Perspectives for Cyber Strategists on Law for Cyberwar

Charles J. Dunlap Jr., Major General, USAF, Retired

The proliferation of martial rhetoric in connection with the release of thousands of pages of sensitive government documents by the WikiLeaks organization underlines how easily words that have legal meanings can be indiscriminately applied to cyber events in ways that can confuse decision makers and strategists alike.[1] The WikiLeaks phenomenon is but the latest in a series of recent cyber-related incidents—ranging from cyber crises in Estonia and Georgia[2] to reports of the Stuxnet cyberworm allegedly infecting Iranian computers[3]—that have contributed to a growing perception that "cyberwar" is inevitable, if not already underway.[4]

All of this generates a range of legal questions, with popular wisdom being that the law is inadequate or lacking entirely. Lt Gen Keith B. Alexander, the first commander of US Cyber Command, told Congress at his April 2010 confirmation hearings that there was a "mismatch between our technical capabilities to conduct operations and the governing laws and policies."[5] Likewise, Jeffrey Addicott, a highly respected cyber-law authority, asserts that "international laws associated with the use of force are woefully inadequate in terms of addressing the threat of cyberwarfare."[6]

This article takes a somewhat different tact concerning the ability of the law of armed conflict (LOAC) to address cyber issues.[7] Specifically, it argues that while there is certainly room for improvement in some areas, the basic tenets of LOAC are sufficient to address the most important issues of cyberwar. Among other things, this article contends that very often the real difficulty with respect to the law and cyberwar is not any lack of "law," per se, but rather in the complexities that arise in determining the necessary facts which must be applied to the law to render legal judgments.

Prof. Charles J. Dunlap Jr. is associate director of the Center on Law, Ethics, and National Security at Duke Law School and a visiting professor of the practice there. Before retiring as a major general in June 2010 after 34 years of active duty, he served as deputy judge advocate general of the Air Force. He also serves on the board of advisors for the Center for a New American Security.

That is not to say that applying the facts—such as they may be discernable in cyber situations—to a given legal principle is anything but a difficult task. Yet doing so has a direct analogy to the central conundrum faced by military decision makers fighting in more traditional battlespaces—that is, the need to make quick decisions based on imperfect data. Because of the inherent fog of war,[8] commanders gamely accept a degree of uncertainty in the legal advice they receive, just as they tolerate ambiguity inherent in other inputs. Too often it seems as if cyber strategists, schooled in the explicit verities of science, expect a level of assurance in legal matters rivaling mathematical equations. All law, but especially LOAC, necessarily involves subjectivity implicit in human reasoning that may be troubling to those of a technical mind-set accustomed to the precision that their academic discipline so often grants.

This article will not provide cyber strategists with "cookbook" solutions to all the permutations of every legal dilemma cyberwar could produce. Instead it offers some broad legal considerations to facilitate thinking about the role of LOAC in cyberwar and suggests cautions for the military cyber strategist in the future.

Perspectives on the law are expressed here as definitively as possible to counter complaints about indecisiveness of legal analysis. The author chose among differing and even conflicting legal interpretations and theories, and readers should understand that positions in this writing may be disputed by other legal experts. Accordingly, cyber strategists must always seek the advice of legal counsel for guidance in specific situations, especially as law and policy evolve.

Cybersizing LOAC

Discomfort among cyber strategists relying on existing LOAC norms is understandable. After all, most of the international agreements and practices of nation-states that comprise LOAC predate the cyber era. Indeed, many observers believe the need for a new legal regime designed for cyberwar is urgent.[9] Cyber expert Bruce Schneier warns that time is running out to put in place a cyber treaty that could, he advocates, "stipulate a no first use policy, outlaw unaimed weapons, or mandate weapons that self-destruct at the end of hostilities."[10]

However, to paraphrase former Secretary of Defense Donald Rumsfeld, you go to war with the LOAC you have, not the LOAC you may want.

While agreements that might expedite cyber-law enforcement efforts are possible, it is not likely that any new international treaty governing cyberwar or cyber weaponry will be forthcoming in the foreseeable future. To begin with, the utility of such treaties is checkered at best. Although most people cheer international treaties that have banned chemical and biological weapons, some experts see them as unintentionally inhibiting the development of nonlethal and low-lethality weaponry.[11] More generally, pundit Charles Krauthammer gives this scorching analysis: "From the naval treaties of the 1920s to his day, arms control has oscillated between mere symbolism at its best to major harm at its worst, with general uselessness being the norm. The reason is obvious. The problem is never the weapon; it is the nature of the regime controlling the weapon."[12]

The Obama administration also seems guarded with respect to cyber arms agreements. Writing in a recent issue of *Foreign Affairs*, Deputy Secretary of Defense William Lynn observed that "traditional arms control agreements would likely fail to deter cyberattacks because of the challenges of attribution which make the verification of compliance almost impossible."[13]

Even more substantively, nations may perceive the goals of any cyber treaty differently. For example, the Russians have long proposed an international cyber agreement (although couched in terms aimed at "information warfare").[14] However, journalist Tom Gjelten warns that "democracies have reason to proceed cautiously in this area, precisely because of differences in the way cyber 'attacks' are being defined in international forums." The Russians and others see "ideological aggression" as a key cyberwar evil and appear to be seeking an agreement that assists government censorship of the Internet and bans outside countries from supporting the cyber efforts of dissidents.[15]

Gjelten notes that at a 2009 meeting to discuss the Russian proposals, the "U.S. delegation declared that existing international law could theoretically be applied to cyber conflict and that the United States would support the establishment of 'norms of behavior' that like-minded states could agree to follow in cyberspace."[16] American cyber strategists, however, should remain cautious of even that modest initiative. As attractive as it may be to have more clarity as to what the international community considers, for example, as an "act of war" in cyberspace, once an international norm is established, it forever after can be a legal impediment. If, as Gjelten argues, the United States has the most advanced cyberwar capability,

any new agreement or norm would likely oblige it to "accept deep constraints on its use of cyber weapons and techniques."[17]

The "Act of War" Conundrum

As already suggested, of all the legal issues bedeviling cyber strategists, the issue of when a cyber event amounts to an act of war seems to capture the most interest.[18] This is not a new query but one that is critical because its resolution can define the options available to decision makers. If it is truly "war," then a response under a national-security legal regime is possible; if not, then treating the matter as a law enforcement issue is appropriate. This is a distinction with a difference.[19]

A national-security legal regime is one where LOAC largely governs, while the law enforcement model essentially employs the jurisprudence of criminal law. The former is inclined to think in terms of eliminating threats through the use of force; the latter uses force only to contain alleged lawbreakers until a judicial forum can determine personal culpability. An action legitimately in the realm of national security law may be intolerant of any injury and, when hostile intent is perceived, may authorize a strike to prevent it from occurring. Law enforcement constructs presume the innocence of suspects and endure the losses that forbearance in the name of legal process occasionally imposes.

All things being equal, cyber strategists should default to the law enforcement modality. This makes practical sense, because many experts see cyber crime (as opposed to cyberwar) as the most serious and most common threat in the cyber domain.[20] "Crime," incidentally, could include acts at the behest of a nation-state, such as cyber espionage targeting a government or industry. As a general proposition, nondestructive computer methodologies employed for espionage may violate the domestic law of the victim nation-state but are not contrary to international law.[21]

In any event, "act of war" is a political phrase, not a legal term.[22] It might be said that the United Nations Charter was designed, in essence, to ban "war" from the lexicon of nations.[23] Article 2 (4) of the Charter demands that nations "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[24] It sanctions only two exceptions to this prohibition on the use of force: (1) when the Security Council authorizes force, and (2) when a nation acts in self-defense. As to self-defense, Article 51 says

that nothing in the Charter shall "impair the inherent right of individual or collective self-defense if an armed attack occurs" against a UN member.[25] It is this self-defense provision that often confounds cyber strategists and their lawyers. Why?

The logic can be confusing. Specifically, Article 2 prohibits all threats and uses of "force," while Article 51 allows the use of force *only* in response to a certain kind of attacking force, specifically, an "armed attack." Retired Air Force colonel turned law professor Michael N. Schmitt notes that "all armed attacks are uses of force [within the meaning of Article 2], but not all uses of force qualify as armed attacks" that are a prerequisite to an *armed* response.[26] Thus, a nation may be the victim of cyber "force" of some sort being applied against it but cannot respond in kind because the force it suffered did not amount to an armed attack. However, a victim state may engage in a number of activities short of the use of force, including the unilateral severance of economic and diplomatic relations, civil lawsuits, and application to the UN Security Council for further action. In appropriate cases, pursuing criminal prosecution is an option.[27]

Of course, a cyber technique *can* qualify as an armed attack. Cyber methodologies may qualify as "arms" under certain circumstances,[28] and existing LOAC provisions provide ready analogies for construing their use as an "attack." Specifically, although cyber techniques may not involve kinetics, as a matter of law an attack may take place even without a weapon that uses them. *Protocol I* to the Geneva conventions defines *attacks* to mean "acts of violence against an adversary,"[29] which is properly interpreted to "extend to violent consequences of an attack which does not consist of the use of kinetic force."[30] The leading view, therefore, among legal experts focuses on the consequences and calls for an *effects-based* analysis of a particular cyber incident to determine whether or not it equates to an "armed attack" as understood by Article 51.[31]

Schmitt pioneered this approach and offers seven factors to consider in making the judgment as to whether a particular cyber event constitutes "force" at all: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[32] It is beyond the scope of this article to detail the nuances of each of those factors,[33] but it is important to understand that in determining whether the cyber activity is severe enough to amount to the legal equivalent of an armed attack (as opposed to merely a use of some force), the consequences must extend to more than mere inconvenience; there must be at least temporary damage of

some kind.[34] Schmitt points out that the "essence of an 'armed' operation is the causation, or risk thereof, of death or injury to persons or damage to or destruction of property and other tangible objects."[35]

Cyber events that have violent effects are, therefore, typically the legal equivalent to armed attacks. To be clear, not all adverse cyber events qualify; accordingly, before responding in any way that constitutes a use of force—to include even actions that do not amount to an armed attack—the evidence must show that the effects of the triggering event amount to the equivalent of an armed attack. If they do not reach that level, the response must be limited to acts like those mentioned above which do not amount to a use of force. Dispassionately assessing the consequences of a cyber incident to determine their similarity to an armed attack can be difficult, as initial impressions of the effects can be wildly inflated.

Further convoluting the analysis is the fact that not all damaging cyber events that seemingly equate to an armed attack may be sufficiently egregious to authorize the use of any kinetic or cyber force in response. Although not involving cyber matters, an opinion of the UN–sanctioned International Court of Justice (ICJ) provides some insight. In *Nicaragua v. U.S.*, the ICJ seemed to indicate that an armed attack within the meaning of Article 51 did not arise in every case of an armed clash. Rather, the ICJ considered the "scale and effects" of the use of force to determine if it met the Article 51 requirement.[36]

As an illustration of inadequate levels of violence, the ICJ cited a "mere frontier incident."[37] Although the court did not elaborate on this example, the context implies that such an incident would involve some low level of violence. While apparently accepting (without using the words) the concept of an effects-based approach, the ICJ nevertheless held that "assistance to rebels in the form of the provision of weapons or logistical or other support" was insufficient provocation for an Article 51 response.[38] Such activities may be uses of force prohibited by Article 2 of the UN Charter but do not equate to armed attacks so as to permit self-defense (Art. 51) actions involving the use of force.

Because not every disturbance sourced in a cyber methodology amounts to an armed attack under international law, the Department of Defense (DoD) definition of "computer network attack" is not necessarily coterminous with what cyber strategists should consider as sufficient to trigger a response involving the use of force. Specifically, the DoD characterizes *attack* as actions "taken through the use of computer networks to disrupt,

deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." Quite obviously, this definition takes no cognizance of "scale and effects" and would, therefore, encompass events that are the legal equivalent—in the cyber world—of the "mere frontier incidents" that the ICJ found did not permit an Article 51 response.

The principle of self-defense is also complicated by the issue of anticipatory or "preemptive" self-defense. This is important to cyber strategists as cyber weaponry can be employed rapidly and, once a cyber strike is underway, can be difficult to counter or contain. Nevertheless, many nations claim that bona fide self-defense actions can only be taken *after* an armed attack, not before.[39] However, the United States and some other countries insist that it permits the use of force before suffering actual injury; that is, taking a self-defense action that anticipates and deflects the blow or otherwise preempts an aggressor's ability to take the proverbial "first shot." So long as the response was proportional to the threat posed, the act is lawful.

Classic anticipatory self-defense theory requires evidence that a specific attack is imminent; that is, about to occur. However, American University law professor Kenneth Andersen argues that since at least 1980,

> [the United States] has taken the position that imminence can be shown by a pattern of activity and threat that show the intentions of actors. This can satisfy imminence whether or not those intentions are about to be acted upon. Even events taking place in the past can suffice if the risk is severe enough, and those events can include meeting, planning, and plotting. It is not necessarily or only about a threatened specific event, but about a group or a threat in some broader way. This is sometimes called "active self defense."[40]

This may be attractive to some cyber strategists who want a legal basis to take defensive actions that amount to a use of force against suspicious threats. However, disaggregating intent from capability could have unintended consequences. For example, it may behoove cyber strategists to avoid embracing a legal interpretation that would categorize the nondestructive insertion of a cyber capability into the computer system of another nation as either a use of force or an armed attack. The better view today would be that such activities—without an accompanying intent for imminent action—would not be uses of force, so long as the cyber capability lies dormant.

In interpreting self-defense under Article 51, cyber strategists should keep in mind that the UN Charter governs relations between nation-states, not individuals. The DoD general counsel opines that when "individuals carry

out malicious [cyber] acts for private purposes, the aggrieved state does not generally have the right to use force in self-defense."[41] To do so ordinarily requires some indicia of effective state control of the cyber actors to impute state responsibility.[42]

Nevertheless, if the aggrieved nation requests action from the state from whose territory the cyber attack was carried out and it becomes evident that the state is "unwilling or unable to prevent a recurrence," actions in self-defense are justified.[43] This is the rationale to which Harold Koh, legal advisor to the State Department, alluded when he spoke about self-defense in the context of "the willingness and ability of those nation-states to suppress the threat the target poses."[44] Of course, the problem of attribution stubbornly permeates every aspect of cyber operations; it is, indeed, the "single greatest challenge to the application of the law of armed conflict to cyber activity."[45] Essentially, however, this is a technical issue, not a legal one. Nonetheless, the identity of the attacker may well determine if a state of war exists.

A State of War?

Even the occurrence of a cyber event that equates to an armed attack warranting a lawful self-defense response does not automatically create a state of war (or armed conflict).[46] The presence—or absence—of a state of armed conflict carries significance, because during armed conflict the actions of belligerents are usually governed by LOAC, not the more-restrictive rules applicable to law enforcement situations. In determining the existence of a state of war, we look to traditional definitions, the clearest of which is offered by scholar Yoram Dinstein, who describes it as:

> [A] hostile interaction between two or more States, either in a technical or in a material sense. War in the technical sense is a formal status produced by a declaration of war. War in the material sense is generated by actual use of armed force, which must be comprehensive on the part of at least one party to the conflict.[47]

For cyber strategists, the words "States," "armed force," and "comprehensive" are key because they help distinguish the actions of criminals or cyber vandals from the persistent and comprehensive cyber attacks equating to armed force that increasingly appear to be only within the capability of nation-states. As a matter of legal interpretation, nation-states do not wage *war* against criminals; rather, they conduct law enforcement operations against them. As Schmitt notes, "Cyber violence of any intensity engaged

in by isolated individuals or by unorganized mobs, even if directed against a government," does not create an armed conflict within the meaning of the Geneva conventions.[48]

That said, certain nonstate adversaries can make themselves subject to much the same LOAC regime as a conventional state (albeit without some of the privileges to which a nation-state combatant is entitled). Jamie Williamson, legal counsel to the International Committee of the Red Cross (ICRC), acknowledges that nonstate actors organized into armed groups can constitute "the armed forces of a nonstate party."[49] In accord is Koh's declaration that "as a matter of international law, the United States is in an armed conflict with al-Qaeda," which he characterizes as an "organized terrorist enemy."[50] And this same reasoning applies to the cyber setting. Schmitt observes that "only significantly destructive [cyber] attacks taking place over some period of time and conducted by a group that is well-organized" is sufficient to constitute an internationally recognized armed conflict.[51]

When a state of armed conflict exists, the "fundamental targeting issues are no different in cyber operations as compared to those applicable to kinetic targeting."[52] Koh summarizes the most important of these issues:

> First, the principle of distinction, which requires that attacks be limited to military objectives and that civilians or civilian objects shall not be the object of the attack; and Second, the principle of proportionality, which prohibits attacks that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, that would be excessive in relation to the concrete and direct military advantage anticipated.[53]

Regarding the targeting of civilians and civilian objects, it is also true that only weaponry (cyber or kinetic) capable of discrimination (i.e., directed against legitimate targets) can be used.[54] However, cyber strategists should know that legitimate targets can include civilian objects—especially those having cyber aspects—that have dual military and civilian uses.[55] So long as the principal of proportionality is observed, these normally can be targeted lawfully if they meet the definition of a military objective.[56]

In this area particularly, cyber strategists need to distinguish prudent targeting from legal mandates. In his confirmation hearings, General Alexander said that it "is difficult for me to conceive of an instance where it would be appropriate to attack a bank or a financial institution, unless perhaps it was being used solely to support enemy military operations."[57] However sensible that may be from a policy perspective, cyber strategists should

understand that no LOAC rule requires a target that otherwise qualifies as a military objective to be used *solely* to support military operations—it can have *dual* uses.

Of course, there is no such thing as a "dual use" civilian, but civilians can be targeted consistent with the principle of distinction under certain limited circumstances. Williamson of the ICRC accepts that international law permits the targeting of civilians for such time as they "directly participate in hostilities." If they are members of an organized armed group of nonstate actors, the period of vulnerability may be extended to parallel that of the uniformed military of nation-states; that is, they would be subject to attack virtually at any time or place during an ongoing conflict. However, he advises that the ICRC "takes a 'functional'—not membership—approach." So defined, the nonstate "armed force" consists "only of individuals whose constant function is to take a direct part in hostilities, or, in other words, individuals who have a continuous combat function."[58]

In determining what amounts to a "continuous combat function" in the cyber context, consider the ICRC illustrations. Its examples of "direct participation" by civilians in hostilities include such cyber activities as "[i]nterfering electronically with military computer networks (computer network attacks) and transmitting tactical targeting intelligence for a specific attack."[59] Accordingly, a civilian can be targeted when performing those acts, and one who continuously engages in such conduct can be said to have a continuous combat function, making that person susceptible to attack for as long as that status persists. To anticipate what other cyber activities one might reasonably determine to constitute direct involvement in hostilities, it may help for cyber strategists to consider what activities of the enemy they would consider so intrinsic to a particular cyber process that they would need to target as a matter of military necessity.

As Koh's remarks suggest, LOAC tolerates "incidental" losses of civilians and civilian objects so long as they are "not excessive in relation to the concrete and direct military advantage anticipated." In determining the incidental losses, cyber strategists are required to consider those that may be reasonably foreseeable to be directly caused by the attack. Assessing second- and third-order "reverberating" effects may be a wise policy consideration,[60] but it does not appear LOAC currently requires such further analysis. Another hurdle for cyber strategists may be the difficulty in predicting the effect of a given cyber methodology. Absent a suitable cyber modeling capability that estimates civilian losses, it is unclear how a decision

maker fulfills the legal requirement to weigh those effects against the military advantage sought.

LOAC does require that targeteers "do everything feasible" to ensure the target is a proper military objective.[61] How sure must a cyber strategist be? International courts have used the "reasonable commander" standard; that is, whether the decision is one that a "reasonably well informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her" would have concluded the target met the legal standards.[62] As to degree of certainty, Schmitt offers a "clear and compelling standard" which is "higher than the preponderance of evidence . . . standard used in certain civil and administrative proceedings and lower than criminal law's 'beyond a reasonable doubt' " criterion.[63]

Parenthetically, this discussion of civilians has other implications for cyber strategists; that is, who may conduct cyberwar? Generally, only bona fide members of the armed forces can wage war with the protection of the "combatant privilege." This means so long as LOAC is otherwise observed, military personnel are legally permitted to engage in killing and destruction in war without fear of prosecution for doing so. Thus, conducting cyber activities which have the lethality and destructiveness of traditional kinetic weaponry should be reserved to uniformed members of the military. As Richard Clark states in *Cyberwar*, "It will have to be . . . military personnel [who] enter the keystrokes to take down enemy systems."[64]

In a *Washington Post* op-ed, LOAC expert (and retired Marine Corps judge advocate) Gary Solis takes a harsh view of civilians operating lethal systems. Calling CIA drone pilots "America's own unlawful combatants," he accuses them of "employing armed force contrary to the laws and customs of war" and "violating the requirement of distinction, a core concept of armed conflict."[65] Although Solis is correct in saying that if captured, CIA civilian employees (and/or CIA contractors) are not entitled to prisoner of war status and that they could be legally tried a under the capturing state's domestic law, is his insinuation of war crimes overstated?

A 1999 DoD publication provides some insight. Specifically, in discussing "retaining the requirement that combatant information operations during international armed conflicts be conducted only by members of the armed forces," the DoD general counsel opined that if cyber operations (amounting to a use of armed force) are "conducted by unauthorized persons, their government may be in violation of the law of war, depending on the circumstances, and the individuals concerned are at least theoretically

subject to criminal prosecution either by the enemy or by an international war crimes tribunal."[66]

Cybering and the Citizenry

The nature of the cyber domain is such that it necessarily involves consideration of the domestic environment and its citizenry. Somewhat paradoxically, given the above discussion about the role of civilians in cyberwar, concerns also arise about the appropriate role of the armed forces in cyber operations, especially in situations short of armed conflict.

The vast majority of cyberspace usage involves the lawful activities of the public. As the U.S. armed forces are generally outwardly focused towards external threats, friction with the citizenry has been largely avoided. Unfortunately, the military intelligence apparatus has occasionally been improperly turned inward "to collect personal information about Americans who posed no real threat to national security."[67] The technical potential to do so today is very great. For example, every day the DoD—via the National Security Agency (NSA)—"intercept[s] and store[s] 1.7 billion e-mails, phone calls and other types of communications."[68] Moreover, it is continually seeking new cyber systems to collect even greater quantities of information more broadly and effectively.[69] Of course, these military intelligence capabilities were designed to address external threats, but they are being exploited to address domestic security.

Regrettably, incidents of impropriety still occur. In the aftermath of 9/11, the NSA was "secretly given authority to spy on Americans as part of the war on terrorism."[70] Specifically, the NSA was allowed to eavesdrop on phone calls, monitor e-mails, and track Internet activity without getting a warrant from the special courts established by the Foreign Intelligence Surveillance Act (FISA). The Justice Department vigorously defended what it described as a "terrorist surveillance program" by insisting that bypassing FISA procedures was legal and incident to the president's authority as commander in chief.[71] The courts found otherwise, and in late December 2010 the government was ordered to pay $2.5 million in attorney fees and damages for the NSA's illegal activity.[72]

Other unsettling incidents include reports of the unexplained military monitoring of Planned Parenthood and other organizations.[73] Media stories also show the military having "burrowed into the mushrooming cyber world of blogs" to post content in an attempt to "influence public opinion

about U.S. operations in Iraq and Afghanistan."[74] More recently, journalist Walter Pincus reports the military wanting to expand its intelligence role in cyberspace to counter what is called "the use of the Internet by extremists."[75] ADM James A. Winfield, commander of US Northern Command, says that although his command's role is to defend its networks, he has a "very ambitious staff, and they would like nothing more than to own all of the cyber response inside North America."[76]

Because it "possesses extraordinary technical expertise and experience, unmatched in the government, in exploring and exploiting computer and telecommunication systems," powerful imperatives are pushing further NSA involvement in domestic cyber activities.[77] In a major new development, a cyber security memorandum of agreement was executed between the DoD and the Department of Homeland Security (DHS) in October 2010.[78] For the first time, the DoD is becoming directly involved in protecting domestic civilian cyber infrastructure. To do so, an NSA "cyber-support element will move into Homeland Security's Cybersecurity and Communications Integration Center." Although DHS personnel are supposed to ensure privacy and the protection of civil liberties, Marc Rotenberg of the Electronic Privacy Information Center says he does not think "DHS can oversee the Defense Department."[79]

With powerful cyber systems like Einstein 3 coming online that call for a major NSA role, thoughtful experts like Jack Goldsmith of the Harvard Law School offer a roadmap for proceeding consonant with civil liberties. Among other things, he would require the NSA to obtain "independent approval . . . from the FISA court or a FISA-type court" prior to employing advanced cyber security measures domestically.[80] Legislation such as the Protecting Cyberspace as a National Asset Act now pending also includes safeguards intended to protect privacy and civil liberties.[81]

Nevertheless, cyber strategists may want to encourage the development of fully civilian domestic surveillance cyber systems and, concomitantly, discourage involvement of the armed forces in any cyber operations that might seem to conflict with the sensibilities and mores of the American people, even if technically legal. The armed forces are the most authoritarian, least democratic, and most powerful institution in American society. The restraint intrinsic to a domestic law enforcement mind-set is not its natural state; its purpose, as the Supreme Court puts it, is to wage war.[82] And as this article and other sources suggest, relatively few cyber incidents, domestic or global, meet that legal standard.[83] If nothing else, the fact

that the armed forces unapologetically restrict the rights and privileges of their own members[84] should militate toward avoiding their use in civilian settings where the public properly expects those rights and privileges to flourish.

Cyber strategists need to be especially conscious of emerging public attitudes. As experts question whether the threat of terrorism[85] and even the threat of cyberwar are overstated,[86] Americans may be becoming uncomfortable with what Fareed Zakaria describes as the "national-security state [that] now touches every aspect of American life, even when seemingly unrelated to terrorism."[87] The recent furor over full-body scans at airports, along with a generalized distrust of government,[88] reflects what could be burgeoning public discontent with intrusive government activity (some of which may already be percolating with respect to military cyber activities).[89] In short, cyber strategists must be extremely sensitive to involving the DoD in domestic cyber activities that might align such animosity with the armed forces, as this could undermine the public support and esteem they need to sustain and prevail on tomorrow's battlespaces.

Concluding Observations

Cyber activities do present a number of legal challenges for cyber strategists, but many problems masquerading as "legal" issues are really undecided policy issues with a number of legal alternatives. Cyber strategists rightly carry a heavy element of complicated and difficult policymaking, because cyber issues are so entwined with the lawful activities of citizens and the legitimate needs of commerce.

Solid legal advice in cyber matters is imperative, and the Pentagon is moving to improve its resources to provide it.[90] As one expert put it, in today's world, law is a "center of gravity" because "our enemies carefully attack our military plans as illegal and immoral and our execution of those plans as contrary to the law of war."[91] Closer to home, cyber strategists may wish to consider the admonition of Michael Riesman and Chris Antoniou in their 1994 book, *The Laws of War*, that for democracies like the United States, "even a limited armed conflict requires a substantial base of public support." That support "can erode or even reverse itself rapidly, no matter how worthy the political objective, if people *believe* that the war is being conducted in an unfair, inhumane, or iniquitous way" (emphasis added).[92]

In cyberwar, like any other conflict, victory depends much on what people believe. Cyber strategists would be well served to ensure that what they do in the coming years not only meets the challenges in cyberspace, but also fulfills the American people's expectations of all their warriors, regardless of the domain in which they operate. SSQ

Notes

1. See, for example, John Sutter, "Is Wikileaks engaged in 'Cyberwar'?" *CNN*, 9 December 2010, http://articles.cnn.com/2010-12-09/tech/wikileaks.cyber.attacks_1_cyber-war-cyber-weapons-cyber-attacks?_s=PM:TECH.

2. For a discussion of the Estonia and Georgia incidents, see Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), 11–21.

3. Norman Friedman, "Virus Season," *Proceedings* 136, no. 11 (November 2010): 88.

4. For purposes of this article, *cyberwar* may be defined as conflict waged by means of *cyber operations*. The latter are, in turn, defined by the DoD to be "employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace." The DoD defines *cyberspace* as "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." Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*, as amended through 30 September 2010, 118, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

5. LTG Keith B. Alexander, USA, quoted in Thom Shanker, "Cyberwar Nominee Sees Gaps in Law," *New York Times,* 14 April 2010, http://www.nytimes.com/2010/04/15/world/15military.html.

6. Jeffrey F. Addicott, "Cyberterrorism: Legal Policy Issues," in *Legal Issues in the Struggle against Terrorism*, eds. John N. Moore and Robert F. Turner (Durham, NC: Carolina Academic Press, 2010), 550.

7. This article considers LOAC to encompass jus ad bello (the international law which rationalizes recourse to armed conflict) and jus in bello (the international law which governs actions during armed conflict). For a discussion of jus ad bello and jus in bello in the cyber context, see, CDR Todd C. Huntley, JAGC, USN, "Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare," *Naval Law Review* 60 (2010): 1–40, http://www.jag.navy.mil/documents/navylawreview/NLRVolume60.pdf.

8. Strategist Carl von Clausewitz wrote: "The great uncertainty of all data in war is a peculiar difficulty, because all action must, to a certain extent, be planned in a mere twilight, which in addition not infrequently—like the effect of a fog or moonshine—gives to things exaggerated dimensions and unnatural appearance." Clausewitz, *On War*, bk. 2, chap. 2, par. 24.

9. See "Time for a Treaty" (editorial), *Defense News*, 18 October 2010, 36, http://www.defensenews.com/story.php?i=4921341.

10. Bruce Schneier, "It will soon be too late to stop the cyberwars," *Financial Times*, 2 December 2010, http://www.ft.com/cms/s/0/f863fb4c-fe53-11df-abac-00144feab49a.html#axzz19cNCeszp.

11. See John B. Alexander, "Optional Lethality: Evolving Attitudes towards Nonlethal Weaponry," *Harvard International Review*, 7 May 2006, http://hir.harvard.edu/the-future-of-war/optional-lethality.

12. Charles Krauthammer, "The Irrelevance of START," *Washington Post*, 26 November 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/25/AR2010112502232.html.

13. William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010), http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

14. See Richard W. Aldrich, "Information Warfare & the Protection of Critical Infrastructure," in *National Security Law*, 2d ed., eds. John N. Moore and Robert F. Turner (Durham, NC: Carolina Academic Press, 2005), 1243–44.

15. Tom Gjelten, "Shadow Wars: Debating Cyber 'Disarmament'," *World Affairs*, November/December 2010, http://www.worldaffairsjournal.org/articles/2010-NovDec/full-Gjelten-ND-2010.html.

16. Ibid.

17. Ibid. In 1999 the DoD Office of General Counsel concluded that "there seems to be no particularly good reason for the United States to support negotiations for new treaty obligations in most areas of international law that are directly relevant to information operations." Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, 2nd ed. (Washington: DoD, November 1999), 49, http://www.cs.georgetown.edu/~denning/infosec/DOD-IO-legal.doc [hereinafter *GC Memo*].

18. See Anna Mulrine, "When is a Cyberattack an Act of War?" *Christian Science Monitor*, 18 October 2010, 20, http://www.csmonitor.com/USA/Military/2010/1005/Pentagon-The-global-cyberwar-is-just-beginning.

19. Thomas Wingfield sees a third legal regime as applicable to cyber operations: intelligence collection law. Wingfield, in *Cyberpower and National Security*, ed. Franklin D. Kramer et al. (Washington: NDU Press, 2009), 541.

20. Elinor Mills, "Demilitarizing Cyberspace (Q&A)," *Tech Reviews* blog, December 2010, http://tech-reviews.findtechnews.net/demilitarizing-cybersecurity-qa/.

21. Walter Gary Sharp Sr., *Cyberspace and the Use of Force* (San Antonio, TX: Aegis Research Corp., 1999), 123–32.

22. See *GC Memo*, 11. Act of war is an "obsolete concept not mentioned in the UN Charter and seldom heard in modern diplomatic discourse."

23. *Charter of the United Nations and Statute of the International Court of Justice* (San Francisco: United Nations, 1945), http://treaties.un.org/doc/Publication/CTC/uncharter.pdf.

24. Ibid., 3.

25. Ibid., 10.

26. Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington: National Academies Press, 2010), 163, http://books.nap.edu/openbook.php?record_id=12997&page=R1.

27. For example, see Jeffrey F. Addicott, *Terrorism Law: Materials, Cases, Comments* (Tucson, AZ: Judges and Lawyers Publishing Co., 2011), 311–12.

28. Wg Cdr Duncan Blake, RAAF, and Lt Col Joseph S. Imburgia, USAF, " 'Bloodless weapons'? The need to conduct legal reviews of certain capabilities and the implications of defining them as 'weapons'," *Air Force Law Review*, 14 December 2010, 181–83.

29. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I),* 8 June 1977, Art. 49.1, http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079. Although the United States is not a party to *Protocol I*, it accepts that most of it comprises customary international law which binds all nations.

30. William Boothby, *Weapons and the Law of Armed Conflict* (Oxford, UK: Oxford Scholarship Online, 2009), 238.

31. See David E. Graham, "Cyber Threats and the Law of War," *Journal of National Security Law* 4, no. 1 (2010): 91, for a discussion of the "instrument-based approach" and the "strict liability" approach as competing analyses.

32. Schmitt, "Cyber Operations in International Law," 155–56.

33. For a discussion of the Schmitt criteria, see Wingfield, "International Law and Information Operations,"527–31.

34. Boothby, *Weapons and the Law of Armed Conflict*.

35. Schmitt, "Cyber Operations in International Law."

36. *Military and Paramilitary Activities in and against Nicaragua* (*Nicar. v. U.S.*), 1986 I.C.J. 14 (June 27), para. 195.

37. Ibid.

38. Ibid.

39. Michael Byers, *War Law: Understanding International Law and Armed Conflict* (New York: Grove Press, 2005), 72–81.

40. Kenneth Anderson on *Baumann v. Wittes*, *Lawfare* blog, 1 December 2010, http://www.lawfareblog.com/2010/12/kenneth-anderson-on-baumann-v-wittes/.

41. *GC Memo*, 20.

42. Schmitt, "Cyber Operations in International Law," 157.

43. *GC Memo*, 20.

44. Harold Koh, "The Obama Administration and International Law," speech, American Society of International Law, 25 March 2010, http://www.state.gov/s/l/releases/remarks/139119.htm.

45. Huntley, "Controlling the Use of Force in Cyberspace," 34.

46. In this context, "war" and "armed conflict" are interchangeable.

47. Yoram Dinstein, *War, Aggression and Self-Defence*, 4th ed. (Cambridge, UK: Cambridge University Press, 2005), 15.

48. Schmitt, "Cyber Operations in International Law," 175.

49. Jamie A. Williamson, "Challenges of Twenty-First-Century Conflicts: A Look at Direct Participation in Hostilities," *Duke Journal of Comparative & International Law* 20, no. 3 (Spring 2010): 464, http://www.law.duke.edu/journals/djcil/.

50. Koh, "Obama Administration and International Law."

51. Schmitt, "Cyber Operations in International Law," 176.

52. *Air Force Operations & the Law* (Maxwell AFB, AL: USAF Judge Advocate General's School, 2009), 99.

53. Koh, "Obama Administration and International Law."

54. See Burris Carnahan, "Weapons," in *Crimes of War: What the Public Should Know*, eds. Roy Gutman and David Rieff (New York: W. W. Norton, 1999), 380, http://www.crimesofwar.org/thebook/weapons.html.

55. See James P. Terry, "The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self Defense During Periods Short of Armed Conflict: What Are the Targeting Constraints?" *Military Law Review* 69 (September 2001): 70.

56. *Military objectives* are defined as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage." *Protocol I,* Art. 49.1.

57. Alexander quoted in Shanker, "Cyberwar Nominee Sees Gaps in Law."

58. Williamson, "Challenges of Twenty-First-Century Conflicts."

59. "Direct Participation in Hostilities: Questions and Answers," International Committee of the Red Cross, 2 June 2009, http://www.icrc.org/eng/resources/documents/faq/direct-participation-ihl-faq-020609.htm.

60. See CDR J. W. Crawford, "The Law of Noncombatant Immunity and the Targeting of National Electrical Power Systems," *Fletcher Forum of World Affairs*, Summer/Fall 1997, 101.

61. *Protocol I*, Art. 57.2(a)(i).

62. See Laurie Blank and Amos Guiora, "Teaching an Old Dog New Tricks: Operationalizing the Law of Armed Conflict in New Warfare," *Harvard National Security Journal* 1 (13 May 2010): 56–57, citing *Prosecutor v. Stanislav Galic*, http://www.harvardnsj.com/wp-content/uploads/2010/05/Vol.-1_Blank-Guiora_Final.pdf.

63. Schmitt, "Cyber Operations in International Law," 168.

64. Clarke and Knake, *Cyber War*, 40.

65. Gary Solis, "CIA drone attacks produce America's own unlawful combatants," *Washington Post*, 12 March 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/11/AR2010031103653.html.

66. *GC Memo*, 7.

67. Stephen Dycus et al., "The Military's Role in Homeland Security and Disaster Relief," in *National Security Law*, 4th ed. (New York: Aspen Publishers, 2007), 960.

68. Dana Priest and William Arkin, "A Hidden World, Growing beyond Control," *Washington Post*, 19 July 2010, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/?referrer=emaillink.

69. See Steve Lohr, "Computers That See You and Watch Over You," *New York Times*, 1 January 2011, 1, discussing the Defense Advanced Research Projects Agency's award of a grant for a research program called the Mind's Eye, which seeks "machines that can recognize, analyze and communicate what they see," http://www.nytimes.com/2011/01/02/science/02see.html?hp; and Siobhan Gorman, "U.S. Plans Cyber Shield for Utilities, Companies," *Wall Street Journal*, 8 July 2010, discussing an "expansive" NSA program "dubbed 'Perfect Citizen'," http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html.

70. DoD News Release, "Joint Statement by Secretary Gates and Secretary Napolitano on Enhancing Coordination to Secure America's Cyber Networks," 13 October 2010, http://www.defense.gov/releases/release.aspx?releaseid=13965.

71. Department of Justice Public Affairs, "The NSA Program to Detect and Prevent Terrorist Attacks: Myth v. Reality," 27 January 2006, http://www.justice.gov/opa/documents/nsa_myth_v_reality.pdf.

72. Paul Elias, "Judge Orders Feds to Pay $2.5 million in Wiretapping Case," *Washington Post*, 21 December 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/21/AR2010122105307.html.

73. Kim Zetter, "Military Monitored Planned Parenthood, Supremacists," *Wired* magazine, 25 February 2010, http://www.wired.com/threatlevel/2010/02/military-spied-on-planned-parenthood/.

74. Jason Sherman, "CENTCOM Eyes Blogs to Shape Opinion," *Military.com*, 3 March 2006, http://www.military.com/features/0,15240,89811,00.html.

75. Walter Pincus, "Military Expands Intelligence Role," *Washington Post*, 8 June 2010, A-15, http://www.washingtonpost.com/wp-dyn/content/article/2010/06/07/AR2010060704696.html.

76. Quoted in Mark V. Schanz, "Air Sovereignty Never Sleeps," *Air Force Magazine*, December 2010, 56, http://www.airforce-magazine.com/MagazineArchive/Documents/2010/December%202010/1210sovereignty.pdf.

77. Jack Goldsmith, *The Cyberthreat, Government Network Operations, and the Fourth Amendment* (Washington: Brookings Institution, 8 December 2010), 15, http://www.brookings.edu

/~/media/Files/rc/papers/2010/1208_4th_amendment_goldsmith/1208_4th_amendment_goldsmith.pdf.

78. DoD News Release, "Joint Statement by Secretary Gates and Secretary Napolitano."

79. William Matthews, "DoD to Protect Some Civilian Infrastructure," *Defense News*, 18 October 2010, 6.

80. Goldsmith, *Cyberthreat,* 14.

81. See Senate press release, "Lieberman, Collins, Carper Unveil Major Cybersecurity Bill to Modernize, Strengthen, and Coordinate Cyber Defenses," 10 June 2010, for a link to the bill, http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=227d9e1e-5056-8059-765f-2239d301fb7f.

82. The "primary business of armies and navies [is] to fight or be ready to fight wars should the occasion arise." *United States ex rel. Toth v. Quarles*, 350 U.S. 11 (1955).

83. See Gary McGraw and Ivan Arce, "Software [In]security: Cyber Warmongering and Influence Peddling," *informIT.com*, 24 November 2010, http://www.informit.com/articles/article.aspx?p=1662328#.

84. "The rights of men in the armed forces must perforce be conditioned to meet certain overriding demands of discipline and duty." *Burns v. Wilson*, 1953, 346 U.S. 137 (1953). "The essence of military service is the subordination of the desires and interests of the individual to the needs of the service." *Goldman v. Weinberger*, 475 U.S. 503 (1986).

85. Risk-management experts John Mueller and Mark G. Stewart conclude from a survey of many studies that the risk of terrorism is "hardly existential" and is, in fact, "so low that spending further to reduce its likelihood or consequences is scarcely justified." See Mueller and Stewart, "Hardly Existential: Thinking Rationally about Terrorism," *Foreign Affairs.com*, 2 April 2010, http://www.foreignaffairs.com/articles/66186/john-mueller-and-mark-g-stewart/hardly-existential.

86. See Seymour M. Hersh, "The Online Threat," *New Yorker*, 1 November 2010, http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh.

87. Fareed Zakaria, "What America Has Lost; It's Clear We Overreacted to 9/11," *Newsweek*, 13 September 2010, 18, http://www.newsweek.com/2010/09/04/zakaria-why-america-overreacted-to-9-11.html.

88. See Mark Silva, "Few trust the government, poll finds," *Los Angeles Times*, 19 April 2010, http://articles.latimes.com/2010/apr/19/nation/la-na-distrust19-2010apr19.

89. See Hersh, "Online Threat."

90. The new DoD *Law of War Manual* is expected to have a "17-page chapter on information and cyberspace operations." See W. Hays Parks, "National Security Law in Practice: The Department of Defense *Law of War Manual*," speech, 18 November 2010, http://www.abanet.org/natsecurity/hays_parks_speech11082010.pdf.

91. William George Eckhardt, "Lawyering for Uncle Sam When He Draws His Sword," *Chicago Journal of International Law 4, no. 2 (Fall 2003): 431.*

92. W. Michael Reisman and Chris T. Antoniou, eds., *The Laws of War* (New York: Vintage, 1994), xxiv.