Journal of Military Ethics,
Vol. 9, No. 4, 411–423, 2010

Routledge
Taylor & Francis Group

'Cyberation' and Just War Doctrine: A Response to Randall Dipert

COLONEL JAMES COOK
US Air Force Academy, Colorado Springs, USA

ABSTRACT *In this essay, I reject the suggestion that the just war tradition (JWT) does not apply to cyberwarfare (CW). That is not to say CW will not include grey areas defying easy analysis in terms of the JWT. But analogously ambiguous cases have long existed in warfare without undercutting the JWT's broad relevance. That some aspects of CW are unique is likewise no threat to the JWT's applicability. The special character of CW remains similar enough to other kinds of warfare; the distinctions are more differences of degree than of kind.*

KEY WORDS: conventional war, conventional attack, cyberation, cyber attack, cyber ethics, cyber tactics, cyberspace, cyber strategy, cyber war, cyber weapons, just-war tradition, just-war theory, malware, military ethics, non-conventional attack, non-conventional war, non-conventional weapon, Stuxnet, unconventional attack, unconventional war, unconventional weapon, virus, war, worm

Does the just-war tradition (JWT) apply to cyberwarfare (CW)? I attempt to answer that question in several ways: in the first section below by rejecting the peculiar logic that says the JWT doesn't apply because CW is not really war; then by offering a positive case for the JWT's relevance to CW; and third, by showing that scenarios dubbed "hard cases" involving responses to conventional and cyber attacks conform nicely to long-established JW principles. In the fourth and final section below I suggest ways in which CW might pose special challenges to JW analysis. I conclude that CW's moral and logical ambiguities, though somewhat new, present differences of degree rather than kind; analogously ambiguous cases have long existed in warfare without undercutting the JWT's broad relevance.

1. Rejecting the stacked rhetorical deck

Consider the claim that cyberspace as a medium and CW as a set of means, tactics, and strategies are so novel as to defy application of the JWT. Another way of expressing the same claim: analogies linking cyberspace and CW to

Correspondence Address: James Cook, Department of Philosophy, 2354 Fairchild Drive, USAF Academy, Colorado Springs, CO 80840, USA. E-mail: james.cook@usafa.edu

1502-7570 Print/1502-7589 Online/10/040411–13 © 2010 Taylor & Francis
http://www.informaworld.com
DOI: 10.1080/15027570.2010.536406

predecessor military media, means, tactics, and strategies are often too weak to be of use to just-war thinkers. We might call this the "claim of disanalogy."

We should evaluate this view in light of two working assumptions:

(1) Much of the JWT—the in bello guidelines as well as the ad bellum just cause, proportionality, last resort, and reasonable hope principles—passes judgment on the *effects* rather than the means or media of aggression. Before the JWT can offer its most useful guidance in any given case, those effects must meet three conditions: (a) they must be known or strongly predicted; (b) they must be linked to known intentional actors; and finally, (c) they must manifest as destruction or imminent destruction—of lives, property, governments, cultures, etc.

(2) Many longstanding strategies, tactics, means, and media of warfare have defied easy application of the JWT because of uncertainty as to their probable effects. Similarly, we can't always identify the agents of violence or their intentions. The Unabomber demonstrated that regrettable fact, as did the corpse on whom the FBI finally pinned the 2001 anthrax attacks. Had either enjoyed a foreign government's or domestic terror group's backing, they might have wreaked greater havoc and might still be operating today. As for foreign-backed terrorists, one need look no further than this year's Times Square Bomber to see how difficult attribution might be. When Faisal Shahzad bought the SUV that was to carry and become part of his bomb, he paid cash yet gave the seller his actual phone number. Even so, he was already seated on a Dubai-bound flight at Kennedy International when he was arrested. One wonders what might have happened if things had worked out even a little differently—if Shahzad had guarded his anonymity when buying the SUV, if the bomb had exploded as planned, and so on.[1] Yet even though the so-called attribution problem can be vexing in cases of non-cyberattack, the JWT continues to offer useful guidance.

Dr. Dipert[2] seems to believe the claim of disanalogy. But he arrives at his opinion after stacking the rhetorical deck. He insists that in contrast to the "lethality and massive destructiveness of war .... cyberwarfare often won't be like that–although it *could be* both lethal and physically destructive" (Dipert 2010: 386). Now if one says up front that CW *often* won't be as destructive as earlier sorts of "war," then it's no surprise if the JWT *often* won't easily apply. How could it if the very definition of CW undercuts the first assumption above? Similarly, in several passages Dr. Dipert indicates that the means, media, tactics, and strategy of CW as he defines it will obscure effects, actors, and intentions. Fair enough. But based on the second assumption above it would then follow—in an uninteresting because nearly tautological way—that the JWT often won't apply in those cases.

I find the position Dr. Dipert attributes to Jeff McMahan much easier to stomach.[3] That position—that many a cyberattack will be a clear-cut casus belli—conforms to my intuitions. I find it commonsensical that the JWT, concerned primarily as it is with effects and intentions rather than means and medium, will often have something interesting to say about CW, a type of warfare than can cause vast, intentional harm.

Dr. Dipert himself undercuts the claim of disanalogy by indicating ways that cyber activities can do grave damage. For instance, he notes that "much of our economic and defense informatics infrastructure is vulnerable to [cyber] attack" (Dipert 2010: 406). There is no reason why such damage could not result from a *military* cyberattack, one we could analyze through the lens of the JWT.

Despite stacking the rhetorical deck, however, Dr. Dipert doesn't much dilute what seems to me his paper's more interesting agenda—offering a lucid primer on CW. Dr. Dipert's discussion provides a taxonomy of cyber activity that suggests (among other things) what should be excluded from the definition of "cyberwarfare" as "war" in the sense meant by the JWT. There are, however, a few parts of his presentation that suffer from the stacked deck's influence. I'll consider those in section 3. below after first considering why and how the JWT applies to CW.

2. The JWT does in fact apply to cyberwarfare: a heuristic case by analogy

If it's true that Dr. Dipert has stacked the rhetorical deck—that he has defined cyberwarfare such that the JWT often cannot apply before he "shows" that it in fact often fails to apply—it still remains to make a positive case that the JWT can inform and evaluate CW.

We grow up accustomed to the idea that information instigates kinetic effects. It's not just that we spur others to action and they in turn actuate us by imparting information, e.g., in the form of words. The baby cries, the mother soothes, the baby falls asleep; the teenager cries, the mother says curfew's relaxed but just for tonight, the teenager disappears 'til dawn; and so on. Our earliest education in the world's ways underscores what experience has already taught us. Fairy tales often feature magic words that overcome otherwise insuperable obstacles: Speak to Rapunzel in the right way and you can get into the tower; say "Rumpelstilzchen" and you get to keep the child that a nasty gnome would otherwise take away. It's no different in military operations: information—transmitted or intercepted information, for example—matters in warfare. We know it mattered to the outcome of the American Revolution that colonials could track British troop and supply movements and communicate their intelligence through command and control systems. Had the old North Church been a modern C2 node, the proper signal—"one if by land, two if by sea"—might never have been transmitted or received via secure BostoNet. British cyberattack troops might have rendered the system unusable through a virus or worm or a denial of service attack. Years later the British might even have co-opted Longfellow's word processor and destroyed "Paul Revere's Ride." We know the allied cryptanalyst effort managed to break the code known as JN-25 thanks in large part to the volume of Japanese message traffic intercepted. Breaking the code in turn allowed the US fleet to engage the Japanese at Midway and, arguably, change the war's course in the space of a few hours. Nowadays cyber activity can send legitimate go codes as well as obstruct, intercept, and fabricate them. Done in a certain way under certain circumstances, those activities could become a means of CW, causing or enabling immense destruction.

Consider an admittedly flawed analogy to cyberspace and the goings-on there: that medium and its cyber-things and –activities are at least a little like the air-space continuum and the aviation that goes on it. In both cyber activity and aviation lots of stuff goes to and fro. Some of that to'ing and fro'ing is patently military; much of it isn't; some of it isn't until it is (think 9/11); and enough of it's so ambiguous that one couldn't craft an accurate Venn diagram, at least not one that wasn't obsolete as soon as it was complete.

Besides aviation, one might draw many similar analogies to *cyberation*[4]—e.g., maritime and even postal ones (recall the 2001 US anthrax attacks and the plethora of letter bombs sent to Israeli targets in the 1970s). All such analogies would share obvious features. First, there's the distinction among realms, cyberspace vs. the rest of the world and the air-space continuum versus the earth and sea. Second, there's movement between and within the realms. Finally, the interfaces are conceptually distinct even if they're somewhat vague in practice, as when a helicopter lowers its payload to earth or a C130 shoves a pallet out the door at low altitude rather than landing.

So does the JWT apply to aviation or navigation? We might justifiably think that anyone who asked such a question had failed to express herself clearly. She must have meant to ask a related question, such as *how* the JWT applies to aviation, or *what* aspects of aviation might be used for war and therefore belong in the JWT's bailiwick. *Of course* the JWT will help us judge many activities under the rubrics of aviation and navigation. That would have been harder to say of aviation before observation balloons and other aircraft had become part of the battlefield's mise en scène. But now it's so obvious as to require no defense. Why shouldn't we consider cyberation in the same way? Why shouldn't we say that just as military aviation is a subset of aviation, so military cyberation is a subset of cyberation?

A weak—and false—answer to those questions is that military aviation is somehow different in kind from anything that can happen in cyberspace. Air- and spacecraft are physical things that can cause physical effects. Not so cyber entities and what they can do, or so someone might claim.

But this alleged difference is misleading. Military aircraft can attack other aircraft, military and civilian, as well as targets on the land and at sea. In more abstract terms, military aviation can directly or indirectly destroy targets in its air-space domain and reach across its interface with the land and sea domains to destroy targets there. If one were to apply the language of CW to aviation, one might say that military aviation falls under the JWT because it can cause great harm across interfaces, and that harm is kinetic: people die and things break.

CW is no different from military aviation in this regard. Its interfaces are not just conceptual; they're real, physical things. However, we should think of this conceptual-physical duality as being less Cartesian than Heideggerian. We should avoid analogies of the sort that suggest mind is to body as cyber is to non-cyber. We should avoid them not only because cyber entities such as processes are physical. More importantly, those who labor across the interface of cyberspace are not working in any important sense differently than aviators or navigators. Heidegger points out that I (as *Dasein*) am inevitably in-the-world, properly conceived, and not somehow less or more so depending on the task at hand; what is "closest" or "next" to me is not first and foremost explicable as a function of Cartesian dualism but rather in terms of what I'm attending to. Further, theoretical vivisections of the world are metaphysically secondary, not primary; when I'm working "in" cyber I'm as much in touch with reality as a plumber. (I'm hesitant to enlist thinkers so cursorily and superficially, but perhaps it's pardonable to indicate if only by allusion that the cyber-versus-non-cyber distinction is often overdrawn.)

Although the analogies are imperfect, the JWT must attend to cyberation for the same reasons it applies to aviation: there are aspects of cyberation that can be used as military means to cause great harm. Consider this quotation from a military cyberation veteran, Jason Healey, speaking about the late 1990s predecessor to the recently-established US Cyber Command: "'It was supposed to be a war fighter unit, not a geek unit.'"[5] Without going into specifics, Healey explains why: cyberation can kill people and destroy infrastructure—within cyberspace and outside it—just as military aviation can. That cyberation is removed from aspects beyond its interfaces in a somewhat unique way doesn't matter all that much. Foreign military aviation can kill a US citizen walking down Main Street by targeting her with a kinetic weapon such as a missile—a direct kill. Or it can kill her by ensuring she has no food, power, medical care, etc., or by kinetically destroying her means of obtaining those things. Obviously cyberation can cause similar deprivation and destruction. Although a bit or a byte can't kinetically hit her on the head, cyberation can cause the missile to launch even though its keepers didn't want that to happen or kill her by diverting a missile intended for another target.

With that in mind, it's not particularly instructive to claim that much of cyberation doesn't fall under the JWT. The same is true of much of aviation and navigation—e.g., what we call "civil aviation." The interesting question is, What cyber activities can fall under JWT? The easy answer is that military cyberation is changing too fast for us to do much more than guess. We know some cyber activities that can kill and destroy; we know how to stop a subset of those things; but we probably don't know but a small fraction of the offensive and defensive possibilities. Breakthroughs such as supercruising might be used in any number of ways in aviation, civilian as well as military. The same is true of advances such as quantum computing: it's too soon to know how they'll apply to cyberation in general or to CW in particular. We do know that some kinds of cyberation can destroy just as some kinds of aviation can. That means CW can meet the test of assumption 1 in the previous section.

What else might motivate the claim that CW isn't real war and that therefore the JWT doesn't apply? One such contention is that so-called cyberweapons are merely the ho-hum spinoff of quotidian cyberstuff such as the office or home PC—at most tools of mischief, that is, rather than weapons of war. We should be skeptical of claims to the effect that "there are no exotic components to cyber weapons" (Dipert 2010: 385). True, cyber weapons need not be exotic. Some are clumsy things that can be conceived and launched by individuals. But consider: homegrown, part-time hackers working alone can do enough damage with worms, viruses, and the like to drive an enormous PC security industry. Norton and McAfee represent an iceberg's tip; the cyber security infrastructure is huge because the threats are extremely varied.[6] Now imagine what large teams with significant budgets and state backing could do. We should expect that some cyber weapons will be very exotic.

Even if some cyber tools are common, we should not assume that therefore they cannot become immensely destructive weapons. Fertilizer components, gasoline, cars, trucks, and cell phones are the stuff of everyday life. They're also useful in building improvised explosive devices (IEDs) and their suicide vehicle-borne variants (SVBIEDs), which have killed more coalition troops in Iraq and Afghanistan than any other single weapon system.

3. Rethinking the "hard cases" and the extent to which received theories apply

With the positive case for the relevance of the JWT to CW in mind, we can consider the ethics of a range of scenarios.

Dr. Dipert poses and answers five "moral questions of CW" (Dipert 2010: 392). While he believes there is prima facie moral justification for cyberattack in response to conventional or cyberattack, he finds two other scenarios problematic. The question of whether a nation may respond conventionally to a cyberattack he considers to be "a very hard case indeed." (Dipert 2010: 394) The other question he finds especially vexing is whether it's ever permissible to launch a first-strike cyberattack "with UN sanction, preemptively, preventively, or for some other reason" (Dipert 2010: 392).

If it's true that the JWT applies to CW, and if it's further true that the JWT concerns itself primarily with effects rather than means or media, these two questions appear to be easily answerable in theory if not in practice. The JWT permits a nation that suffers significant damage from an unjust attack to defend itself and punish the wrongdoer in any number of ways, provided principles such as the reasonable hope of success and proportionality are obeyed. The means of the attack is of secondary importance; the effect—the harm suffered—is what matters most. Similarly, the JWT seeks primarily to regulate the effects rather than the means of any military response to the initial aggression. Military aggression that happens to be a cyberattack is not ipso facto less (or more) damaging than a conventional attack. One simply cannot generalize. No wonder, then, that it's easy to imagine circumstances in which a patently military and vastly destructive cyberattack requires a nation to strike back kinetically. For instance, suppose a hostile nation uses a cyberattack to destroy part of our early-warning capability; we're suddenly blind to missiles and air-breathing threats in one sector. We might then choose to eliminate those threats preemptively using kinetic means.

The parity of CW and other sorts of war with respect to their possible effects should help us evaluate the morality of cyber first strikes as well—one of Dr. Dipert's hard cases. If the JWT endorses some kinds of first strike—to preempt unjust attack, for instance—the effect is again the key. It must conform to relevant JW principles such as proportionality. If it does, we won't pay much attention to the means of attack in most cases. Exceptions prove that rule. Admittedly the perfectly discriminate use of a tactical nuclear weapon would cause alarm because it was a nuclear weapon. That would seem to argue against the notion that the effect is everything, the means nothing. But in fact we'd worry about the nuclear means in such a case because we are ultimately concerned with effects: we'd fear any precedent that might make the use of indiscriminate nuclear weapons more likely. In other words, we'd still focus on effects, not on whether a given attack was carried out with cyber or other means. This is true of any kind of attack, including first strikes. A just-war adherent might find room in the tradition for first strikes that preempt imminent devastating attack (Israel 1967) or obstruct unwarranted harm being done to a third party (Kosovo 1999) but no place for first strikes that prevent vague dangers at an unspecified future date (Iraq 2003). A second just-war thinker might disagree on each point. But their disagreement would not have to do primarily with the *means* of first strike but rather with the effect. In most cases the JWT will care *why* CW is used and what its *effects* are, not that it's CW rather than another kind of warfare.

If the JWT applies to CW, it seems impossible to defend the notion that "traditional ethical and political theories—utilitarianism, Kantian theory, natural rights theory, etc.—cast so little light on this new, and difficult domain [CW]" as opposed to other domains (Dipert 2010: 406). How could that be true of CW and not equally true of other sorts of war? The JWT does not provide axioms; rather, it offers principles derived from meta-theories such as the ones Dr. Dipert mentions. In other words, take away "traditional ethical and political theories" and the JWT has no basis for its pre- and proscriptions. I know of no one who'd disagree with Dr. Dipert that game theory can provide useful insights into the nature and ethics of CW (as it has long done in analysis of non-CW). However, it seems not just counterintuitive but indeed demonstrably false that "traditional ethical and political theories" won't usefully inform our analysis of cyber issues even if those theories by themselves prove insufficient to solve the problems we perceive.

In fact, US directives relevant to CW are already indebted to such theories. Arguably the major post-9/11 documents relevant to CW are the *Federal Information Security Management Act of 2002* (FISMA), the *National Strategy to Secure Cyberspace*, the *National Institute of Standards & Technology Special Publication 800–53*, the *National Military Strategy for Cyberspace Operations*, and the *44th President's National Cyberspace Policy Review*. Each in its own way refers to a theoretical underpinning. The *44th President's National Cyberspace Policy Review*, for example, includes the following language: "But with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights. The government has a responsibility to address these strategic vulnerabilities to ensure that the United States and its citizens, together with the larger community of nations, can realize the full potential of the information technology revolution"[7] One can make too much of a single line in a single document. That granted, however, the statement above is as much related to "traditional ethical and political theories" as anything one would expect to find in documents related to war more generally. Consider this passage from the opening paragraph of the 2010 National Security Strategy: "We live in a time of sweeping change. The success of free nations, open markets, and social progress in recent decades has accelerated globalization on an unprecedented scale. This has opened the door to hundreds of millions of people, and made peace possible among the major powers. Yet globalization has also intensified the dangers we face—from international terrorism and the spread of deadly technologies, to economic upheaval and the changing climate. ... we will be unwavering in our commitment to the security of our people, allies, and partners."[8]

A strong assertion of government's role in guaranteeing security is evident in both statements above, an assertion that one could tie to several political theories. One could argue that such a tether doesn't in itself demonstrate the usefulness of received theory in solving practical contemporary problems. But the similarity in the quotations does suggest that cyber policy is no more distant from "traditional ethical and political theories" than national defense policy is. Perhaps Dr. Dipert is not arguing for the mistaken position; perhaps he simply wants to point out that broad-brush theories are difficult to apply to any specific activity in actual war, cyber or not. If he does mean to say that CW is somehow *uniquely* isolated from ethical and political theory, he might have fallen victim to the stacked rhetorical deck discussed in Section 1 above.

4. Differences

Despite CW's similarities to other forms of war, I agree with Dr. Dipert that CW isn't quite like anything else. There's no perfect analogy between military cyberation and military aviation or military navigation, for instance. CW is not just newer; it's arguably faster-evolving. Here are some potential challenges that the JWT will have to accommodate:

Visibility and accountability. It goes without saying that it will sometimes be hard to defend against CW. But defense aside, what can citizens on the aggressor's side know about their country's CWs? Arguably citizens of democracies will have less visibility and therefore less control of what their governments do in CW than in other kinds of war. This will be a difference of degree rather than kind. Governments can hide, and have long hidden, their uses of other means of war such as military aviation. An executive authority such as a US president can order many kilotons of ordnance to be dropped secretly in places like Laos and Cambodia or on officially off-limits targets. Officers such as General Lavelle can be co-opted and then made the scapegoats if prying journalists or others find out.[9] But if a government sends its military aircraft to attack covertly and lies to its citizens, it's still possible that someone will snap a photo, find some traceable dud ordnance or shrapnel, or otherwise document the activity. CW will take place in the form of physical processes too. Theoretically, those will also be traceable as a nexus of causes and effects pointing to an initiator. But the level of sophistication necessary to perform such a trace, and the relative impenetrability of the areas where those clues might be had, are arguably new in the history of warfare. We've grown used to the notion of embedded journalists, and we can imagine the rogue journalist who goes where she's not supposed to, finds out the covert truth, and then tells the world. But what would the embedded journalist-hacker look like? Could she slip away into the off-limits zones of cyberspace and discover a CW that a government had tried to conceal? I find it implausible. That's not to say journalists don't find it challenging to work in conventional war zones too. And surely it shouldn't be impossible to report on CW and cyber combatants; perhaps it won't even be harder than investigating other kinds of covert operation. Still, CW doesn't have to be enormously easier to cover up than other types of war; a matter of degree can be significant as citizens try to hold their government accountable.

Devolution to blunt instrument. Many weapons technologies are theoretically surgical but become practically indiscriminate. Aviation had traced something like that trajectory by the time strategic bombers attacked Hiroshima and Nagasaki. Many of us hoped "smart" weapons of the last generation had turned that corner. On the other hand, smart weapons killed enough civilians in Afghanistan to prompt General McChrystal to restrict and reduce aerial attacks. Nuclear attacks much more potent and numerous than those of 1945 remain a possibility. Whether or not airborne weapons eventually become surgical in their technical capabilities and unfailingly discriminate in their employment, one can imagine CW methods that a nation might be tempted to use too frequently and broadly. Cyberattacks on industrial control systems (ICSs) may provide a case in point: a nation that can neutralize its enemies' centers of gravity such as power grids through CW rather than kinetic attack will be tempted to do so. That sort of attack is likely to be at least somewhat indiscriminate because it targets dual-use assets. Many other examples come to mind.

Practitioners' evolving identities. In 2005 the U.S. Air Force changed its mission description, putting cyberspace on a par with its longtime bailiwicks of air and space. The new text reads: "Deliver sovereign options for the defense of the United States of America and its global interests – to fly and fight in Air, Space, and Cyberspace."[10] Just a few months ago the Air Force dubbed a number of its former communications-computer officers "cyber operators" and changed their numerical specialty code. In Air Force culture the term "operator" delineates those who are closest to the spear's tip as opposed to those who work in "support" career fields: pilots, navigators, some missile crew members, and now certain cyber specialists are "operators." Certainly cyber operators *might* be targets of enemy attack, and one can imagine scenarios where they are especially endangered. But it seems more likely that many will never face the dangers that, say, infantrymen are used to. The cyber operators' daily grind might resemble that of drone pilots, who suddenly find themselves the subjects of a fast-growing literature. A focal point of that literature is the oddity of “warriors” sitting in air-conditioned control modules in Nevada while piloting armed drones above Afghanistan and Pakistan. If bombs were falling in a one-hundred-mile radius around Las Vegas, one might consider the RPA (remotely piloted aircraft) pilots somewhat analogous to, say, a mortar crew on an active battlefield. As things stand, however, a number of drone pilots are too far from the action for that analogy to hold. They more closely resemble the crew of a missile submarine or perhaps of a B-52 on a mission to fire standoff weapons such as cruise missiles. Yet the Nevada operators are not pursued by other vessels in a hostile medium such as the sea’s depths or the troposphere and stratosphere. So what are they? Skilled technicians? Certainly. Officers subject to the UCMJ and beholden to a professional code? Yes. “Soldiers” in other senses? Perhaps not. Cyber operators might be like the RPA pilots in all these senses. The relatively unique status or RPA pilots and cyber operators may well challenge the JWT. For instance, if the cyber operators sleep in Las Vegas and its suburbs, are their homes and neighborhoods military facilities? Has the US adequately separated cyber operators from non-combatants?[11]

Autonomous CW. Arguably defense against some kinds of cyberattack is already largely autonomous. One can imagine advantages if offensive CW followed suit, advantages significant enough to convince molasses-paced carbon units to step aside. (Imagine a cyber equivalent of the US Navy’s Phalanx anti-missile system: at some point it *must* function fully autonomously or fail to do its job.) To the extent CW becomes autonomous under the sense-think-act paradigm, it will face some of the same ethical issues as autonomous agents that we don’t currently tend to consider cyber weapons. This will raise additional problems, among them:

Under- and overconfidence in cyber technology. In Robert Heinlein’s science fiction novel *Friday*,[12] a veteran parabolic ballistic “airline” captain named Ian Tormey admits to the novel’s namesake, Friday Baldwin, that a computer could fly the passenger craft more proficiently than he can . . . and often does. But Captain Tormey hastens to add that air travelers require a degree of confidence that most can place only in another human being. To know a computer held their lives in its chips would be unacceptable to many; they’d never be willing to fly. Besides, Captain Tormey explains, the average passenger trusts not just the competence but also the empathy of the protoplasm pilot. The looming worry is that a computer algorithm would lack emotion and so not feel desperate to save the human passengers of the aircraft in case of emergency; maybe it would just give up. Of course a computer might be less likely that a human pilot to disguise a fundamental misanthropy or turn psychopathic under pressure or get drunk a couple of hours before takeoff. Then again, we find it all too easy to suspend our disbelief that computers could act against our interests as we read Arthur Clarke’s short story or watch Kubrick’s film version.[13] Even in what is arguably Heinlein’s most sympathetic portrayal of a computer—Mike in *The Moon is a Harsh Mistress*[14]—the question of confidence is front and center.

To the extent that Mike the computer is self-aware, is his identity that of a capricious child or of a steadfast moral agent? Mike is juxtaposed with his human technician's bionic limb: Mike is a computer that can run a planet and more alone, without any human help at all, while the artificial limb is a computer of sorts that is always and necessarily at the technician's beck and call. This juxtaposition reveals a tension that's presumably here to stay. Reasons to make CW increasingly autonomous (analogous to the reasons why the Navy's Phalanx system must have a fully autonomous mode) will sometimes encounter the doubts of a populace not yet ready to cede important wartime decisions to computers.

The other side of the confidence coin is a sort of techno-hubris. The key principles of the JWT are both well and badly served by technology, depending on one's perspectives and aims. Consumers of news, advertisement, and government policy papers in the U.S. hear that technology such as global positioning satellites and receivers make projection of military power much more efficient. So do stealth technologies that help aircraft penetrate hostile airspaces, and so do smart weapons that can hit their targets with greater accuracy and therefore discrimination than earlier generations of weapons. But consider: during the air campaign over Kosovo, U.S. stealth aircraft, guided at least in part by GPS, bombed the Chinese embassy in Belgrade. The U.S. was quick to call the attack an unfortunate error caused by bad intelligence.[15] Frequently punctuating our idealization, perhaps even idolization of so-called smart weaponry are reports of civilian casualties caused by air attacks in Afghanistan and Pakistan. It's likely the same confidence some now place in air supremacy-cum-smart weapons will transfer to the tools of autonomous CW. It's too easy to forget that even the most sophisticated CW systems will share the vulnerabilities of other weapons. Bad intelligence, for instance, could cause otherwise superb tools of CW to destroy many innocent lives.

An international legal bias favoring cyber-haves versus cyber-have-nots. A troubling literature suggests that the law doesn't just fall silent in times of war, as Cicero suggested, but that powerful countries routinely succeed in manipulating international law in general and LOAC in particular to favor their own ways of war. Dr. Thomas W. Smith notes that "Just war theorists contend that soldiers hold a different moral status than that of civilians and thus assume greater risk to life and limb. The Pentagon has weakened, if not reversed, that assumption. RAND's Project Air Force found that the U.S. military favors a 'liberal interpretation' of legal duties to avoid collateral damage, 'one that permits an extremely high level of force protection so long as an appropriate level of accuracy is ensured."[16] One need not accept all of Dr. Smith's conclusions nor his skepticism of what Dr. Alan Vick et al concluded about the ethics of US air attack on urban targets to understand how his reasoning might apply to CW. To the extent that LOAC will be written by the movers and shakers on the international scene, it's possible that future laws governing the use of cyber weapons could allow something like the "appropriate level of accuracy" that RAND envisioned as US military aviation's goal. Where would that leave groups—national or otherwise—who have no access to sophisticated cyber weapons? Presumably they would employ whatever options the asymmetry of the martial landscape allowed while accusing cyber-capable enemies of war crimes or the like. "Contemporary laws of war *are* humanitarian at the low-tech end, and have been crucial in condemning atrocities, including sexual violence, associated with ethnic and other civil conflicts. But if hi-tech violence is shielded from prosecution, this may sap the moral force of the law and allow low-end offenders to paint themselves as the victims of politicized proceedings."[17]

Conclusion

It's worth repeating that all of these existing and potential problems in the application of the JWT to CW represent differences in degree rather than kind. Although CW presents somewhat new ethical challenges, it is not so unique as to defy analysis by the JWT. On the contrary, the JWT focuses on effects and intentions regardless of the type of warfare waged; those elements will be discernible in CW just as they are in other modes of warfare. Problems such as that of attribution will present complications, but that's hardly new to CW. Similarly, JW thinkers might encounter grey areas where cyber harm falling short of CW complicates analysis. Again, that's nothing new: just as aviation includes not just military but also civilian sectors and a grey area uniting both, what I've called "cyberation" will encompass both broad categories of use and a grey area somewhere at the center. The JWT will not solve all the ethical issues of CW any more than it does for any other kind of warfare. Still, its guidance will be not just relevant but indispensable to the conduct of just CW.

Notes

[1] William K. Rashbaum and Al Baker, "Smoking Car to an Arrest in 53 Hours." The New York Times, 4 May 2010, http://www.nytimes.com/2010/05/05/nyregion/05tictoc.html?scp=14&sq=faisal%20shahzad%20al%20baker&st=cse

[2] This issue of JME.

[3] I cannot find the passage Dr. Dipert refers to in Owens, William et al, eds., *Technology, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* National Academies Press, 2009. Professor Jeff McMahan did participate in an October 2006 meeting of the Committee on Offensive Information Warfare, an effort that supported the overall agenda of Admiral Owens et al. But there is no mention of Prof. McMahan's specific contributions. See Appendix B in http://www.nap.edu/openbook.php?record_id=12651.

[4] In 1866 G.J.G. de La Landelle coined the term *aviation* on the pattern of the word *navigation* (*avis*, bird + *agere*, to drive; *navis*, ship + *agere*). If we take Norbert Wiener's cybernetics (Fr. *cybernétique* <Gk. *kybernetes*, a steersman) and Gibson's derivative, *cyberspace*, would we be tempted to create *cyberation*? Either it's redundant—driving him who steers seems too close to driving him who drives—or else appropriately analogous to *aviation* and *navigation*, since in some sense birds and ships do drive themselves. Close enough: for present purposes it suffices to have a generic term to describe cyber goings-on on in a way that "saves the phenomena" (all three of them—cyberspace, cyber stuff, and cyber activities) in the same way that *aviation* and *navigation* link common parlance and common conception.

[5] *Washington Post*, 23 Sep 2010.

[6] The movie *WarGames* (United Artists, 1983) challenged Hollywood's public to think of "military computers" as those controlling missile sensors and launch facilities. But of course developed nations' defense establishments are tied to an enormous range of industrial cyber infrastructures. So-called industrial control systems (ICSs) are critical to facilities ranging from military bases to private corporations. ICSs supporting Iran's nuclear development provide a recent example of a cyber attack which some might see as "exotic": q.v. John Markoff and David Sanger, "In a Computer Worm, a Possible Biblical Clue." *The New York Times*, 29 September 2010, http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?pagewanted=1&_r=1&ref=todayspaper.)

[7] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[8] http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf, p. i.

[9] http://www.nytimes.com/2010/08/08/opinion/08sun3.html?_r=1&ref=richard_milhous_nixon; cf. Charles Stevenson, "General Misconduct." http://www.nytimes.com/2010/08/19/opinion/19stevenson.html?ref=richard_milhous_nixon.

[10] http://www.af.mil/news/story.asp?id=123013440.

[11] Cf. 1977 Protocol Additional . . . Part IV. Art. 58. http://www.icrc.org/ihl.nsf/WebART/470-750074?OpenDocument

[12] Heinlein, Robert A. *Friday.* New York: Del Rey, 1983 (1982).

[13] *2001: A Space Odyssey.* MGM 1968. Screenplay Stanley Kubrick and Arthur Clarke. Based on Clarke's short story "The Sentinnel."

[14] Heinlein, Robert A. *The Moon Is a Harsh Mistress.* New York: Orb, 1997 (1966).

[15] *The Guardian* (UK) had a different take. See John Sweeney, Jens Holsoe, Ed Vulliamy, "NATO Bombed the Chinese Deliberately." *The Guardian*. 17 October 1999. http://www.guardian.co.uk/world/1999/oct/17/balkans.

[16] Thomas W. Smith, "The New Law of War: Legitimizing Hi-Tech and Infrastructural Violence." *International Studies Quarterly.* Vol 46, No. 3 (Sep 2002), pp. 355–374, p. 361.

[17] Smith 362.

Reference

Dipert, R. R. (2010) The Ethics of Cyberwarfare, *Journal of Military Ethics*, 9(4), pp. 384–410 (Abingdon, Routledge).

Biography

James Cook is professor and head of the Department of Philosophy at the US Air Force Academy.