# Some Reflections on the Intersection of Law and Ethics in Cyber War

Maj Gen Charles J. Dunlap Jr., USAF, Retired

Few security issues have captured the attention of the public as has the specter of cyber war. In a recent op-ed, President Obama warns that "the cyber threat to our nation is one of the most serious economic and national security challenges we face."[1] This, in turn, has raised many questions about the legal parameters of cyber operations, including the rules applicable to actual cyber war.[2]

Parallel to the growing interest in the legal aspects of cyber war are an increasing number of questions focused on the ethical dimension. That is an important consideration for any military endeavor but one just emerging with respect to cyber operations.[3] Mounting concern about the ethical aspects of cyber activities led the US Naval Academy to sponsor an entire conference on the subject in the spring of 2012.[4] Even

more recently, the *Atlantic* published an article entitled "Is It Possible to Wage a Just Cyberwar?," which discussed several intriguing issues.[5]

This article reflects upon a few issues that illustrate how legal and ethical concerns intersect in the cyber realm. Such an intersection should not be especially surprising. As historian Geoffrey Best insists, "it must never be forgotten that the law of war, wherever it began at all, began mainly as a matter of religion and ethics. . . . It began in ethics and it has kept one foot in ethics ever since."[6] Understanding that relationship is vital to appreciating the full scope of the responsibilities of a cyber warrior in the twenty-first century.

## Law and Ethics

How do law and ethics relate? Certainly, adherence to the law is a baseline ethical responsibility, but it is only that—a baseline. In the March 2012 edition of *Armed Forces Journal*, Lt Gabriel Bradley, USN, points out that "the law of armed conflict sets minimum standards." He goes on to argue persuasively that inculcating individual and institutional moral and ethical values—a sense of honor, if you will—is essential to ensuring *actual* compliance with the law. And he is certainly right when he quotes Christopher Coker's observation that "laws can reaffirm the warrior ethos; they cannot replace it."[7]

Of course, even determining the baseline—that is, the law—is not always easy in twenty-first-century operations generally but especially with regard to cyber activities. Among the many reasons for this difficulty is the fact that most of the law of armed conflict was designed to address conflicts waged mainly with kinetic weaponry. Nevertheless, in this writer's view, existing law has ready applicability to cyber operations, a notion that perhaps brings us to the first issue regarding the intersection of law, ethics, and cyber operations.[8] Specifically, we sometimes hear that cyberspace is such a new domain that no existing law could—or even *should*—apply to military operations in it.

Such an idea is simply untrue. Most of the law of armed conflict is not domain specific. Along this line, consider a recent project by the Harvard Program on Humanitarian Policy and Conflict Research to write a manual specifically on the international law applicable to air and missile warfare.[9] The program did produce a useful volume, but it is a relatively thin one since the project discovered a comparatively modest amount of law that seemed wholly unique to the air and space domains. One can say much the same about the cyber domain, including ethical considerations.[10]

Furthermore, what sometimes masquerades as a legal problem in cyber operations is often more of a technical issue or a policy conundrum—*not* an authentic legal problem. The much ballyhooed issue of what constitutes the proverbial "act of war" in the cyber domain offers a good example. Although the phrase "act of war" is a political term, not a legal axiom, such phrases as "use of force" and "armed attack" *do* have legal meaning and could relate to a casus belli in terms of a forceful response.[11]

In fact, the interpretation of such expressions in the cyber realm is resolvable under the law if—*and, really, only "if"*—technology can provide adequate data regarding, for example, the actual harm caused by the supposed "attack," as well as sufficient information about who actually did it. Of course, the absence of attribution data (technically challenging to obtain in the cyber realm) can be a definitive legal and ethical bar to a forceful response. This may prove frustrating when people want to "do something" in answer to a cyber incident, but it is hardly unreasonable for the law—*and ethics*—to require reliable information concerning who might be responsible before launching a counter of some kind.

Technologically speaking, the daunting task of determining attribution is *not* a problem for lawyers or, for that matter, ethicists; rather, it is something for technologists to solve.[12] It is interesting, therefore, that the authors of the above-mentioned *Atlantic* article argue—in relation to the alleged use of a cyber weapon (Stuxnet) against Iran's nu-

clear development facilities—that "the lack of attribution of Stuxnet raises ethical concerns because it denied Iran the ability to counterattack, encouraging it towards ever more extreme behavior."[13]

Aside from the question of whether Iran would necessarily have a legal or moral basis to counterattack as a result of the alleged Stuxnet operation, it is of further interest that the authors of the *Atlantic* piece say that "to make attribution work, we need international agreements." These would include, they contend, agreements that "cyberattacks should carry a digital signature of the attacking organization" and that certain networking protocols could be used to "make attribution easier."[14]

Most experts would probably say that current law does not require such facilitation of cyber attribution.[15] Nevertheless, the authors of the *Atlantic* article argue for "better [cooperation] on international network monitoring to trace sources of attacks" and seem to believe that "economic incentives, such as the threat of trade sanctions, can make such agreements desirable."[16] Again, one might disagree with much about these proposals, but the authors should be commended for at least beginning the dialogue on possible ways of addressing one of the most perplexing legal and moral questions of cyber war.

As with attribution, technological issues—not the law per se—are also the most challenging aspect of the targeting of cyber weaponry. The cardinal legal and ethical principles of distinction and proportionality require technical data that will inform decision makers as to who might be affected by a particular technique, and to what extent.[17] Again, that this may prove technically difficult is neither a legal nor an ethical problem but a scientific one. Indeed, one can say that the ability to model effects with dependable accuracy represents one of the most needed capabilities in the world of cyber operations. Such an ability would give decision makers—not to mention lawyers and ethicists—the kind of information that is patently essential for making reasoned judgments about employing a cyber methodology.

## Do Legal and Ethical Values Unduly Encumber Cyber Warriors?

Over and above questions about the application of legal regimes and ethical mores to a particular cyber scenario is the broader question of whether any restraints should apply at all. More specifically, some people believe that attempts to apply the law will encumber the United States' cyber efforts and put its security at risk. This rather surprising question lies at the heart of a serious debate in which Stewart Baker and this writer engaged under the auspices of the American Bar Association.[18]

By way of context, Mr. Baker, a highly respected lawyer with the prestigious Washington law firm of Steptoe and Johnson, had previously served in government as general counsel for the National Security Agency as well as assistant secretary for policy in the US Department of Homeland Security. He begins his polemic this way: "Lawyers don't win wars. But can they lose a war? We're likely to find out, and soon. Lawyers across the government have raised so many showstopping legal questions about cyberwar that they've left our military unable to fight, or even plan for, a war in cyberspace."[19]

Mr. Baker further claims that any attempts to "impose limits on cyberwar [are] . . . doomed."[20] Among the most troubling aspects of his argument is really an ethical one of the first order. He points to the devastation caused by air warfare during World War II and refers to the claim made by former British prime minister Stanley Baldwin in 1932 that in air warfare "the only defense is in offense, which means that you have got to kill more women and children more quickly than the enemy if you want to save yourselves."[21]

Mr. Baker then goes on to cite Mr. Baldwin's "kill more women and children more quickly" concept by asserting that "if we want to defend against the horrors of cyberwar, we need first to face them *with the candor of a Stanley Baldwin*" (emphasis added).[22] Only after construct-

ing a cyber war strategy so framed would Mr. Baker consider it appropriate to "ask the lawyers for their thoughts."[23]

Fully reprising my response lies beyond the scope of this article (although the title—"Lawless Cyberwar? Not If You Want to Win"—may suggest its content).[24] Suffice it to say that it is vitally important in cyber war (as in any military operation) to ground the "limits" whenever possible, not only in the law or ethics per se but also in pragmatic, war-fighting rationale. In the case of cyber, this is not particularly difficult to do, especially if the actual war fighters do not perceive an asymmetry between what law and ethics might require and what they believe they need to accomplish their mission.

Notwithstanding Mr. Baker's assertion that legal machinations have left the armed forces "unable to fight, or even plan for, a war in cyberspace," Gen Robert Kehler, USAF, commander of US Strategic Command, whose subordinate organization US Cyber Command is the leading proponent of military cyber planning and operations, seems to disagree. In November 2011, he declared that he did "not believe that we need new explicit authorities to conduct offensive operations of any kind." Furthermore, Kehler said that that he did "not think there is any issue about authority to conduct [cyber] operations."[25] In short, the *war fighters* apparently do not see an incompatibility with legal and ethical restraints and their ability to effectively "plan for a war in cyberspace."

Adherence to the rule of law is especially important in the cyber realm because nearly all experts agree that confronting the threat requires the cooperation of foreign countries in order to track and neutralize cyber threats—in peace or war.[26] Nations vital to this effort, including especially the world's major democracies, doubtlessly would not be inclined to cooperate with any country that rejected limits on military operations, cyber or otherwise. Professors Michael Reisman and Chris T. Antoniou point out in their book *The Laws of War* that "in modern popular democracies, 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).[27]

A dismissal of Mr. Baker's construct for cyber war does not suggest, however, that ethical and legal concerns about cyber war are therefore obviated. For example, one of the most serious concerns involves the role of civilians in cyber operations.

## Civilian Cyber Warriors

It almost goes without saying that enormous cyber expertise lies in the civilian community and that the armed forces must have access to it. That said, the extent of that access and precisely what that access does—or *should*—mean are properly the subject of legal and ethical scrutiny.

The basics are not hard. To enjoy the combatant privilege—that is, a "license," so to speak, to engage in lawful destructive acts against the enemy's person or property without fear of prosecution—one must ordinarily be a member of the duly constituted armed forces of a belligerent in an armed conflict.[28] People have often mistakenly taken this to mean that a civilian cannot directly participate in hostilities. Actually, civilians can do so without necessarily committing a war crime, but there are consequences.

Chief among them is the fact that if civilians fall into the hands of enemies, they might properly subject them to domestic criminal law for acts that, if done by a member of the opposing military, would be privileged from prosecution. Moreover, under the law of war, civilians are targetable—by either kinetic or cyber means—when they directly participate in hostilities. In the cyber context, one should understand that even the International Committee of the Red Cross explicitly uses as examples of direct participation acts that one would expect of a cyber warrior—that is, "interfering electronically with military computer networks (computer network attacks) and transmitting tactical targeting intelligence for a specific attack."[29]

What does all of this mean from an ethical perspective? For one thing, it is essential that civilians understand the potential consequences, especially when they are away from the work site, such as at home with their families. Despite the debate in the international community about circumstances that would allow an adversary to target a civilian on the same basis as a member of the armed forces, the International Committee of the Red Cross agrees that such targeting applies to civilians who "assume a 'continuous combat function' " (as opposed to merely "participating in hostilities in a spontaneous, sporadic or unorganized way").[30]

Members of the armed forces—along with civilians regularly engaged in a "a continuous combat function" such as computer network attack—can be attacked with any legal weapon wherever and whenever found, regardless of whether at that particular moment they present an imminent threat or are otherwise performing a military function. This means, for example, that a civilian cyber warrior regularly engaged in computer network attack operations could legitimately come under attack by a lawful belligerent (not a terrorist) in his or her home in a Washington suburb. Further, the adversary could use any lawful weapon—not just a cyber weapon—if it otherwise complies with the law of war. Accordingly, if the civilian is sufficiently critical to military cyber operations, he or she could be assaulted with great violence wherever found. However, the incidental death and injury to innocent civilians (e.g., the cyber warrior's own family) that might occur in the attack should not be "excessive in relation to the concrete and direct military advantage anticipated" ("military advantage," of course, refers to the elimination or neutralization of the cyber expert).[31]

Thus, the ethical issue for cyber warriors may be the extent to which one may appropriately ask civilians to take these kinds of risks. It is one thing for members of the armed forces who voluntarily undertake the proverbial "unlimited liability contract" of military service to put themselves at risk. It is quite another to ask civilians to do so—and something further to expect the families of civilians to accept that they

may become collateral damage in a conflict that has violent expressions along with nonkinetic cyber effects. In cyber war, the "front lines" may be far from what anyone might recognize as the traditional battlefield.

No one knows how real this kind of threat might be. However, in an era of "sleeper cells" and the proliferation of other clandestine special operations forces among many countries, this type of counter to America's cyber capabilities may not be as outlandish as some might think. In any event, this discussion of personal risk that cyber operations might occasion makes it somewhat ironic that cyber warriors need to steel themselves for a cruel assault on their ethics and professionalism by some critics.

## Challenges to the Martial Ethic of Cyber Warriors?

Perhaps one of the most perplexing critiques that has accompanied the growing use of advanced technologies in war is the penchant among some contemporary commentators to assume that it is somehow "unmanly" or "unworthy" to employ them. Consider the experience of drone operators who, like cyber combatants, wage war from computer consoles. One pundit's very recent article entitled "With Its Deadly Drones, the US Is Fighting a Coward's War" offers an example of the kind of nasty rhetoric used.[32] Though such aspersions have not yet made their way to cyber warriors, it is perhaps only a matter of time before they find themselves subject to the same kind of insult to their professional ethic.

How did all of this start? We might trace it to remarks a few years ago by Dr. David Kilcullen, a lieutenant colonel retired from the Australian army who has become one the foremost advocates of the ground-centric, manpower-intensive form of counterinsurgency that found expression in Field Manual 3-24 / Marine Corps Warfighting Publication 3-33.5, *Counterinsurgency*, published in 2006.[33] It is important to understand that the manual is rather hostile to air operations in

general, devoting just five pages to them in the 300-page document, so Dr. Kilcullen's critique of drones does not seem inconsistent with his broader views about airpower.

In any event, Dr. Kilcullen argued before Congress in 2009 that drone attacks against terrorists were "backfiring": "In the Pashtun tribal culture of honor and revenge, face-to-face combat is seen as brave; shooting people with missiles from 20,000 feet is not." According to Kilcullen, "using robots from the air . . . looks both cowardly and weak."[34] Quite obviously, one might rather easily apply his thesis to cyber operations and those who conduct them.

What makes these statements stunning in their irony is that the adversary to which Kilcullen refers not only uses remotely detonated improvised explosive devices to kill US forces from the safety of distance, but also employs children to plant them.[35] Would that not make such an enemy, by his own "culture of honor" standards, "cowardly and weak"? Regardless, this entire discussion, however demoralizing and inaccurate, is—in terms of actual war fighting—rather immaterial. The "object of war," as Gen George Patton rather graphically put it, "is not to die for your country but to make the other guy die for his."

Physical courage, however admirable, is not the only quality one needs for victory in twenty-first-century warfare—and perhaps ever. Native Americans, for example, waged war with extraordinary courage. Yet, in the April 2012 issue of the *Journal of Military History*, historian Anthony R. McGinnis points out that Native Americans' individualistic and stylized form of warfare was no match for "a modern technologically advanced nation" with "ultimate victory as its goal."[36] Of course, there is nothing wrong with being "a modern technologically advanced nation" with "ultimate victory as its goal" as long as one uses those technological advances in a legally and ethically appropriate way.

In reality, there is nothing unethical about waging war from afar, and there is nothing especially unusual about it. Since practically the beginning of time, warriors have sought to engage their adversaries in

ways that denied them the opportunity to bring their weapons to bear. For example, as this writer has said elsewhere,

> David slew Goliath with a missile weapon before the giant could bring his weapons to bear; the sixteen-foot pikes of Alexander the Great's phalanxes reached their targets well ahead of the twelve foot pikes wielded by their opponents; English longbowmen destroyed the flower of French knighthood at Agincourt from afar when they rained arrows down upon the horsemen; and, more recently, U.S. and British tanks destroyed the heart of Saddam's armor forces during 1991's Battle of 73 Easting much because their guns outranged those of Iraq's T-72 tanks. There is nothing new about killing from a distance.[37]

Still, something about computerized warfare draws special scorn from certain individuals, however wrongly and unfairly. For example, the United Nations commissioned Philip Alston, a New York University law professor, as a "special rapporteur" to write a report on targeted killings. The document he produced included his opinions about drone operators. In it he charged that because drone operations can be conducted "entirely through computer screens and remote audiofeed, there is a risk of developing a 'Playstation' mentality to killing."[38]

A "Playstation" mentality to killing? That even the suggestion of such an insulting lack of professionalism would find itself into an official United Nations report is, itself, disquieting. The principal evidence for Professor Alston's finding appears to be his own speculations about the mind-set of those doing a task he himself has never performed. The actual evidence, however, points in a very different direction than the one Alston suggests—one that reinforces the idea that these officers hardly consider their duties a game. Indeed, Dr. Peter Singer of the Brookings Institution said in 2010 that in his studies he found "higher levels of combat stress among [some drone] units than among some units in Afghanistan." He concluded that operators suffered "significantly increased fatigue, emotional exhaustion and burnout."[39] These maladies are hardly indicative of "game" players.

More recently, the *Air Force Times* quoted an Air Force official who countered the "video game" accusation directly by pointing out that

the responsibilities of drone operators were extremely stressful and that the operations were "a deeply, deeply emotional event. It's not detached. It's not a video game."[40] While debate still roils, it demonstrates how quickly some critics deride the professionalism of principled people doing what their nation asks them to do.[41] Quite obviously, the comparison with cyber operations is not quite the same. Regardless, cyber operators are in the very serious business of defending their country and, in doing so, may be called upon to wreak havoc via cyber methodologies upon an adversary. Though the means of doing so may be different, the professionalism demanded by the operations is very high, and the psychological burdens on those who conduct them are likely very great.

Another aspect of the drone campaigns has emerged that might find analogy in the ethics and professionalism that cyber operators must display. In an April 2012 article in *Rolling Stone*, controversial writer Michael Hastings claims that

> the remote-control nature of unmanned missions enables . . . the Pentagon and the CIA [to] now launch military strikes or order assassinations without putting a single boot on the ground—and without worrying about a public backlash over U.S. soldiers coming home in body bags. The immediacy and secrecy of drones make it easier than ever for leaders to unleash America's military might—and harder than ever to evaluate the consequences of such clandestine attacks.[42]

For all his bluster, Hastings has something of a point when he says that "the immediacy and secrecy of drones make it easier than ever for leaders to unleash America's military might." In this writer's experience, senior decision makers are keenly aware that any military operation can have unintended consequences—no matter how "cost free" it might seem in planning. Still, what he says with respect to drones might find a parallel with cyber operations and could call upon cyber warriors to robustly exhibit ethical virtues, including especially candor and courage.

## The Need for Frank, Holistic Advice

The newness of cyber operations, the uncertainty of their precise effect, and the sheer difficulty of their execution may not always be fully understood by all participants in the chain of decision. These conditions may give rise to another ethical responsibility: to render frank, holistic advice. It is possible that in a given situation, those involved in the process may have to step out of their lane, so to speak, to ask the hard questions or point out inconvenient facts. If America's cyber power is to be "unleashed," as Hastings might put it, the nation must do so with the same care as it would with a more traditional military operation. To underline this point, we may call upon someone to go beyond the norm, just to make sure that all the right concerns are taken into account—including ethical and legal ones—so that the best decisions are made.

Fortunately (for lawyers, anyway) the American Bar Association's Model Code of Professional Conduct—the ethical "bible" for lawyers—specifically allows such holistic advice. Rule 2.1 of the code calls upon lawyers to "exercise independent professional judgment and render candid advice." Furthermore, lawyers are not limited to providing legal advice, as the rule goes on to say that "in rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client's situation."[43] In truth, this is the right guidance not just for lawyers but, really, for *all* military and civilian cyber professionals because the success of such operations depends upon a wide range of factors, and it is incumbent upon all involved to work together to ensure that they come to light and receive appropriate consideration.

The American Bar Association's rule mentions candor. Again, this is not something simply for attorneys but a fundamental ethical virtue for all defense professionals.[44] Among other things, one should keep this trait in mind when assessing the potential threat that cyber represents. Misstating or, worse, deliberately misrepresenting the threat can lead to poor allocations of resources and other errors in judgment. Opinions

about the scope and nature of the threat differ widely; in a *PBS Newshour* interview in the spring of 2012, Terry Benzel of the Information Research Institute insists that "all of us in [the cyber] community, we talk about cyber-Pearl Harbor. And it's not if. It's when."[45] Similarly, a "leading European cybersecurity expert says international action is needed to prevent a catastrophic cyberwar and cyberterrorism."[46]

Not everyone agrees, however. In April 2012, Rear Adm Samuel Cox, director of intelligence at US Cyber Command, reportedly "downplayed the prospect that an enemy of the United States could completely disable the nation's electric power grid or shut down the Internet because those systems are designed to withstand severe cyberattacks."[47] More stinging is an article of February 2012 in *Wired*, in which researchers Jerry Brito and Tate Watkins debunk much of the histrionic talk about the threat of cyber war: "Evidence to sustain such dire warnings [about cyberwar] is conspicuously absent."[48] Consistent with their conclusions is a 2011 report by the Organization for Economic Cooperation and Development. Asserting that governments "need to make detailed preparations to withstand and recover from a wide range of unwanted cyber events, both accidental and deliberate," the authors of the study nevertheless conclude "that very few single cyber-related events have the capacity to cause a global shock."[49] Writing in *Foreign Policy*, analyst Thomas Rid contends that cyber war is "still more hype than hazard."[50]

All of this raises concerns because Brito and Watkins say that "in many respects, rhetoric about cyber catastrophe resembles threat inflation we saw in the run-up to the Iraq War." They also point out that "cybersecurity is a big and booming industry" and that "Washington teems with people who have a vested interest in conflating and inflating threats to our digital security." Although they stop short of actually accusing anyone of pushing fears of cyber war for personal gain, they do call for a "stop [in the] apocalyptic rhetoric" and insist that "alarmist scenarios dominating policy discourse may be good for the cybersecurity-industrial complex, but they aren't doing real security any favors."[51]

The scope and immediacy of the threat are rightly debated, yet all might agree that, in any case, deliberately overstating (or understating) the threat—*even for the well-intentioned reasons of advocacy*—can raise questions of ethics and professionalism. As Brito and Watkins suggest, the run-up to the war with Iraq in 2003 makes clear what can happen when a threat is misconstrued (perhaps the reason that they entitle their polemic "Cyberwar Is the New Yellowcake"). In short, candor—and tempered rhetoric *if appropriate*—are critical qualities for cyber warriors. President Obama's measured language, which urges people to take the cyber threat "seriously" and to make planning for it a "priority," represents a responsible approach that highlights the dangers without falling victim to counterproductive and misleading hyping.[52]

## The Virtue of Competence

Finally, one of the key ethical responsibilities of cyber warriors is competence. Again, the American Bar Association's Model Rules of Professional Conduct provide guidance that all cyber professionals may want to consider analogizing to their responsibilities. Rule 1.1 of that code says that "competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[53] For those concerned about the legal and ethical aspects of cyber war, the mandate for competence goes well beyond knowledge and understanding of law and/or ethics per se.

Undoubtedly, many aspects of cyber operations are extraordinarily complex. Thus, legal—and other—advisers must become as familiar as possible with the cyber client's "business," including its technical aspects. A working knowledge of the technology not only will help advisers understand the facts sufficiently to apply legal and ethical principles to them, but also will give such advisers all-important *credibility* with those who seek their counsel in the first place. Decision makers in the cyber realm, like those seeking counsel in other activities, naturally will gravitate towards those who show a genuine understanding of the many intricacies of their discipline.

This is not an easy task. Staying current with the technology in this phenomenally complicated field is a time-consuming and never-ending job. But it is one that must be undertaken well in advance of need because failing to do so may lead to a lifetime of regret. Winston Churchill once observed that "to every man, there comes in his lifetime that special moment when he is figuratively tapped on the shoulder and offered that chance to do a very special thing, unique to him and fitted to his talents. What a tragedy if that moment finds him unprepared or unqualified for that which would be his finest hour."[54]

## Concluding Observations

This article has sought to illustrate just a few of the examples of how law and ethics might intersect. It may invite the question, Which of these imperatives will best operate to impose the limits on cyber war that honorable, yet pragmatic, people demand? Kenneth Anderson, a professor of law at American University, recently had occasion to consider one of his earlier writings about the efficacy of law and honor as "engines" for right behavior in conflict:

> Faith in legality as the engine driving such adherence as exists to the laws of war seems to me, however, entirely misplaced; it is a fantasy tailor-made for lawyers, and especially for American lawyers. Lawyers believe the problem is one of enforcement, whereas in fact it is one of allegiance. Codifications of international law are a useful template for organizing the categories of a soldier's duties. But, in the end, the culture relevant to respect for international humanitarian law is not the culture of legality and the cult of lawyers, but instead it is the culture of the professional honour of soldiers, and what they are willing or not willing to do on the battlefield.[55]

The question of whether "honor" is conterminous with ethics or a subset of the same may be appropriate for a lively university debate. What is more important to note, however, as Anderson does, is that John Keegan, perhaps the most eminent military historian of the modern era, had no reservations in saying that "there is no substitute for

honour as a medium for enforcing decency on the battlefield, never has been, and never will be."[56]

The cyber "battlefields" may not much resemble the ones to which Keegan refers, but his view certainly has equal applicability. In the end, honor and the ethical mind-set it implies are indispensable. Yet the discussion cannot end there because merely having developed the character to come to know the right answer is not enough since it may take courage to insist upon it.

The courage that cyber warriors need is not necessarily the *physical* courage that traditional battlefield combatants are called upon to display. Rather, it is vastly more likely that cyber combatants will need to exhibit *moral* courage.[57] This is especially so as norms develop for the conduct of cyber operations. Doing the right thing, particularly in circumstances of extreme urgency for which we have no explicit guidance—save for reference to classic tenets of law and ethics—may be quite a challenge.

Cyber combatants may wish to consider that in his classic study of military heroism, another British historian, Max Hastings, concludes that "physical bravery is found [in the military] more often than the spiritual variety." "Moral courage," he insists "is rare."[58] Yet, cyber warriors most need to exhibit exactly this kind of "rare." The law can provide an architecture, but only when honor and moral courage intersect can we truly rest assured that ethical principles worth defending are actually preserved. ✪

## Notes

1. Barack Obama, "Taking the Cyberattack Threat Seriously," *Wall Street Journal*, 19 July 2012, http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html.

2. For example, the International Law Division of the US Naval War College held a conference devoted to the legal aspects of cyber war in June 2012. See "2012 ILD Conference," US Naval War College, accessed 25 September 2012, http://www.usnwc.edu/ILDJune2012.

3. See, for example, Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (December 2010): 384, 385. "There are no informed, open, public or political discussions of what an ethical and wise policy for the use of such [cyber] weapons would be" (ibid., 385).

4. "McCain Conference: Warfare in a New Domain; The Ethics of Military Cyber Operations," United States Naval Academy, Stockdale Center for Ethical Leadership, 26–27 April 2012, http://www.usna.edu/ethics/publications/mccain2012.php. Much of this article comes from a presentation the author made at this conference.

5. Patrick Lin, Fritz Allhoff, and Neil Rowe, "Is It Possible to Wage a Just Cyberwar?," *Atlantic*, 5 June 2012, http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/.

6. Geoffrey Best, *War and Law since 1945* (Oxford, UK: Oxford University Press, 1994), 289.

7. Lt Gabriel Bradley, "Honor, Not Law," *Armed Forces Journal* 149, no. 7 (March 2012), http://www.armedforcesjournal.com/2012/03/9563756.

8. Harold Hongju Koh, legal advisor, Department of State, "International Law in Cyberspace" (remarks, USCYBERCOM Interagency Legal Conference, Fort Meade, MD, 18 September 2012), http://www.state.gov/s/l/releases/remarks/197924.htm.

9. Program on Humanitarian Policy and Conflict Research, *Manual on International Law Applicable to Air and Missile Warfare* (Cambridge, MA: Program on Humanitarian Policy and Conflict Research, Harvard University, 2009), http://ihlresearch.org/amw/HPCR%20Manual.pdf.

10. See, for example, Roger Crisp, "Cyberwarfare: No New Ethics Needed," *Practical Ethics* (blog), 19 June 2012, http://blog.practicalethics.ox.ac.uk/2012/06/cyberwarfare-no-new-ethics-needed/.

11. These terms are used, for example, in Article 2 and Article 52, respectively, of the Charter of the United Nations. United Nations, *Charter of the United Nations and Statute of the International Court of Justice* (Washington, DC: Government Printing Office, 1946), http://treaties.un.org/doc/Publication/CTC/uncharter.pdf.

12. "Over the last two years, DoD has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America." Secretary of Defense Leon E. Panetta (remarks on cybersecurity to the Business Executives for National Security, New York City, 11 October 2012), http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

13. Lin, Allhoff, and Rowe, "Is It Possible?"

14. Ibid. If, for example, one can make a factual case for the proper application of the doctrine of anticipatory self-defense by a nation-state, then Iran would have neither a legal nor a moral basis to respond. For a discussion of anticipatory self-defense, see, generally, Kinga Tibori Szabó, *Anticipatory Action in Self-Defence: Essence and Limits under International Law* (Hague, Netherlands: T. M. C. Asser Press, 2011).

15. See, for example, Crisp, "Cyberwarfare," 9.

16. Lin, Allhoff, and Rowe, "Is It Possible?"

17. Harold Koh, legal adviser for the US State Department, explains the terms: "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" (emphasis in original). Harold Hongju Koh, "The Obama Administration and International Law" (speech, Annual Meeting of the American Society of International Law, Washington, DC, 25 March 2010), http://www.state.gov/s/l/releases/remarks/139119.htm.

18. Stewart A. Baker and Charles J. Dunlap Jr., "What Is the Role of Lawyers in Cyberwarfare?," *ABA Journal*, 1 May 2012, http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/.

19. Ibid.

20. Ibid.

21. Ibid.

22. Ibid.

23. Ibid.

24. Charles J. Dunlap Jr., "Lawless Cyberwar? Not If You Want to Win," American Bar Association, accessed 21 September 2012, http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch9/ch9_ess2.html.

25. Quoted in Jim Wolf, "U.S. Military Better Prepared for Cyber Warfare: General," Reuters, 16 November 2011, http://www.reuters.com/article/2011/11/17/us-usa-cyber-military-idUSTRE7AG03U20111117?feedType=RSS&feedName=everything&virtualBrandChannel=11563.

26. See, for example, Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 9, http://www.defense.gov/news/d20110714cyber.pdf. "Cyberspace is a network of networks that includes thousands of [Internet service providers] across the globe; no single state or organization can maintain effective cyber defenses on its own" (ibid.).

27. W. Michael Reisman and Chris T. Antoniou, eds., *The Laws of War: A Comprehensive Collection of Primary Documents on International Laws Governing Armed Conflict* (New York: Vintage Books, 1994), xxiv.

28. See, generally, Gary D. Solis, *The Law of War* (New York: Cambridge University Press, 2010), 41–42.

29. "Direct Participation in Hostilities: Questions and Answers," International Committee of the Red Cross, 6 February 2009, http://www.icrc.org/eng/resources/documents/faq/direct-participation-ihl-faq-020609.htm.

30. Ibid.

31. Koh, speech.

32. George Monbiot, "With Its Deadly Drones, the US Is Fighting a Coward's War," *Guardian* (United Kingdom), 30 January 2012, http://www.guardian.co.uk/commentisfree/2012/jan/30/deadly-drones-us-cowards-war.

33. Field Manual 3-24 / Marine Corps Warfighting Publication 3-33.5, *Counterinsurgency*, December 2006, http://armypubs.army.mil/doctrine/DR_pubs/DR_a/pdf/fm3_24.pdf.

34. Quoted in Doyle McManus, "U.S. Drone Attacks in Pakistan 'Backfiring,' Congress Told," *Los Angeles Times*, 3 May 2009, http://articles.latimes.com/2009/may/03/opinion/oe-mcmanus3.

35. Christopher Leake, "Taliban Make Children Plant IEDs to Thwart Army Snipers," *Daily Mail*, 6 February 2010, http://www.dailymail.co.uk/news/article-1249044/Taliban-makes-children-plant-IEDs-thwart-Army-snipers.html.

36. Anthony R. McGinnis, "When Courage Was Not Enough: Plains Indians at War with the United States Army," *Journal of Military History* 76, no. 2 (April 2012): 473.

37. Charles J. Dunlap Jr., "Does Lawfare Need an Apologia?," *Case Western Reserve Journal of International Law* 43, no. 1/2 (2011): 132.

38. United Nations, General Assembly, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston: Addendum, Study on Targeted Killings*, A/HRC/14/24/Add.6 (New York: United Nations, General Assembly, 28 May 2010), 25, http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf.

39. Marc Pitzke, "Interview with Defense Expert P. W. Singer: 'The Soldiers Call It War Porn,' " *Spiegel Online International*, 12 March 2010, http://www.spiegel.de/international/world/0,1518,682852,00.html.

40. Jeff Schogol and Markeshia Ricks, "Demand Grows for UAV Pilots, Sensor Operators," *Air Force Times*, 21 April 2012.

41. See, for example, Kenneth Anderson, "Laurie Blank on Mark Mazzetti's 'The Drone Zone'—Last in Series from Lewis, Dunlap, Rona, Corn, and Anderson," *Lawfare* (blog), 21 July 2012, http://www.lawfareblog.com/2012/07/laurie-blank-on-the-mazzetti-the-drone-zone-last-in-series-from-lewis-dunlap-rona-corn-and-anderson/.

42. Michael Hastings, "The Rise of the Killer Drones: How America Goes to War in Secret," *Rolling Stone*, 16 April 2012, http://www.rollingstone.com/politics/news/the-rise-of-the-killer-drones-how-america-goes-to-war-in-secret-20120416#ixzz22VDkfR00.

43. "Rule 2.1: Advisor," American Bar Association, Center for Professional Responsibility, accessed 25 September 2012, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_2_1_advisor.html.

44. Compare the following from the listing of "Primary Ethical Values" found in the Department of Defense's *Joint Ethics Regulation*:

a. Honesty. Being truthful, straightforward and *candid* [emphasis added] are aspects of honesty.

> (1) Truthfulness is required. Deceptions are easily uncovered and usually are. Lies erode credibility and undermine public confidence. Untruths told for seemingly altruistic reasons (to prevent hurt feelings, to promote good will, etc.) are nonetheless resented by the recipients.
>
> (2) Straightforwardness adds frankness to truthfulness and is usually necessary to promote public confidence and to ensure effective, efficient conduct of Federal Government operations. Truths that are presented in such a way as to lead recipients to confusion, misinterpretation or inaccurate conclusions are not productive. Such indirect deceptions can promote ill-will and erode openness, especially when there is an expectation of frankness.
>
> (3) *Candor is the forthright offering of unrequested information. It is necessary in accordance with the gravity of the situation and the nature of the relationships. Candor is required when a reasonable person would feel betrayed if the information were withheld. In some circumstances, silence is dishonest, yet in other circumstances, disclosing information would be wrong and perhaps unlawful*. (emphasis added)

Department of Defense Regulation 5500.07-R, *Joint Ethics Regulation*, 17 November 2011, 118, http://www.dtic.mil/whs/directives/corres/pdf/550007r.pdf.

45. "Preventing a 'Cyber-Pearl Harbor,' " *PBS Newshour*, 16 April 2012, http://www.pbs.org/newshour/bb/science/jan-june12/deterlab_04-16.html.

46. "Expert Warns on Cyberwar Threat," UPI.com, 16 March 2012, http://www.upi.com/Science_News/2012/03/16/Expert-warns-on-cyberwar-threat/UPI-33781331937216/#ixzz1sRYZauJc. The article cities Eugene Kaspersky, chief executive officer and cofounder of Kaspersky Lab, the self-described largest antivirus company in Europe.

47. Quoted in Richard Lardner, "US Needs Top-Level Approval to Launch Cyberattacks," *Salon*, 24 April 2012, http://www.salon.com/2012/04/24/us_needs_top_level_approval_to_launch_cyberattacks/.

48. Jerry Brito and Tate Watkins, "Wired Opinion: Cyberwar Is the New Yellowcake," *Wired*, 14 February 2012, http://www.wired.com/threatlevel/2012/02/yellowcake-and-cyberwar/.

49. Peter Sommer and Ian Brown, *Reducing Systemic Cybersecurity Risk* ([Paris, France:] Organization for Economic Cooperation and Development, 14 January 2011), 5, http://www.oecd.org/dataoecd/57/44/46889922.pdf.

50. Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, no. 192 (March/April 2012): 80, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full.

51. Brito and Watkins, "Wired Opinion."

52. Obama, "Taking the Cyberattack Threat Seriously."

53. "Rule 1.1: Competence," American Bar Association, Center for Professional Responsibility, accessed 25 September 2012, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html.

54. Quoted in Maj Gen Stephen R. Lorenz, "Lorenz on Leadership," *Air and Space Power Journal* 19, no. 2 (Summer 2005): 7–8.

55. Kenneth Anderson, "Sir John Keegan, Ave Atque Vale," *The Volokh Conspiracy* (blog), 3 August 2012, http://www.volokh.com/2012/08/03/sir-john-keegan-ave-atque-vale/.

56. Quoted in ibid.

57. The author has discussed the need for moral courage elsewhere. See, for example, Charles J. Dunlap Jr. "The Ethical Issues of the Practice of National Security Law," *Ohio Northern University Law Review* 38 (2012): 1093–95.

58. Max Hastings, *Warriors: Portraits from the Battlefield* (New York: Vintage Books, 2005), xvii.

**Maj Gen Charles J. Dunlap Jr., USAF, Retired**

General Dunlap (BA, St. Joseph's University; JD, Villanova University School of Law) is the executive director of the Center on Law, Ethics and National Security at Duke University Law School. His 34-year career as judge advocate included tours in both the United Kingdom and Korea, and he deployed for military operations in Africa and the Middle East. A distinguished graduate of the National War College, General Dunlap has recently published such cyber-related pieces as "Perspectives for Cyber Strategists on Law for Cyberwar" (*Strategic Studies Quarterly*, Spring 2011) and "Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors" (*Nebraska Law Review*, 2008). He and Stuart Baker debate cyber law issues in *Patriots Debate: Contemporary Issues in National Security Law*, published in 2012 by the American Bar Association.

**Let us know what you think! Leave a comment!**

During the Vietnam War, the US government placed an extra tax on phone system. members of the Youth International Party ('yippies'; actually a largely fictional pseudo-party or rather a motley mix of performance artists and political pranksters) advocated bypassing the payments (essentially phreaking) as a legitimate means of protest.Â  While Bruce Sterling defines hackers somewhat differently (confusing the hacker/cracker line) and does not focus on the socially motivated cracking, his Hacker Crackdown sheds light to many interesting facts from the early days of computing. Hacktivism. The term was coined by author/culture critic Jason Sack in an article about media artist Shu Lea Cheang, published in InfoNation in 1995. Cyber operations during an armed conflict are covered by the existing law of armed conflict, and should abide by the principles of necessity, distinction, proportionality and unnecessary suffering. Much cyber activity, however, takes place beneath this threshold.Â  As a shortcut, I employ Max Weberâ€™s distinction between the ethics of conviction and the ethics of responsibility, and the importance of the latter in exploring the challenges of political leadership. Put simply, as voters we do not expect our elected leaders to make decisions solely on the basis of their personal beliefs. They should be mindful of a duty to act in accordance with the best interests of the nation â€“ and perhaps with some broader conception of the common good, including global public goods. â€”Jonathan Zittrain, Professor of Law and Professor of Computer Science at Harvard University, and author of The Future of the Internetâ€”And How to Stop It. â€œSinger and Friedman do a highly credible job of documenting the present and likely future risky state of cyber-affairs. This is a clarion call.â€Â  Dening Cyberwar A War by Any Other Name? The Legal Side of Cyber Conict What Might a â€œCyberwarâ€ Actually Look Like?Â  Some liken today to the time before World War I, when the militaries of Europe planned to utilize new technologies like railroads. The problem was that they, and the civilian leaders and publics behind them didnâ€™t understand the technologies or their implications and so made uninformed decisions that inadvertently drove their nations into war.