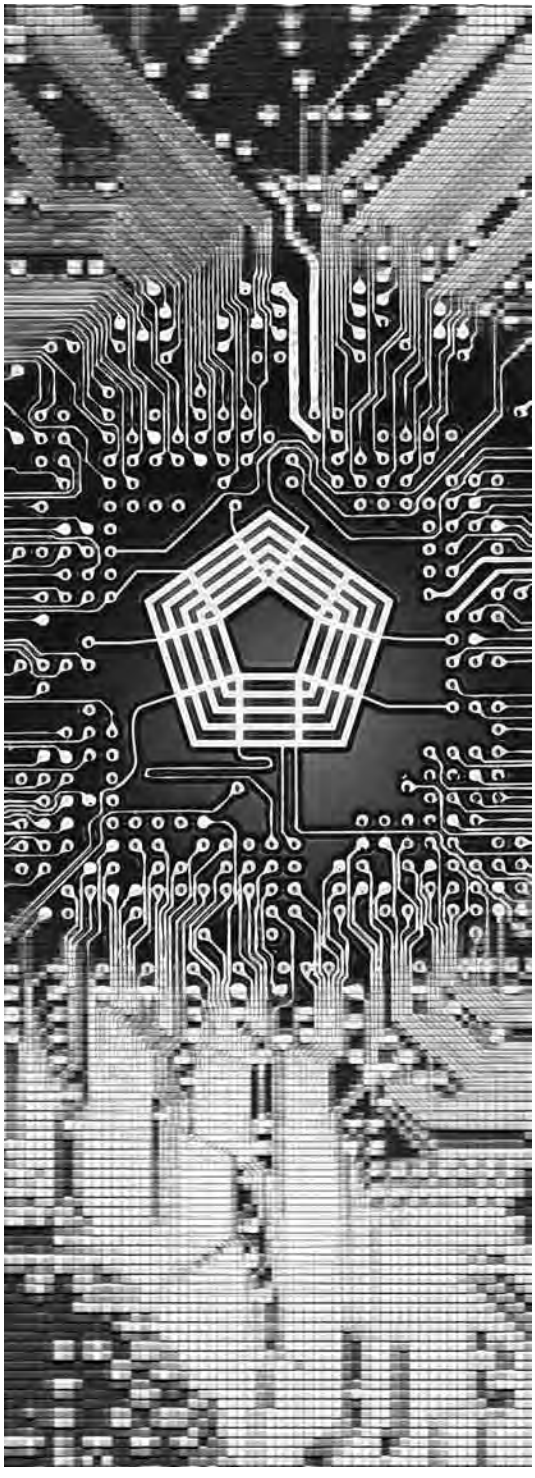

Joint Targeting in Cyberspace

Maj Steven J. Smart, USAF

America relies on our digital infrastructure daily, and protecting this strategic asset is a national security priority.

—President Barack Obama, 2010

Security in cyberspace is a clear national priority, but the role of the US military in this new domain is not so clear. With the activation of US Cyber Command in 2010, debate concerning the militarization of cyberspace and the conduct of cyber "warfare" has taken center stage among US government policy makers.[1] Complicating matters is the uncertain practice of governing behavior in cyberspace by applying domestic legal and policy guidelines as well as international treaties based on kinetic warfare.[2] Despite this uncertainty, Department of Defense (DOD) policy requires that DOD components "comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations."[3] Although it remains to be seen what roles and responsibilities policy makers in Washington, DC, will carve out for the military, the DOD should prepare to conduct military operations in the cyber domain. To do so effectively, the department should apply, with slight modification, time-tested joint targeting principles to military operations in cyberspace.[4] This article explores the efficacy of Joint Publication (JP) 3-60, *Joint Targeting*, as applied to military operations in cyberspace and proposes recommendations for joint targeting doctrine for cyberspace.[5]

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Joint Targeting in Cyberspace	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Headquarters US Air Force,Office of the Judge Advocate General,Pentagon,Washington,DC,20301**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**11**	

Foundational Principles of Joint Targeting

Before we can address the adequacy of applying JP 3-60 to cyber targeting, we must understand the foundations of its principles, the reason for its application, and the relationship between doctrine and law. "Joint doctrine presents fundamental principles that guide the employment of US military forces," and "[commanders] at all levels [must] ensure their forces operate in accordance with the 'law of war,'" which is "binding on the United States."[6] Joint doctrine incorporates what the United States has agreed to follow in international law as well as operational best practices. The "law of war" consists of conventional international law (treaties and agreements between nation-states) and customary international law (based on state practice).[7] The latter develops from state practice—namely, official governmental conduct reflected in a variety of acts, including published doctrine. Thus, joint doctrine not only reinforces binding legal obligations but also advances the development of customary international law.

For simplicity, the primary canons that set the foundation for the modern law of war are divided between rules for the *conduct* of war and the *treatment* of parties to the conflict and its bystanders: the Hague and the Geneva conventions, respectively.[8] Additionally, the Charter of the United Nations outlines obligations of the organization's member states with regard to the "use of force" against other states.[9] Domestic law (federal statutes and judicial decisions), US government policy, joint and service doctrine, as well as rules of engagement (ROE) specify how US military forces will comply with these international obligations. We must understand that neither military doctrine nor ROEs, whether standing or mission specific, replace or supersede the laws of war. Rather, they represent US implementation of agreed-upon international principles to a specific situation.

We can distill this vast body of rules, regulations, and doctrine to five simple principles that apply to any specific operation. First, the use of force presupposes the existence of *military necessity* (a valid military reason to use force necessary to carry out the mission).[10] Second, the proposed employment of force must not cause the civilian population or the targeted enemy force *unnecessary suffering*.[11] Commanders must apply this principle—the basis for later conventions that outlaw certain types of weapons and munitions (e.g., chemical weapons)—not only to potential "collateral damage" (incidental loss of civilian life or damage to civilian property) but also to the intended object of attack. Third, the employment of force must *discriminate* or distinguish between combatants and noncombatants as well as forgo intentional attacks against civilian populations not directly participating in hostilities.[12] In short, the operator must use a weapon capable of being aimed and must distinguish between civilians and adversaries—the underlying principle that guides joint targeting analysis, explored in greater detail below. Fourth, the proposed military operation must be *proportional*—that is, it must avoid excessive collateral damage in light of the expected military advantage.[13] Finally, the parties in the armed conflict must maintain *chivalry* or a "certain amount of fairness . . . and a degree of mutual respect and trust."[14] Applying these principles guides the employment of force in general and individual targeting decisions in particular.

In military circles, the term *targeting* often describes an action of a military force engaging, or preparing to engage, an adversary. Officially, joint doctrine defines targeting as "the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities."[15] This definition—specifically, the process of selecting the target and matching the appropriate response to it—most directly entails obligations under the law of war. Target selection is the primary premise upon

which the principle of discrimination rests. *Military* objects are lawful targets, but forces should not attack civilians intentionally and should spare them from collateral effects as much as possible.[16] Therefore, the law of war holds the military commander and operator responsible for identifying, functionally characterizing, and attributing to a combatant—as accurately as practicable—the intended object of a proposed military operation.

Military doctrine sets forth principles to guide forces in carrying out their obligation of discrimination. JP 3-60 includes the overarching targeting principles for conducting combined or joint operations. Military service doctrine, such as Air Force Doctrine Document (AFDD) 2-1.9, *Targeting*, complements joint doctrine with principles specifically designed for the individual service's primary responsibility.[17] These principles derive from best practices, drawing on the collective experience of the US military and its allies during previous military campaigns and operations. Because no military service has primary responsibility for the cyberspace domain and because little, if any, collective best practice for military operations in cyberspace exists, current doctrine for other war-fighting domains shapes cyber operation planning and informs cyber targeting decisions.[18] Therefore, JP 3-60 is *by default* the current foundational publication on joint targeting in cyberspace.

Application to Cyberspace

Applying existing military doctrine (specifically, targeting and law-of-war principles) to operations in cyberspace is easy in theory but may prove extremely difficult in practice. Cyber warfare differs fundamentally from traditional armed conflict. Unlike the conduct of past warfare, opponents (including state actors, criminals, terrorists, and hackers) can wage cyber warfare from far reaches of the globe rapidly, cheaply, anonymously, and devastatingly. Current military doctrine looks to the experiences and theories of *kinetic* warfare between nation-states in battlespaces that exist almost exclusively in a physically recognizable and understandable area (air, land, sea, and space). Cyber warfare, by contrast, occurs in "a realm located simultaneously at logical and physical layers that intersects activities in, through, and concerning the electromagnetic spectrum which seamlessly crosses other domains as well as geographic and recognized political boundaries."[19]

The extent to which cyber warfare differs from kinetic warfare and represents a paradigm shift in modern military affairs is a contentious subject best suited to academic historians. However, differences exist between the actors and the means/methods of armed conflict in the physical world and their counterparts associated with conflicts in cyberspace. These variations illustrate the complex challenges of applying current law, policy, and military doctrine to keystrokes and mouse clicks.

First, participation in cyber warfare is not limited to agents of the nation-state. Unlike conventional military attack, conducting a strike in cyberspace does not require government sponsorship.[20] Second, the attacker does not need expensive, traditional weapon systems—only a computer, an Internet connection, and basic cyber expertise.[21] Third, unlike attributing an attack in the kinetic world, identifying the source of a cyber strike is extremely difficult. For example, finding the aggressor nation responsible for a missile attack is relatively easy because key "fingerprints" such as the missile's size, speed, range, and type of warhead point to a relatively small list of countries that have the technology, will, and expertise to conduct such an attack. A cyber attack, however, can originate from anywhere and with anyone, including state-sponsored "hacktivists," nonstate actors, or "free lancers packing a politically motivated laptop punch."[22]

The key differences between cyber warfare and its kinetic cousin raise pertinent questions. First, is it realistic to expect even state-sponsored cyber operators to

comply with legal principles and military doctrine based on traditional notions of kinetic war in this new domain? Second, do we need a new joint publication specifically dedicated to cyberspace targeting to account for these differences?

Despite disparities in the operational domains, cyber warriors are fundamentally the same as their counterparts on land, at sea, and in the air. Both rely upon their knowledge of the domain, operational environment, and weapon system capabilities. The complexity of war fighting resists any attempt to reduce it to a formulaic checklist for commanders. Astute leaders may discern and apply enduring truths of war, including the framework for its legal use, within the context of a particular operational or strategic environment. With a few modifications, cyber operators can apply legal principles and military doctrine based on traditional kinetic warfare to cyber operations and still produce the intended effects. Similarly, with only slight adjustments for cyber nuances, JP 3-60 can continue to serve as the US military's foundational publication for both kinetic and nonkinetic targeting.

Military Doctrine in Cyberspace

In the recent past, only one joint publication concerned itself exclusively with conducting military operations in the cyber domain.[23] JP 3-13, *Information Operations*, identified information operations (IO) as "the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own."[24] Doctrinally, CNO, including computer network attack (CNA) and defense (CND), represented just a subset of a larger category of arguably dissimilar activities. Doctrine asserted the centrality of these capabilities to IO as a whole, noting that they would help the joint force commander influence an adversary. But grouping them together suggested that IO itself is a war-fighting specialty capable of rapid integration into a joint task force. Unfortunately, this is not the way the services train their personnel. Rather, they currently train an individual in one or two competencies, such as EW or PSYOP. Within CNO, only rarely does a person have both CNA and CND proficiency. Therefore, an IO cell at the joint task force level may be composed of "cylinders of excellence" (i.e., individuals well versed in their narrow field of training but possessing little understanding of the other capabilities). This is particularly true with regard to the concept of targeting: JP 3-13 does not contain guidance on the topic.

Assuming the "core" nature of these capabilities, why does JP 3-13 include no instruction on targeting? Three reasons come to mind. First, targeting is so essential to war fighting that nearly every military member has a general understanding of the concept. However, targeting that successfully attains both military and political objectives is an extremely complex process that relatively few individuals have mastered. Simply put, most military professionals know what targeting means, but few of them know how to do it. Second, JP 3-13 does not address the specifics of core capabilities. Rather, it refers the IO planner to other publications for guidance, suggesting that these capabilities are not as closely linked as JP 3-13 asserts. Instead, in the minds of conventional military planners, they are merely several unique, unconventional military activities difficult to integrate into an operations plan. Finally, many planners believe that "targeting is targeting," no matter the platform or domain.

Most cyber operational planners would declare that they understand the general concept of targeting as contemplated in the official doctrinal definition and as outlined in JP 3-60. However, their application of the concept and definition to their core IO ca-

pability may mean something very different. For example, a proposed PSYOP activity might "target" a foreign audience whose behavior and actions targeteers want to influence, but an EW operation might target signals from a radio tower. JP 3-13 suggests that the five types of IO functions listed above are operationally interrelated yet offers no guidance on how to target the adversary using these functions specifically.[25] The IO planner or operator must then refer to another subject-matter-specific publication for guidance.[26] The fact that JP 3-13 represents the only joint guidance on network operations complicates matters for the CNO planner.[27] Thus, CNO planners at the joint level must often look backward to service doctrine for such guidance.

The Air Force recently released AFDD 3-12, *Cyberspace Operations*, which differentiates between cyber and information operations.[28] This document represents the service's best effort to understand, organize, train, and guide Airmen in cyberspace operations. Basic enough for the cyber novice yet comprehensive enough for the expert, AFDD 3-12 provides technically sound and operationally relevant guidance to Airmen in the absence of guidance at the joint level—a particularly remarkable feat. Even more impressive, the document relates principles of joint operations to cyberspace operations, offering input across the range of military operations and outlining fundamental principles for the Air Force cyber warrior.[29] Arguably, AFDD 3-12 is the most comprehensive document on cyber operations in the DOD; indeed, the joint force would be well served by a joint publication having its breadth and depth. Admittedly, even though AFDD 3-12 discusses many issues useful in cyber targeting, such as technical relationships in cyberspace infrastructure, information assurance, compressed decision cycles, and the anonymity and attribution challenge, it does not specifically address cyber targeting per se.[30] In fact, the document refers readers to JP 3-60, suggesting that the joint publication's principles, guidance, and theory properly apply to Air Force operations in cyberspace.

On the one hand, the subject of targeting seldom appears in current DOD, joint, or service doctrine on cyberspace, perhaps because the military has only now begun formally organizing its cyber forces or because the services do not have a large, collective cyber-targeting experience from which to draw.[31] On the other hand, DOD leaders may simply believe that JP 3-60's principles of targeting are so sound that they translate easily to military operations in the cyber domain. Whatever the rationale, JP 3-60 remains the seminal joint publication on targeting in cyberspace despite the fact that it makes no reference to the domain itself.

Review of Joint Publication 3-60

Organized in three main sections—fundamentals of targeting, the joint targeting process, and duties and responsibilities—JP 3-60 proceeds logically from defining the term *target*; through target development, target engagement, and damage assessment; to command responsibilities and oversight. A targeting novice can quickly grasp the fundamentals of this concise, well-written document. For example, one simple chart (fig. II-1, the Joint Targeting Cycle) conveys the essence of combat targeting.[32] To understand the cycle is to understand targeting.

The joint targeting cycle quickly outlines the who, what, where, when, why, and how of adversary engagement.[33] After the joint force commander announces an *end state and objective*, planners *develop and prioritize targets* toward that end. Target selection drives *weapon/capability pairing*, which ensures successful engagement while minimizing collateral damage. The particular weapon selected determines *force assignment*, which informs *mission planning* and drives *execution*, after which an *assessment* tells the commander whether the mission has fulfilled the objectives or whether additional targeting is

necessary, as determined through evaluation of predetermined measures of effectiveness and measures of performance. Skipping steps in the cycle jeopardizes mission effectiveness; adding steps outside the cycle is superfluous. From a legal perspective, adherence to the joint targeting cycle process and to other fundamental principles in the publication, coupled with sound command judgment, virtually assures compliance with the laws of war.

Thus, JP 3-60 appears to be a "plug and play" guidebook for targeting in any domain. Unfortunately, analysis which assumes that the cyber domain shares essentially the same characteristics with air, land, sea, and space fails to account for its uniqueness.

Like the other domains, cyberspace occupies an area, is subject to exploitation by governments and entrepreneurs, and serves as a medium for the exchange of commerce among corporations, nations, and individuals. Yet this unique medium "has to be appreciated on its own merits; it is a man-made construct."[34] Computers enable actions in near real time and may provide near anonymity for the user. The fact that criminals, terrorists, and state actors use the same cyber infrastructure employed by commercial enterprises and individuals to conduct their operations adds a "social context" to military operations in this domain.[35] In the air, space, and sea domains, relatively few adversaries are competent enough to effectively threaten or challenge the United States and its military. By contrast, the cyber domain is crowded with actors capable of pressuring, confronting, or intimidating the United States, its allies, and each other. This congested battlespace complicates using JP 3-60 as a guide to cyber targeting in five key areas: (1) positive identification of targets, (2) location of targets, (3) attribution of attack, (4) capability/target pairing, and (5) assessment of potential collateral damage.

First, positive identification of a potential cyber target is complicated by the intricacy of the dual-use global cyberspace infrastructure. The two sections of JP 3-60 that address target identification—chapter 2, "The Joint Targeting Process," and appendix E, "Legal Considerations in Targeting"—make clear that a valid and lawful military target requires a degree of distinctive identification and characterization conducted during either a normal or time-sensitive targeting cycle. Neither section addresses the fleeting nature or uniqueness of cyber targets or notes that the latter exist almost exclusively in a dual-use medium.

To illustrate, suppose that planners nominate three targets to a joint targeting coordination board, a group that "facilitates and coordinates joint force targeting activities . . . to ensure that the [joint force commander's] priorities are met."[36] The first nominated target is a tank, the second a website, and the third an online "persona." Initially, the board might validate the tank as a military target but hold that neither the website nor the persona qualifies as a valid military target as contemplated by JP 3-60 or the laws of war because it is not a physical object but a formulaic composition of ones and zeros—an incorrect assessment. In fact, JP 3-60 does not limit a target to the physical world, instead defining it as "an *entity* or object considered for possible engagement or action. It may be an area, complex, installation, force, equipment, capability, function, individual, group, system, *entity*, or *behavior* identified for possible action" (emphasis added).[37] This broad definition encompasses both the website and persona.

The lawfulness of engaging an adversary's tank is clear because of that weapon's exclusive purpose of destroying and killing within the confines of armed conflict, but a law-of-war analysis of the website and persona must go one step further. Both the website and persona would have to meet a "use" rather than a "purpose" test—that is, at the time of the proposed attack, is the adversary using them to further his war-fighting or war-sustaining capabilities? If so, then they may be the lawful objects of military attack. The exact timing of when these dual-use objects, entities, or behaviors in and through cyberspace actually contribute to the adversary's cause makes engagement

difficult. Unlike the validation of targets during kinetic warfare, the process with cyber targets demands both consistent updating of the validating intelligence and positive identification in near real time.

Second, the location of a cyber target presents unique challenges. JP 3-60 and the laws of war address target location in the context of physical encroachment on a sovereign nation. Neither the doctrine nor the law contemplates one target existing in several different places around the globe at the same time or causing effects in multiple theaters of conflict, as can happen in cyberspace. For instance, an adversary can conduct command and control through websites hosted simultaneously on servers in different countries and can thwart attack by moving those websites frequently. Problematically, the particular ROEs applicable to the military planner and operator may preclude actions in certain places outside the joint operations area even though the adversary uses an ever-changing global network to deliver effects there. This dilemma leads to a significant and an important debate. What is the target? Is it the adversary physically located in the joint operations area, or is it his globally distributed command and control network? If location precludes engagement, then the military planner naturally reassesses the exact target. Is it the fielded forces or their networks?

Third, attribution of cyber capabilities, equipment, and usage to a particular, declared hostile entity is demanding in cyberspace. Even though attribution may fall under positive identification, this article treats it as a separate issue to illuminate differences between offensive and defensive cyber targeting.[38] The anonymity afforded by cyberspace allows an enemy to mask his actions and falsely attribute them to a noncombatant or any other entity. An adversary could hijack the computers of innocent civilians, groups, or governments and use them as a "bot net" to launch a cyber attack. Once the victim of the attack conducts rudimentary forensics, attribution of the attack would point to the innocent noncombatants rather than the true perpetrator. Strictly speaking (depending upon the amount of damage), the law of war could view such an attack as the war crime of perfidy. Practically speaking, if the attack were continual (e.g., a distributed denial of service), must the victim obtain positive identification of each target, in essence attributing it to a declared hostile entity, prior to launching defensive measures at the "attacking" computers? Fortunately, as mentioned above, the law of war recognizes the inherent right of self-defense (focusing on location of the threat) and does not require positive identification of the attacker. But in cyberspace, even a purely defensive response to an attacking computer could have severe cascading, unintended consequences for the global cyber infrastructure—not to mention the political nightmare of counterattacking against the wrong party.

Fourth, the pairing of capability and target in cyberspace entails unique issues. Offensive action may call for precision capabilities to avoid significant collateral damage. A defensive posture (or crisis response) may necessitate the use of powerful counterattack and deterrent capabilities against a broad range of attackers—creating more of a broad firewall rather than a pinpoint strike.

Fifth, the arduous process of assessing potential collateral damage in cyberspace demands significant intelligence, and the interconnectivity of networks and the redundancies in systems require meticulous planning. At present we have no formal methodology of collateral damage estimation for cyber targeting.[39] Applying kinetic formulas would be problematic because cyberspace exits at both physical and logical levels.

Despite these unique challenges to targeting in cyberspace, JP 3-60 provides a sufficient doctrinal framework for the military cyber operations planner.[40] There is, however, room for improvement and clarification with regard to cyber operations, particularly in the areas of collateral damage estimation and battle damage assessment.[41]

Recommendations

Improvements to existing cyber-targeting doctrine should start with a declaration in the next edition of JP 3-60 that the fundamentals described in the publication apply to targeting in the newly recognized cyber domain. Such a statement would have the twofold purpose of recognizing the importance and uniqueness of military operations in cyberspace and affirming the universality of the publication's combat-targeting principles.

As mentioned above, JP 3-60 should provide an overview of how to conduct collateral damage estimation and battle damage assessment in cyberspace, perhaps including tactics, techniques, and procedures for identifying other hostile and civilian websites located on a server or tracing potential second- and third-order effects and their likely geographic location. In reality, because most offensive cyber operations would not cause physical damage, JP 3-60 should describe methodology for determining collateral *effects* in cyberspace by distinguishing between effects and damage in cyberspace. This distinction should use "kinetic damage" (physical destruction or degradation caused by a cyber operation) as the determining criterion. Any cyber operation that does not cause physical destruction would yield only "effects." Planners would collect battle damage assessment only for actions that cause physical damage to intended targets and nontargeted systems and would measure collateral effects much as they do for other cyber operations.

An updated JP 3-60 should contain a brief section about the complexity of the cyber domain, utilizing the "Understanding Cyberspace" and "Operational Environment" sections of AFDD 3-12 as an excellent template.[42] Such a discussion would allow the joint planner to recognize the unique, additional considerations of deliberate and time-sensitive targeting in and through cyberspace.

Furthermore, the next version of JP 3-60 should pay careful attention to the differences between offensive and defensive cyber targeting—specifically, the level of attribution necessary for positive identification of a cyber target. For offensive cyber operations (e.g., CNA), attribution of a computer network, website, persona, or infrastructure should approach complete certainty (a true representation of positive identification) so as to comply with the law of war's principle of discrimination. Application of the principle of self-defense to cyberspace allows greater flexibility for the joint planner, having the goal of repelling an attack or imminent strike against friendly computer systems. The recommended course of action for cyber defense would involve implementing a sliding scale of adversary attribution whereby the confidence level is commensurate with the level of anticipated damage or effects produced by the response. At one end of the scale, a response whose scope, duration, and intensity will likely cause significant kinetic damage would demand almost complete certainty of attribution. At the other end, a purely technical—perhaps even automated—administrative self-defense action not really amounting to a use of force would require no attribution. Such cyber "countermeasures" include detecting, quarantining, and removing a virus or simply blocking malicious traffic and disrupting network connections between the attacking and targeted computers.

Finally, an updated JP 3-60 should introduce the concepts of an *adversary's cyber center of gravity* and a *cyberspace joint operations area*. An adversary's cyber presence consists of computers, information systems, hardware, online personas, and so forth, which may be geographically separated from his physical center of gravity. Once planners identify the cyber center of gravity (a critical point—a source of power for the adversary's cyber operations), they can target it. The joint task force commander would establish both the physical and logical boundaries of a cyber joint operations area and specify targeting ROEs for that area. Partitioning cyberspace in this manner

minimizes the potential for cascading collateral damage and effects.

In conclusion, JP 3-60 offers the joint cyber war fighter adequate targeting guidance applicable to the cyber domain. With slight modification and incorporation of domain-specific guidance, however, that publication will become even more useful to cyber warriors. ✪

Notes

1. Wesley R. Andrues, "What U.S. Cyber Command Must Do," *Joint Force Quarterly* 59 (4th Quarter 2010): 117, http://www.ndu.edu/press/lib/images/jfq-59/JFQ59_115-120_Andrues.pdf.

2. Tom Gjelten, "Extending the Law of War to Cyberspace," National Public Radio Online, 22 September 2010, accessed 4 October 2010, http://www.npr.org/templates/story/story.php?storyId=130023318. For the purposes of this article, *kinetic* means physical actions traditionally associated with military combat.

3. DOD Directive (DODD) 2311.01E, *DOD Law of War Program*, 9 May 2006 (incorporating change 1, 15 November 2010), 2, http://www.dtic.mil/whs/directives/corres/pdf/231101e.pdf.

4. This article uses the term *principles* (1) within the context of targeting to describe the primary beliefs, accepted best practices, and military philosophy for producing desired operational effects, and (2) within the legal context to describe core tenets of law. Synthesized in joint publications, these meanings are broken out here to highlight certain differences between traditional kinetic military action and potential cyber operations.

5. Joint Publication (JP) 3-60, *Joint Targeting*, 13 April 2007, https://jdeis.js.mil/jdeis/new_pubs/jp3_60.pdf.

6. JP 1, *Doctrine for the Armed Forces of the United States*, 2 May 2007 (incorporating change 1, 20 March 2009), I-1, I-21, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

7. The law of war is "a branch of public international law, and comprised of a body of rules and principles observed by civilized nations for the regulation of matters inherent to, or incidental to, the conduct of a public war." *Black's Law Dictionary*, 6th ed. (St. Paul, MN: West Publishing, 1990), 1583.

8. International Conferences (The Hague), *Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land*, 18 October 1907, http://www.icrc.org/ihl.nsf/full/195. Hereafter Hague IV. See also *Hague Convention (III) Relative to the Opening of Hostilities*, 18 October 1907, http://www.icrc.org/ihl.nsf/FULL/190?OpenDocument; *Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land*, 18 October 1907, http://www.icrc.org/ihl.nsf/FULL/200; and Geneva Conventions I–IV, 12 August 1949, International Committee of the Red Cross, http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/index.jsp.

9. Charter of the United Nations, Article 2(4), 26 June 1945, http://www.un.org/en/documents/charter/chapter1.shtml.

10. Hague IV, Article 23(g).

11. Hague IV, Article 23(e).

12. United Nations General Assembly Resolution 2444 (XXIII), 19 December 1968, as cited in International Committee of the Red Cross, *Weapons That May Cause Unnecessary Suffering or Have Indiscriminate Effects: Report on the Work of Experts* (Geneva, Switzerland: International Committee of the Red Cross, 1973), 13, http://www.loc.gov/rr/frd/Military_Law/pdf/RC-Weapons.pdf.

13. See Geneva IV, Articles 4 and 27.

14. Judge Advocate General's School, *Air Force Operations and the Law: A Guide for Air, Space, and Cyber Forces*, 2nd ed. (Maxwell AFB, AL: Judge Advocate General's School, 2009), 21, http://www.afjag.af.mil/shared/media/document/AFD-100510-059.pdf. See the introduction to Hague IV: "The inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience."

15. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 May 2011), 362, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

16. See MAJ Keith E. Puls, ed., *Law of War Handbook* (Charlottesville, VA: International and Operational Law Department, Judge Advocate General's Legal Center and School, US Army, 2005), 139–42, http://www.loc.gov/rr/frd/Military_Law/pdf/law-war-handbook-2005.pdf.

17. Air Force Doctrine Document (AFDD) 2-1.9, *Targeting*, 8 June 2006, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-60.pdf.

18. Cyberspace is a global domain. See JP 1, *Doctrine for the Armed Forces of the United States*, GL-7; and Cheryl Pellerin, "Cyberspace Is the New Domain of Warfare," *U.S. Air Force AIM Points*, 18 October 2010, accessed 20 October 2010, http://aimpoints.hq.af.mil/display.cfm?id=41748&printer=no.

19. Maj Steve Smart, "Warfare in the Cyberspace Domain" (thesis, Air Command and Staff College, Maxwell AFB, AL, 2010), 3. This is the author's proposed new definition of "cyberspace domain." The characterization of cyberspace as an operational domain is sensitive and controversial. See the unclassified "White House Guidance Regarding the Use of 'Domain' in Unclassified Documents and Public Statements," 14 March 2011. (FOUO)

20. Christina Mackenzie, "Do No Harm," *Aviation Week: Defense Technology International—Cyber War Issue*, September 2010, 37.

21. Ibid.

22. Michael Dumiak, "Casus Belli," *Aviation Week: Defense Technology International—Cyber War Issue*, September 2010, 31.

23. The undersecretary of defense for policy and the chairman of the Joint Chiefs of Staff will revise IO policy and doctrine documents to reflect directed integration of IO into military operations and away from a focus on its core capabilities. This shift marks a significant step toward "mainstreaming" cyber operations. See Robert Gates, secretary of defense, memorandum, subject: Strategic Communication and Information Operations in the DOD, 25 January 2011, http://www.carlisle.army.mil/dime/documents/Strategic%20Communication%20&%20IO%20Memo%2025%20Jan2011.pdf.

24. JP 3-13, *Information Operations*, 13 February 2006, I-1, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf. The new definition of IO is "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." See Gates, memorandum, 2.

25. JP 3-13, *Information Operations*, II-1.

26. See JP 3-13.1, *Electronic Warfare*, 25 January 2007, https://jdeis.js.mil/jdeis/new_pubs/jp3_13_1.pdf; and JP 3-13.2, *Psychological Operations*, 7 January 2010, https://jdeis.js.mil/jdeis/new_pubs/jp3_13_2.pdf.

27. This is not to suggest that the DOD offers no cyber guidance but to make the point that little warfighter guidance exists. See DODD 3600.01, *Information Operations (IO)*, 14 August 2006, http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf; and DODD O-8530.1, *Computer Network Defense (CND)*, 8 January 2001.

28. AFDD 3-12, *Cyberspace Operations*, 15 July 2010, 2, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf.

29. Ibid., 16–20, 22–28.

30. See AFDD 3-12, *Cyberspace Operations*.

31. US Cyber Command is working various roles and missions in the cyber domain and is building a "unified vision." Mark V. Schanz, "Cyber Command Working Out Roles and Relationships," Daily Report, *airforce-magazine.com*, 21 October 2010, http://www.airforce-magazine.com/DRArchive/Pages/default.aspx. The 460th Space Wing at Buckley AFB, CO, completed its first exercise focused exclusively on cyber issues. MSgt J. LaVoie, "A First-of-Its-Kind Cyber Exercise," Daily Report, *airforce-magazine.com*, 29 October 2010, http://www.airforce-magazine.com/DRArchive/Pages/default.aspx.

32. JP 3-60, *Joint Targeting*, II-3.

33. Ibid.

34. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 11, http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.

35. See Timothy L. Thomas, *Cyber Silhouettes* (Fort Leavenworth, KS: Foreign Military Studies Office, 2005), 19.

36. JP 3-60, *Joint Targeting*, III-2.

37. Ibid., I-2.

38. A policy debate is in progress among cyber professionals and government leaders about the necessity of positive identification for all cyber operations and its feasibility during crisis responses.

39. See United States Joint Forces Command, *Joint Fires and Targeting Handbook* (Suffolk, VA: Joint Warfighting Center, Joint Doctrine; Norfolk, VA: Joint Capability Development, Joint Integrated Fires, 19 October 2007), http://www.dtic.mil/doctrine/doctrine/jwfc/jntfiretar_hdbk.pdf.

40. Maj Kevin Beeker (acting J2T, US Cyber Command) and MSgt Dustin Dargis (US Cyber Command), interviews with the author, 2–4 November 2010.

41. Ibid.

42. AFDD 3-12, *Cyberspace Operations*, 2–5.

Maj Steven J. Smart, USAF

Major Smart (AA, Wentworth Military Academy Junior College; BS, John Brown University; MA, Air University; JD, Gonzaga University School of Law) is the chief of strategic communications, Office of the Judge Advocate General, Headquarters US Air Force, Pentagon. Major Smart previously served as the chief of targeting and operational law at US Cyber Command and its predecessor organizations, Joint Functional Component Command–Network Warfare / Joint Task Force Global Network Operations, where he advised the commander and Joint Interagency Task Force on the law of war, rules of engagement, and international law during the planning of military operations in cyberspace. He was the primary legal adviser for targeting and cyber attack teams, crisis and contingency planning cells, and cyber response planners. During his career, Major Smart has served as a military prosecutor and defense counsel as well as a procurement and environmental law attorney. He also served in a leadership role as deputy staff judge advocate. Major Smart is a 2011 graduate of Air Command and Staff College, where he won the Lt Gen Michael Hayden Research Award for contribution to the advancement of information operations, including influence, electronic warfare, and network warfare operations.