

The Intersection of Law and Ethics in Cyberwar: Some Reflections

Major General Charles J. Dunlap, Jr., USAF (Ret.)*



Introduction

Few security issues have captured the attention of the public as has the specter of cyberwar. 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, to include the rules applicable to actual cyberwar.²

Parallel to the growing interest in the legal aspects of cyberwar, 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 to an entire conference on the subject being sponsored by the U.S. Naval Academy in the spring of 2012.⁴ Even more recently, an article appeared in *The Atlantic* magazine entitled *Is it Possible to Wage a Just Cyberwar?* Which discussed several intriguing issues⁵

The purpose of this short essay is to reflect upon a few issues that illustrate how legal and ethical issues intersect in the cyber realm. Such an intersection should not be especially surprising., Historian Geoffrey Best insists, “[I]t 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” Best says “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 21st 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 Journal⁷ US Navy Lieutenant Gabriel Bradley points out that “The law of armed conflict sets minimum standards” and 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.⁸ And he is certainly right when he quotes Christopher Coker’s observation that “laws can reaffirm the warrior ethos; they cannot replace it.”⁹

Of course, even determining the baseline – that is, the law - is not always easy in 21st century operations generally, but especially with regard to cyber activities. Among the many reasons for this is that fact that most of the law of armed conflict (LOAC) was designed to address conflicts waged mainly with kinetic weaponry. Nevertheless, in this writer’s view, existing law has ready applicability to cyber operations. This perhaps brings us to the first issue regarding the intersection of law, ethics, and cyber operations, that is, the notion sometimes heard that cyberspace is such a new domain that no existing law could – or even *should* – apply to military operations in it.

This is simply untrue. Most LOAC 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.¹⁰ It did produce a useful volume, but it is a relatively thin one as it was found that there was a comparatively modest amount of law that could be said to be wholly unique to the air and space domains. Much the same can be said about the cyber domain, to include ethical considerations.¹¹

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 is a good example. Although the phrase “act of war” is a political term, not a legal axiom, there *are* phrases like

“use of force” and “armed attack” that *do* have legal meaning, and could relate to a *casus belli* in terms of a forceful response.¹²

The interpretation of such expressions in the cyber realm is, in fact, resolvable under the law, if – *and, really, only “if”* – technology can provide adequate data as to, for example, the actual harm caused by the supposed “attack,” as well as sufficient information as to who actually did it. Of course, the absence of attribution data – which is technically so challenging to obtain in the cyber realm – can be a definitive legal and ethical bar to a forceful response. This may be 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 as to who might be responsible before launching a counter of some kind.

The fact that technologically-speaking, determining attribution is a daunting task is *not* a problem for the lawyers or, for that matter, ethicists, but something for technologists to solve. It is interesting therefore that the authors of The Atlantic article referenced previously argue, in relation to the alleged use of a cyber-weapon (Stuxnet) against Iran’s nuclear 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 as to whether there would necessarily be a legal or moral basis for Iran to counterattack as a result of the alleged Stuxnet operation,¹⁴ it is of further interest that the authors of the Atlantic piece say that “to make attribution work, we need international agreements.”¹⁵ 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.”¹⁶

While most experts would probably say that current law does not require such facilitation of cyber attribution,¹⁷ the authors of the Atlantic article nevertheless argue for “better on international network monitoring to trace sources of attacks” and seem to believe that “[e]conomic incentives, such as the threat of trade sanctions, can make such agreements desirable.”¹⁸ Again, there is much about these proposals with which one might disagree, but the authors should be commended for at least beginning the dialogue as to how one of the most perplexing legal and moral questions of cyberwar might be addressed.

As with attribution, technological issues – not the law, *per se* – are also the most challenging aspect of targeting of cyber-weaponry. The cardinal legal and ethical principles of distinction and proportionality¹⁹ require technical data that will inform decision-makers as to who might be affected by a particular

technique, and to what extent. Again, that this may be technically hard-to-do is not legal or ethical problem, but a scientific one. Indeed, it can be said that one of the most needed capabilities in the world of cyber operations is the ability to model effects with dependable accuracy, so as to provide decision-makers - not to mention lawyers and ethicists - with the kind of information that is patently essential for making reasoned judgments about employing a cyber-methodology.

Do Legal and Ethical Values Unduly Encumber Cyberwarriors?

Over above questions about the application of legal regimes and ethical mores to particular cyber scenario, is the broader question as to whether any restraints should apply at all. More specifically, some believe that efforts to apply the law will so encumber the U.S.'s cyber efforts that the nation's security is put at risk. This rather surprising question is at the heart of a serious debate in which Stewart Baker and this writer engaged under the auspices of the American Bar Association.²⁰

Just by way of context, Mr. Baker is a highly-respected lawyer with the prestigious Washington law firm of Steptoe & Johnson, and had previously served in government as the general counsel of the National Security Agency, as well as Assistant Secretary for Policy in the U.S. Department of Homeland Security. He begins his polemic in 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.²¹

Mr. Baker further claims that any attempts to "impose limits on cyberwar" and are, in his opinion, "doomed."²² Among the most troubling aspects of his argument is really an ethical one of the first order in that he points to the devastation caused by World War II air warfare and references former British Prime minister Stanley Baldwin 1930s' claim that in air warfare "the only defense is in offence, which means that you have got to kill more women and children more quickly than the enemy if you want to save yourselves."²³

Mr. Baker then goes on to seem to *endorse* 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.*"²⁴ Only after constructing a cyberwar strategy so framed would Mr. Baker consider it appropriate to "ask the lawyers" for their "thoughts."²⁵

It is beyond the scope of this essay to fully reprise my response (though the title - “Lawless Cyberwar? Not If You Want to Win.” – may be indicative of its content), but suffice to say that it is vitally important in cyberwar (as with any military operation) to ground the “limits” whenever possible not just in the law or ethics, *per se*, but also in pragmatic, warfighting rationale. In the case of cyber, this is not particularly difficult to do, especially if the actual warfighters are not perceiving 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,” Air Force General Robert Kehler, the commander of U.S Strategic Command whose subordinate organization U.S. Cyber Command is the leading proponent of military cyber planning and operations, seems to disagree. In November of 2011 he declared that he did “not believe that we need new explicit authorities to conduct offensive operations of any kind.”²⁶ Furthermore, he said that that he did “not think there is any issue about authority to conduct [cyber] operations.”²⁷ In short, the *warfighters* 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.²⁸ Nations vital to this effort, to include 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 Riesman and Chris T. Antoniou point out in their 1994 book, *The Laws of War*:

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.*²⁹

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

Civilian Cyberwarriors

It almost goes without saying that enormous cyber expertise lies in the civilian community, and it is essential that the armed forces have access to it. That

said, the extent of that access, and precisely what that access does – or *should* – mean, is properly the subject of legal and ethical scrutiny.

The basics are not hard. In order 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.³⁰ This has often been misunderstood 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 they fall into the hands of the enemy, they might be properly subject to the enemy’s domestic criminal law for acts which, if done by a member of the opposing military, would be privileged from prosecution. What is more is that under the law of war, civilians are properly targetable – kinetically or cyberly – when directly participating in hostilities. In the cyber context, it should be understood that even the International Committee of the Red Cross explicitly uses as examples of direct participation acts that are the kind of things 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.”³¹

What does all this mean from an ethical perspective? For one thing it is essential that civilians understand the potential consequences, especially when the civilian is away from the work site, such as at home with his or her family. Although there is debate in the international community about what it takes for a civilian to be targetable on the same basis as a member of the armed forces, the International Committee of the Red Cross agrees that those civilians who assume a “continuous combat function” (as opposed to merely “participating in hostilities in a spontaneous, sporadic or unorganized way”) can be targeted on a similar basis as members of the armed forces.³²

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 the individual presents an imminent threat or is otherwise doing a military function. This means, for example, that a civilian cyber-warrior regularly engaged in computer network attack operations might be legitimately attacked by a lawful belligerent (not terrorists) in his home in a Washington suburb. And not just with cyber weapons either; any lawful weapon can be used if otherwise compliant 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, provided the incidental death and injury to innocent civilians – like the cyber-warrior’s own family – that might occur in the attack was not “excessive in relation to the

concrete and direct military advantage anticipated” (that “military advantage” being, of course, the elimination or neutralization of the cyber expert).³³

Thus, the ethical issue for cyber warriors may be the extent to which it is appropriate to 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, however, to ask civilians to do so, and yet 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.

It is impossible to know 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 kind 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 kind of 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 have 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. A very recent article by one pundit entitled “With its deadly drones, the US is fighting a coward's war” is an example of the kind of nasty rhetoric that is used.³⁴ Though such aspersions have not yet been cast upon cyber-warriors, it seem like it is only a matter of time before they will be subject to the same kind of insult to their professional ethic.

How did all this start? It might be traceable to remarks a few years ago by Dr. David Kilcullen, a retired Australian army lieutenant colonel who has become one the foremost advocates of ground-centric, manpower-intensive form of counterinsurgency that found expression in the Army and Marine Corps Counterinsurgency Manual, (FM 3-24) published in 2006.³⁵ It is important to understand that the Manual is rather hostile to air operations in general, and devotes 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.”³⁶ “In the Pashtun tribal culture of honor and revenge,” he said, “face-to-face combat is seen as brave; shooting people with missiles from 20,000 feet is not.”³⁷ According to Kilcullen, “using robots from the air ... looks both cowardly and weak.”³⁸ Quite obviously, his thesis might rather easily be applied 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 use remotely detonated IEDs to kill US forces from the safety of distance, but also employ children to plant them. Would that not make them, by their own “culture of honor” standards, “cowardly and weak”? Regardless, this entire discussion, however demoralizing and inaccurate, is – in terms of actual warfighting - rather immaterial. The “object of war”, as General 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 21st century warfare, and perhaps ever. Native Americans, for example, waged war with extraordinary courage. 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.”³⁹ Of course, there is nothing wrong with being “a modern technologically advanced nation” with “ultimate victory as its goal” so long as those technological advances are used in a legally and ethically appropriate way.

The reality is that not only is there nothing unethical about waging war from afar, there is actually nothing especially unusual about it. Since practically the beginning of time, warriors have sought to engage their adversaries in ways that denied their opponents 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.⁴⁰

Still, there is something about computerized warfare that draws special scorn from some, however wrongly and unfairly. For example, Phillip Altson, a New

York University law professor was commissioned by the United Nations as a “Special Rapporteur” to write a report on targeted killings. The document he produced also included his opinions about drone operators.⁴¹ In it he charged that because drone operations can be conducted “entirely through computer screens and remote audio feed, there is a risk, “ he says, “of developing a ‘PlayStation’ mentality to killing.”⁴²

‘PlayStation’ mentality to killing? That even the suggestion of such an insulting lack of professionalism would find itself into an official UN report is, itself, disquieting. The principle evidence for Professor Alston’s finding appears to be his own speculations about the mindset of those doing a task he has never himself performed. The actual evidence, however, points in a very different direction than the one Alston suggests, and 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.”⁴³ He concluded that operators suffered “significantly increased fatigue, emotional exhaustion and burnout.”⁴⁴ 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.”⁴⁵ While debate still roils,⁴⁶ it demonstrates how quickly some critics deride the professionalism of principled people doing what their nation asks them to do. Quite obviously, the comparison with the cyber operations is not quite the same, but – 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 the operations demand is very high, and the psychological burdens those who conduct them are likely very great.

Another aspect of the drone campaigns has emerged which might find analogy in the ethics and professionalism that cyber operators must display. It is expressed an April 29 2012 article in *Rolling Stone* by controversial writer Michael). In it Hastings claims:

[T]he 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.⁴⁷

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.” This writer’s experience has been that 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 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, and these conditions may give rise to another ethical responsibility, and that is to render frank, holistic advice. It is not impossible 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, it is imperative that it be done so with the same care as would be the case with any more traditional military operation. To underline, this may call upon someone to go beyond the norm, just to make sure that all the right considerations are taken into account – to include ethical and legal ones – so that the best decisions are made.

Fortunately, for lawyers anyway, the American Bar Association 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.”⁴⁸ 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.”⁴⁹ In truth, this is the right guidance not just for lawyers, but – really – for *all* military and civilian professionals engaged in cyber operations because their success depends upon a wide range of factors, and it is incumbent upon all involved to work together to ensure they are surfaced and considered.

The rule mentions candor. Again, this is not something simply for attorneys, but is a fundamental ethical virtue for all defense professionals.⁵⁰ Among other things, it is an important trait to keep 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.”⁵¹ Likewise, a “leading European cybersecurity expert says international action is needed to prevent a catastrophic cyberwar and cyberterrorism.”⁵²

Not all agree, however. In April of 2012 Rear Admiral Samuel Cox, director of intelligence at the U.S. Cyber Command, was reported as having “played down the prospect that an enemy of the U.S. could disable the nation's electric power grid or shut down the Internet, saying those systems are designed to withstand severe cyberattacks.”⁵³ More stinging is a February 2012 Wired, article in which researchers Jerry Brito and Tate Watkins debunk much of the histrionic talk about the threat of cyberwar.⁵⁴ According to Brito and Watkins, “evidence to sustain such dire warnings [about cyberwar] is conspicuously absent.”⁵⁵

Consistent with Brito and Watkins’ conclusions is a 2011 report by the Organization for Economic Cooperation and Development.⁵⁶ While asserting that governments “need to make detailed preparations to withstand and recover from a wide range of unwanted cyber events, both accidental and deliberate,”⁵⁷ the authors of that study nevertheless conclude “that very few single cyber-related events have the capacity to cause a global shock.”⁵⁸ Writing in Foreign Policy analyst Thomas Rid contends that cyberwar is “still more hype than hazard.”⁵⁹

All of this raises concerns because Brito and Watkins say that “[i]n many respects, rhetoric about cyber catastrophe resemble the threat inflation we saw in the run-up to the Iraq War.”⁶⁰ They also point out that “[c]ybersecurity 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.”⁶¹ Although they stop short of actually accusing anyone of pushing cyberwar fears 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.”⁶²

The scope and immediacy of the threat is 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, in considering the run-up to the war with Iraq in 2003 it is clear what can happen when a threat is misconstrued, which may be why they entitle their polemic “Cyberwar Is the New Yellowcake.” In short, candor – and tempered rhetoric *if appropriate* – are critical qualities for cyberwarriors. 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.⁶³

The Virtue of Competence

Finally, one of the key ethical responsibilities of cyber-warriors is competence. Again, the American Bar Association Model Rules of Professional Conduct provides guidance that all cyber professionals may want to consider analogizing to their responsibilities. Rule 1.1 of that Code says “[c]ompetent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”⁶⁴ For those concerned about the legal and ethical aspects of cyberwar, the ethic mandate for competence goes well beyond knowledge and understanding of law and/or ethics, *per se*.

There is no doubt that there are many aspects of cyber operations that are extraordinarily complex. Thus, it is incumbent upon legal - and other advisors - to become as familiar as possible with the cyber client’s “business,” to include its technical aspects. Not only will a working knowledge of the technology help advisors to understand the facts sufficiently enough to apply legal and ethical principles to them; it will also give such advisors 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, as failing to do so may lead to a lifetime of regret. Winston Churchill once observed:

To every man there comes in his lifetime that special moment when he is figuratively tapped on the shoulder and offered a 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 the work which would be his finest hour.⁶⁵

Concluding Observations

This essay has sought to illustrate just a few of the examples of how law and ethics might intersect. This effort may invite the question: which of these imperatives will best operate to impose the limits on cyberwar 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. Professor Anderson maintains:

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.⁶⁶

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 the 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."

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 mindset it implies, is indispensable. Yet the discussion cannot end there, because merely having developing the character to come to know the right answer is not enough, as 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. This is especially so as norms are developed for the conduct of cyber operations. Doing the right thing, particularly in circumstances of extreme urgency where there is 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."⁶⁷ "Moral courage," he insists "is rare."⁶⁸ Yet it is exactly this kind of rare that cyber warriors most need to exhibit. The law can provide an architecture, but it is only when honor and moral courage intersect can we truly be assured that ethical principles worth defending are actually preserved.

Notes

1. Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL STREET JOURNAL, Jul. 19, 2012,

<http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html>.

2. For example, the International Law Division of the U.S. Naval War College held a conference devoted to the legal aspects of cyberwar in June of 2012,

<http://www.usnwc.edu/ILDJune2012>.

-
3. See e.g., Randall R. Dipert, *The Ethics of Cyberwar*, J. OF MIL. ETHICS, Vol. 9, No. 4 (2010), at 384, 385 ([t]here are no informed, open, public or political discussions of what ethical and wise policy for the use of such [cyber] weapons would be.”).
 4. U.S. Naval Academy Stockdale Center for Ethical Leadership, *Warfare in a New Domain: The Ethics of Military Cyber Operations*, April 26-27, 2012 <http://www.usna.edu/ethics/publications/mccain2012.php>. Much of this essay is drawn from a presentation the author made at that conferece.
 5. Patrick Lin, Fritz Allhoff, and Neil Rowe, *Is it Possible to Wage a Just Cyberwar?*, THE ATLANTIC, Jun 5, 2012, <http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/>
 6. Geoffrey Best, *Law and War Since 1945*, 1994, p. 289
 7. Lt Gabriel Bradley, Honor, Not Law, ARMED FORCES JOURNAL, Mar. 2012, *available at* <http://www.armedforcesjournal.com/2012/03/9563756> (last visited Apr. 23, 2012).
 8. *Id.*
 9. *Id.*
 10. Program on Humanitarian Policy and Conflict Research, Manual on International Law Applicable to Air and Missile Warfare (2009), <http://ihlresearch.org/amw/HPCR%20Manual.pdf> [hereinafter AMW Manual].
 11. See e.g., Roger Crisp, *Cyberwar: No New Ethics Needed*, PRACTICAL ETHICS (blog), Jun. 19, 2012, <http://blog.practicaethics.ox.ac.uk/2012/06/cyberwarfare-no-new-ethics-needed/>.
 12. These terms are used, for example, in Article 2 and Article 52, respectively of the Charter of the United Nations, <http://treaties.un.org/doc/Publication/CTC/uncharter.pdf>.
 13. See note 5, *supra*.
 14. If, for example, a factual case can be made for proper the application of the doctrine of anticipatory self-defense by a nation-state, there would be not legal or moral basis for Iran 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 (2011).
 15. *Id.*
 16. *Id.*
 17. See e.g., Crisp, *supra* note 11.
 18. See note 5, *supra*.
 19. Harold Koh, the legal advisor the U.S. 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.
 - Harold Koh, *The Obama Administration and International Law*, speech, American Society of International Law, 25 March 2010, <http://www.state.gov/s/1/releases/remarks/139119.htm>.
 20. Stewart A. Baker and Charles J. Dunlap Jr., *What Is the Role of Lawyers in Cyberwarfare?*, ABA JOURNAL, May 1, 2012, http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/.
 21. *Id.*
 22. *Id.*
 23. *Id.*
 24. *Id.* (italics added).
 25. *Id.*
 26. Jim Wolf, “U.S. Military better prepared for cyber warfare: general,” *Reuters* (November 16, 2011)

<http://www.reuters.com/article/2011/11/17/us-usa-cyber-military-idUSTRE7AG03U20111117?feedType=RSS&feedName=everything&virtualBrandChannel=11563>

27. *Id.*

28. See e.g., U.S. Dep't of Defense, *Department of Defense Strategy for Operating in Cyberspace*, 2011, at 9, <http://www.defense.gov/news/d20110714cyber.pdf> ("Cyberspace is a network of networks that includes thousands of ISPs across the globe; no single state or organization can maintain effective cyber defenses on its own.").

29. W. Michael Riesman & Chris T. Antoniou, *THE LAWS OF WAR* (1994), at xxiv.

30. See generally, Gary D. Solis, *THE LAW OF WAR* (201), at 41-42.

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

32. *Id.*

33. See Koh, *supra*, note 19.

34. George Monbiot, *With its deadly drones, the US is fighting a coward's war*, *The Guardian* (U.K.), Jan. 30, 2012, <http://www.guardian.co.uk/commentisfree/2012/jan/30/deadly-drones-us-cowards-war>

35. U.S. Dep't of the Army, Field Manual 3-24, 2006,

<http://www.fas.org/irp/doddir/army/fm3-24.pdf>.

36. Doyle McManus, *U.S. drone attacks in Pakistan 'backfiring,' Congress told*, *LOS ANGELES TIMES*, May 3, 2009, <http://articles.latimes.com/2009/may/03/opinion/oe-mcmanus3>

37. *Id.*

38. *Id.*

39. Anthony R. McGinnis, *When Courage Was Not Enough: Plains Indians at War with the United States Army*, *J. OF MIL. HISTORY*, April 2012, at 473.

40. Charles J. Dunlap, Jr., *Does Lawfare Need an Apologia, Does Lawfare Need an Apologia?* 43 *CASE WES. RES. J. INT'L L.* (2010), at 121.

41. Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Execution: Study on Targeted Killings, delivered to the Human Rights Council*, U.N. Doc. A/HRC/14/24/Add.6 (May 28, 2010), available at

<http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf> (last visited Sept. 2, 2010).

42. *Id.*, at 25.

43. Marc Pitzke, *Interview with Defense Expert P.W. Singer*, *SPIEGEL ONLINE INTERNATIONAL*, Mar. 12, 2010, <http://www.spiegel.de/international/world/0,1518,682852,00.html>.

44. *Id.*

45. Jeff Schogol and Markeshia Ricks, *Demand grows for UAV pilots, sensor operators*, *Air Force Times*, April 21, 2012,

46. See e.g., Kenneth Anderson, *Laurie Blank on Mark Mazzetti's 'The Drone Zone' – Last in Series from Lewis, Dunlap, Rona, Corn, and Anderson*, *LAWFARE*, Jul. 21, 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/>.

47. Michael Hastings, *The Rise of the Killer Drones: How America Goes to War in Secret*, *ROLLING STONE*, April 16, 2012, <http://www.rollingstone.com/politics/news/the-rise-of-the-killer-drones-how-america-goes-to-war-in-secret-20120416#ixzz22VDkfr00>.

48. ABA Model Rule of Professional Conduct 2.1,

http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_2_1_advisor.html.

49. *Id.*

50. Compare the following from the listing of "Primary Ethical Values" found in the Department of Defense's Joint Ethics Regulation (*italics added*):

a. Honesty. Being truthful, straightforward and *candid* 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.*

U.S. Dep't of Defense Regulation 5500.07-R, *Joint Ethics Regulation*, Nov. 17, 2011, para 12-401a, <http://www.dtic.mil/whs/directives/corres/pdf/550007r.pdf>.

51. *Preventing a 'Cyber-Pearl Harbor'*, PBS NEWSHOUR, Apr. 16, 2012, http://www.pbs.org/newshour/bb/science/jan-june12/deterlab_04-16.html.
52. *Expert warns on cyberwar threat*, UPI.COM, Mar. 16, 2012, http://www.upi.com/Science_News/2012/03/16/Expert-warns-on-cyberwar-threat/UPI-33781331937216/#ixzz1sRYZauJc (citing Eugene Kaspersky, chief executive officer co-founder of Kaspersky Lab, which says it is the largest antivirus company in Europe).
53. Richard Lardner, *US Needs Top-level Approval to Launch Cyberattacks*, SALON.COM, April 24, 2012, http://www.salon.com/2012/04/24/us_needs_top_level_approval_to_launch_cyberattacks/
54. Jerry Brito and Tate Watkins, *Cyberwar is the New Yellowcake*, WIRED, Feb. 14, 2012, available at <http://www.wired.com/threatlevel/2012/02/yellowcake-and-cyberwar/>.
55. *Id.*
56. Peter Sommer and Ian Brown, *Reducing Systemic Cybersecurity Risk*, Organization for Economic Cooperation and Development, Jan 14, 2011, at 5, <http://www.oecd.org/dataoecd/57/44/46889922.pdf>.
57. *Id.*
58. *Id.*
59. Thomas Rid, *Think Again: Cyberwar*, FOREIGN POLICY, Mar/Apr 2012, at 80, <http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full>.
60. Brito and Watkins, *supra* note 54.
61. *Id.*
62. *Id.*
63. *See* note 1, *supra*.
64. ABA Model Rule of Professional Conduct 1.1, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html.
65. As quoted by Maj Gen Stephen R. Lorenz, *Lorenz on Leadership*, AIR & SPACE POWER JOURNAL, Summer 2005, <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/sum05/lorenz.html>

-
66. Kenneth Anderson, *Sir John Keegan, Ave Atque Vale*, LAWFARE, Aug. 3, 2012, <http://www.lawfareblog.com/2012/08/sir-john-keegan-ave-atque-vale/>.
67. Max Hastings, *WARRIORS: PORTRAITS FROM THE BATTLEFIELD*, (2005), at xvii.
68. *Id.*

Contributor



Major General, USAF (Ret.), Executive Director, Center on Law, Ethics, and National Security, Duke University School of Law.