore, even though an attack delivered over the Internet is 'guided,' the exact path from launch platform to target is often indeterminate. In any highly reliable network, these conditions rarely keep a weapon from finding its target but they may affect the delivery timing.

(U//FOUO) Therefore, assuming the target location has been accurately determined through intelligence, the primary factor impacting delivery accuracy analysis of cyber weapons is the **delivery mode:** remote launched vs. implanted, and for the remote launched category: wireless vs. wired, and for the wireless sub-category: delivery accuracy factors (directionality, gain) that are applicable to mission planning.

(U//FOUO) By definition, delivery of first order effects always requires some form of access to the target, whether wired or wireless, privileged or public (i.e. unprivileged). For example, if denial of a target can be achieved by unauthorized root access on the target itself, then our desired effected is a first order effect created by privileged access. If privileged access in not possible, we may still be able to create our desired effect in the first order by using public access to the target. An example of this is a distributed denial of service (DDOS) that floods a port on the target. The first case is **privileged access enabled** (PAE) and the latter is **privileged access independent** (PAI).

(U//FOUO) Often, when the intended target cannot be directly accessed via either public or privileged means, the desired effect can still be achieved by targeting an intermediating link or node so that the desired effect cascades from the first order effect. Therefore, if we desire to create a denial of service effect but can't (or don't want to) access the target node "A," we may still be able to isolate the target by conducting a DDOS attack on a critical link "B" leading to the target. While it is technically correct to call this PAI attack on A, that is an incomplete and therefore potentially misleading description. More properly, it is an attack (either PAE or PAI) on B with cascading PAI effects on A.

(U) Discussion 11 – Targeted Vulnerabilities

(U) The description of vulnerability is another illustration of the inherent differences between traditional and non-traditional warfare. Recall from Discussion 7 that traditional JMEM documents only discuss one category of vulnerability: damage effects resulting from the blast and fragmentation actions of the weapon. The actions of cyber weapons are so much more varied because there are so many categories of weakness to exploit in information systems. This is why the meaning and use of the term vulnerability is different and important in cyberspace.

(U) JP 1-02 has collected three different vulnerability definitions from various sources and mission areas; one of them has some value going forward. Vulnerability definition (3) is the one that applies to cyber warfare: "*In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system.*" This definition contains the correct essence of the term but makes the classical lexicon error of "failing to stop when finished."

(U) Within the context of information systems security, and by extension the entire IT and cyber community, the definition of vulnerability has two key components. The first is the notion of a weakness. Most modern complex systems have design weaknesses somewhere in their internals or in their interfaces. This is a result of the need to reduce the cost/time required for design, build, and test as well as the natural tendency of humans to make mistakes. However, simply identifying a target's weakness does not mean we are ready to declare victory. The second equally important component of vulnerability is that the weakness must be exploitable.

(U) Until we have determined how to both identify *and* reach a target's weakness, we have not established the target's vulnerability. As an analogy, long borders may be a weakness in a nation's security posture, but if they can be effectively guarded, the nation is not vulnerable. Similarly, if an information system has a known, uncorrected design flaw but the system is protected by an external firewall or guard that makes access to the flaw impossible, then that weakness does not represent a vulnerability. Therefore, in the context of cyber warfare, a **vulnerability** is an exploitable weakness.

(U) Returning to the JP 1-02 definition, the notion of exploitable weakness is clearly there, however, it is accompanied by an unnecessary limitation both in the location of the weakness (*security design, procedures, implementation, or internal controls*) and the intended effect of its exploitation (*unauthorized access*). There are clearly information systems that have weaknesses in areas other than security design, procedures, implementation, or internal controls that lead to effects other than unauthorized access. The result of "over-thinking" the definition results in one with restricted utility. In addition, use of the auxiliary verb "could" implies that the exploitability of the weakness is only theoretical, which is incorrect. A vulnerability is a weakness that *can* be exploited. If the exploitability has not yet been determined, there is not necessarily a vulnerability.

(U) Note that a given mission may require identification and exploitation of multiple vulnerabilities in order to achieve the military objective. Commonly, there is a key weakness that must be exploited in order to accomplish the actual effect or objective, but in order to gain access to the part of the system that has this objective-related weakness, we must first get access to the system. This often entails exploitation of a different weakness or set of weaknesses. Therefore, in addition to the high-level term *vulnerability*, there are more specific **objective vulnerabilities** and **access vulnerabilities** that address these requirements.

(U) Also note the distinction between the terms 'target vulnerability' and 'targeted vulnerability.' The former is target-centric and is simply an exploitable weakness that is known to exist in the target. The latter is weapon-centric and is an exploitable weakness that is required to be present in order for the selected weapon to have the desired effect (in other words, the specific vulnerability that is targeted by the weapon). Clearly, matching target vulnerability to targeted vulnerability is the essence of effective weapon/target paring.

(U) Discussion 12 – Cyber Weapon Vulnerabilities

(U//FOUO) The design and operational environment of cyber weapons (CNA capabilities in particular) can result in a variety of vulnerabilities inherent in the weapons themselves. These vulnerabilities are of a type mostly unfamiliar to the kinetic weapons community, and are due to the complexity of the weapons, the dynamic nature of the "atmosphere" of cyberspace, and the difficulty of gathering detailed intelligence about cyber targets. The destructive action of kinetic weapons is intuitive and comparatively crude. The non-destructive action of many cyber weapons is unintuitive, complex, and precise. This combination of circumstances has created new categories of weapon vulnerabilities.

(U//FOUO) Even though kinetic and non-kinetic weapons both have signatures, combatants are rarely concerned with residual signatures of kinetic weapons since kinetic warfare is hard to conceal and the participants' identities are, almost always, known to one another. Warfare in the realms of information frequently requires stealth and anonymity due to the sensitivity and preemptive nature of the operation. Not only is the operation itself sensitive, but also very often so is the technology used to achieve the commander's objective. And even though kinetic technology can also be quite sensitive, it rarely survives weapon delivery. As result, planners and decision-makers often raise concerns about detection, attribution, and other issues related to cyber weapons that are not factors in kinetic planning.

(U//FOUO) Because the barriers to entry to war in cyberspace are so low, it is a crowded battlespace and our capabilities are not necessarily any more sophisticated than those of our adversaries, allies, and other associated or unassociated participants. After the commander's desired effect has been created, in many cases the nature of the effect will mean that the effect will be detected. This does not mean that the capability or weapon itself has been detected or that the operation has been attributed. These are all separate conditions that, though related, are tracked independently. The crowded nature of cyberspace and the proliferation of anonymizing technologies can work to both our advantage and disadvantage, in that attribution can be very difficult for both our adversaries and ourselves. Suspicion, which can be based on circumstances and emotions, is not the same thing as attribution, which requires evidence.

(U//FOUO) The following primary areas of technical vulnerability risk are associated with the design of cyber weapons. These technical risks are complicated and sometimes magnified by environmental interactions, and other risk areas may arise when such weapons are stored, transported, and operated. In particular, for CNA weapons, analysis of this technical risk should be accomplished by the developer and then evaluated during the technical assurance evaluation portion of weapon characterization. Additional risk analysis is always necessary once an actual target or operational environment is selected.

- (U//FOUO) **Detectability** risk – The risk that a weapon will be unable to elude discovery or suspicion of its existence. This includes the adverse illumination risk of hardware weapons.
- (U//FOUO) **Attribution** risk – The risk that the discoverer of a weapon or weapon data will be able to identify the source and/or originator of the attack or the source of the weapon used in the attack.
- (U//FOUO) **Co-optability** risk – The risk that, once discovered, the weapon or its fires will be able to be recruited, used, or reused without authorization.
- (U//FOUO) **Security Vulnerability** risk – The risk that, once discovered, an unauthorized user could uncover a security vulnerability in the weapon that allows access to resources of the weapon or its launch platform. This includes the risk of an adversary establishing covert channels over a weapon's C2 link.
- (U//FOUO) **Misuse** risk – The risk that the weapon can be configured such that an authorized user could <u>unintentionally</u> use it improperly, insecurely, unsafely, etc.
- (U//FOUO) **Policy, Law, & Regulation** (PLR) risk – The risk that the weapon can be configured such that an authorized user could <u>intentionally</u> use it in violation of existing policy, laws, and regulations.

(U) Discussion 13 – Manipulation: The Other Effect

(U//FOUO) Although denial is the offensive cyber effect that receives most of the attention, manipulation is equally important and potentially more effective in combat. Where denial is fundamentally about preventing an adversary from using (typically) their own resources, manipulation is about using, without authorization, adversary resources to support our own mission objectives. Note that the targeted system may appear to continue to function nominally for the adversary while we manipulate it, unlike a denial operation where the reduction in target utility is usually readily apparent to the subject of the attack.

(U//FOUO) As with the illogic and confusion that surrounded the meaning of the four D's, current doctrine has improperly subordinated the term manipulation to deception. The two terms are closely related, but deception is a subset of manipulation. Unfortunately, deception is defined in JP 3-58, Joint Doctrine for Military Deception, as *"those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests."* This definition is overdue for replacement for the following reasons:

- it subordinates manipulation under deception, instead of vice versa;
- it too specifically describes the object of deception as "the enemy," which, although typical, may not always be the case;
- it refers to the mechanism of deception as "evidence" but does not define what that is;
- it limits deceptive actions to those that cause the target to act prejudicial to his own interests, which is not fundamental to the meaning of the term and is therefore overly limiting.

(U//FOUO) An improved definition would recognize that manipulation is the overarching effect and would specify the fundamental characteristics of the actions required to manipulate. In stating that "Deception planners must possess fertile imaginations and the ability to be creative …", JP 3-58 acknowledges that this is an area of military endeavor that is more of an art that a science. Manipulation is also inherently not "above board." It is sneaky, unfair, and insidious. If it were not so, it would not be effective. But primarily, in the domain of cyberspace, manipulation is about accessing and using other people's information and information systems to do our bidding. Whether or not they ultimately continue to do the owner's bidding may be immaterial to our objective.

(U//FOUO) Therefore, one potential definition, to replace deception in the next update of the Joint Pubs, is: **manipulation** – *"To influence, control, or change a target's operation in a manner that supports the commander's objectives. Iincludes deception, decoying, conditioning, spoofing, falsification, etc. Manipulation is concerned with using an adversary's resources for friendly purposes and is distinct from influence* *operations (e.g. PSYOP, etc.).*" This definition does not tie manipulation to action that is directly prejudicial to the target, only that it support our objective.

(U//FOUO) Although it is overdue for an update, much of the other content of JP 3-58 remains valid. The definition of MILDEC itself is still correct since MILDEC is narrowly defined as an activity that specifically misleads others about our military intentions.

(U) Discussion 14 – When Things Go Wrong

(U//FOUO) During times of crisis or pending mission failure, it is important to be able to communicate clearly and without emotion; however, the advent of failure does not always encourage complete transparency. Back when Rolls Royce was still an English concern and their cars were the apogee of sophistication and quality, employees of the company were discouraged from referring to one of their cars as "broken down" or "disabled." A Rolls Royce simply "failed to proceed." A similar level of discomfit may result within government any time a cyber attack is approved and launched, and then does not "proceed" as anticipated. A cyber capability developer, operator, or release authority may be reluctant to admit failure in such circumstances but should be encouraged to speak plainly. Certain weapon failure terms are already in common use and must be considered for adaptation and application to non-kinetic weapons.

(U//FOUO) In addition to the possibility of consequences as described in Discussion 2, there is always the chance that nothing will happen (or seem to happen) when a cyber weapon is triggered. When a kinetic weapon fails to launch or, if launched, fails to detonate, everyone stays far away until they are sure the weapon is inert or safed. When a cyber weapon fails to take an action, even though there may be little fear of physical injury, the potential for bad publicity (or worse) will loom until assurance can be provided that there was no harm and therefore no foul. Since it is quite often impossible to prove a negative (i.e. one can rarely prove that no adversary noticed an aborted attempt at CNA), the better the weapon and the operational environment have been characterized, the easier it will be to: assure leadership that everything is under control; diagnose the failure; and perhaps determine the need for additional intelligence or other remediation.

(U) The kinetic munitions community has a time-honored term to described failed weapon activations: misfire. JP 1-02 defines misfire as *"failure to fire or explode properly; failure of a primer or the propelling charge of a round or projectile to function wholly or in part."* This definition is straightforward and functional, but since we rarely are looking for cyber weapons to actually explode, a revision will make it useful to all weapons communities. **Misfire** is therefore the failure of a weapon to take its designed action; failure of a primer, propelling charge, transmitter, emitter, computer software, or other munitions component to properly function, wholly or in part.

(U) Another common weapon malfunction term found in JP 1-02 is dud, an *"explosive munition which has not been armed as intended or which has failed to explode after being armed."* Again, altering so as to be more inclusive of modern weaponry renders **dud** as a munition that has not been armed or activated as intended, or that failed to take an expected action after being armed or activated.

(U) Discussion 15 – Kinetic Does Not (Necessarily) Equal Lethal

(U) Without definitive explanations of the terms kinetic, non-kinetic, lethal, and non-lethal in Joint doctrine, it has become common practice to equate the terms kinetic and lethal and the terms non-kinetic and non-lethal. While there certainly is a relationship between these terms, it is not true that they are synonymous. In fact, their distinction is a critical one for effects based planning and operations, particularly in cyber warfare.

(U//FOUO) The key to deconflicting these terms lies in the traditional meaning of the words themselves. Fundamentally, kinetics is the study of bodies in motion and the forces that create these motions, and is a subset of physics, the study of the interrelationship between matter and energy. Therefore, kinetic weapons are those that exploit the laws of physics to create their direct effect. Note that electromagnetism is a branch of physics (e.g. "radio physics"), therefore many traditional EA techniques, including broadband jamming, may be considered a form of kinetic warfare ("kinetic RF"). Non-kinetics then, are any other type of capability. The primary forms of non-kinetic warfare come from the IO disciplines of CNA, some EA techniques, and PSYOP. What gives a CNA weapon its effect is the application of the laws of logic, vice the laws of physics. In other words, creation of a CNA effect requires logical access to a target in addition to physical access. (Some sort of wired or wireless physical access is always required in CNA in order to deliver the capability and create the first order effect.) What gives a PSYOP capability its effect is careful selection of a convincing message that gains access to the logic or emotions in the mind of the target. Application of kinetic weapons requires only physical access to the target. These facts lead to the following definitions: **kinetic weapons** are those that use forces of dynamic motion and/or energy upon material bodies; **non-kinetic weapons** are those that do not do this, i.e., they create their effects based upon the laws of logic or principles other than the laws of physics (e.g. CNA, PSYOP, etc.). Note that the effects of chemical and biological weapons could also be considered non-kinetic.

(U) Like kinetics, the lethality of weapons is fundamentally tied to the intent of the weapon designer. Lethal weapons are those designed to kill. Although some dictionaries have allowed the notion of "facility damage" to creep into their definition of lethal, it is not central to either the historic or common usage of the word. If we did not care if weapons killed people, we would have no reason to discuss their lethality. As society has become increasingly concerned with the inhumanity of warfare, increasing attention has been paid to the development and use of non-lethal weapons. Such weapons either are not designed to kill people (although when used inappropriately their application can sometimes be fatal) or cannot be used to target humans directly. An example of the former is a fin-stabilized rubber shotgun projectile and an example of the latter is a CNA weapon. Therefore, **lethal weapons** are those whose primary effect is expected to cause fatalities. **Non-lethal weapons** are those whose primary effect is not expected to cause fatalities, rather to incapacitate, deter, influence, or repel personnel, or to deny or manipulate material, functions, or information. The effects of non-lethal weapons may be reversible and are not required to have zero probability of causing fatalities, permanent injuries, or destruction.

(U) In addition to describing the nature of weapons, the terms kinetic and lethal (and their negative counterparts) are equally useful for describing effects. Just as there are kinetic weapons and kinetic effects, there are lethal weapons and lethal effects. Perhaps the clearest way to illustrate the application of these terms is by example, and the following are offered:

- lethal kinetic weapon: Mk 84 bomb
- non-lethal kinetic weapon: Active Denial System (ADS)
- lethal non-kinetic weapon: Poison applied to adversary water supply
- non-lethal non-kinetic weapon: CNA software weapon

(Note that the order of the adjectives does not change the meaning, merely the emphasis, therefore a 'lethal kinetic weapon' is synonymous with a 'kinetic lethal weapon.') Likewise, effects can be described similarly:

- lethal kinetic effect: kill adversaries by explosion
- non-lethal kinetic effect: deter adversaries by force without killing them
- lethal non-kinetic effect: kill adversaries without damaging infrastructure
- non-lethal non-kinetic effect: remotely deny adversary access to their data networks