2013

The code of the cyberwarrior

Matthew T. Beard

University of Notre Dame Australia, matthew.beard@nd.edu.au

Follow this and additional works at: http://researchonline.nd.edu.au/phil_conference

Part of the Philosophy Commons

This conference paper was originally published as:

This conference paper is posted on ResearchOnline@ND at http://researchonline.nd.edu.au/phil_conference/34. For more information, please contact researchonline@nd.edu.au.
The Code of the Cyberwarrior?
Matthew Beard
Centre for Faith, Ethics & Society, University of Notre Dame, Australia.

Abstract
The emergence of cyberwar as a mode of warfare poses a number of challenges to moral appraisals of war. Although elsewhere I have argued that most of the questions provoked by cyberwar can be resolved within the existing framework of just war theory, there do appear to be important moral differences between individuals carrying out acts of cyberwar and soldiers on the battlefield. As well as being governed by principles of *jus in bello*, warriors tend to see themselves as being bound by a "code of honour". This code includes values like loyalty, fraternity, courage and obedience, as is central to soldiers' ability to take pride in a practice which can be morally dubious.

However, as war shifts into the cyber dimension, it is important to ask whether practitioners of "cyberwar" should see the same warrior codes as governing their conduct. Unlike soldiers, these government-employed hackers face no personal risk. Should they be divided into regiments and seen as military personnel, or are they more akin to intelligence agents? In this paper, I will argue that the cyberwarrior must see himself as governed by a different moral code than the soldier, because he faces no personal risk in plying his trade. The cyberwarrior is much more akin to a spy than a soldier, and thus the "cyberwarrior code" should emphasise values such as discretion, creativity and temperance over courage, loyalty and fraternity.

The Code of the Cyberwarrior

Introduction
I will begin with a broad claim: thus far, discussions of cyberwar have failed to engage in serious conversations about the morality of cyberwarriors. For those of us familiar with military ethics, this is curious, as there is widespread debate within the literature surrounding the morality of soldiers, who seem to be the moral equivalent of cyberwarriors. It is important to discuss the ethics of soldiering because soldiers are asked to, as a matter of necessity, kill other people, which ordinary moral thinking holds to be a *prima facie* wrong. Thus, we require a nuanced account of explaining how soldiers' killings can be justified. There must be similar discussions regarding the profession of the cyberwarrior. Although some of the specifics of what cyberwarriors are asked to do remains unclear, it is important to speculate in a general sense at least about how moral judgement can be brought to bear on those who commit acts of cyberwar.

When ordinary soldiers go to war, they are bound by a series of ethical principles which proscribe particular actions, and forbid others: the Laws of Armed Conflict. However, they are also bound by a more elusive notion, a set of beliefs about what it is honourable or shameful for warriors to do in times of war: the Warrior Code. Both the Laws of Armed Conflict and the Warrior Code co-operate together in motivating soldiers to perform their professional roles with moral distinction. Until this point, discussions of cyberwar have been limited to the discussion of exactly what the Laws of Armed Conflict with regard to cyberwar should be. As worthwhile as this project is, it should not be done in isolation; equally important is the development of a code of honour that applies directly to cyberwarriors. Without a "Code of the Cyberwarrior," the Laws of Armed Conflict are at risk of
lacking the motivating force they require, and military ethics also risks “playing catch-up” in a rapidly advancing field.

This paper will have two major sections. The first will introduce the idea of the Warrior Code and argue that because cyberwarriors are not required to either kill or risk their own lives they should not be seen as warriors in the sense relevant to the code. The second section will suggest that cyberwarriors are more closely connected to the practices of the spy and the saboteur, and that the ethical principles and virtues that govern spies and saboteurs may, therefore, provide a helpful starting point in the development of an honour code for cyberwarriors.

The Warrior Code

In her book, *The Warrior Code*, Shannon E. French argues that warrior cultures scattered throughout history and geography have developed codes of honour: a commonly held standard of what the ideal warrior does and does not do which bears normatively on each warrior within the culture.1 These normative bearings go well beyond the requirements of the Law of Armed Conflict (LOAC), entailing *what it is to be a warrior*. Warrior codes, French contends, ensure that morally upstanding and honourable conduct is intertwined with the warrior’s identity. She refers to an incident discussed by Mark Osiel in which a Marine refrains from killing a noncombatant after receiving the simple rebuke “Marines don’t do that.”

“Marines don’t do that” is not merely shorthand for “Marines don’t shoot unarmed civilians; Marines don’t rape women; Marines don’t leave Marines behind; Marines don’t despoil corpses,” even though those firm injunctions and many others are part of what we might call the Marines’ Code. What Marines internalize when they are indoctrinated into the culture of the Corps is an amalgam of specific regulations, general concepts (e.g. honor, courage, commitment, discipline, loyalty, teamwork), history and tradition that adds up to a coherent sense of what it is to be a Marine.2 French argues that “[t]he [warrior] code is not imposed from the outside. The warriors themselves police strict adherence to these standards, with violators being shamed, ostracized, or even killed by their peers.”3 The reason for the warrior codes’ (there are many different codes, as French’s work shows) being developed by the warriors themselves is because an internally developed code assented to by peers has a more powerful binding force than externally imposed rules. Military education should seek to help warriors “internalize an appropriate warriors’ code that will inspire [them] to recognize and reject a criminal direction from [their] officer.”4

Cyberwarriors, however, are not warriors in the sense that the code is interested in. The reason is because so much of the warrior code is concerned with how people whose task is to kill others can maintain an upstanding moral identity. The warrior code ensures that warriors “take only certain lives in certain ways, at certain times, and for certain reasons. Otherwise, they become indistinguishable from murderers.”5 Cyberwarriors, however, are not killers. If cyberwarriors come to identify themselves as governed by a warrior code, they will find it an ill fit; indeed, insofar as

---

1 French, *The Code of the Warrior*, p. 3
2 French, *The Code of the Warrior*, p. 15
3 French, *The Code of the Warrior*, p. 3
5 French, *The Code of the Warrior*, p. 3
the warrior code esteems valour and what Christian Enemark calls “physical courage,” and cyberwarriors are presented with no opportunities to practice those virtues, the identification of cyberwarriors with a traditional warrior code may well lead to unjustified feelings of shame, alienation, and purposelessness.

The Cyberwarrior: Spy and Saboteur

I believe the cyberwarrior’s craft places him somewhere between the spy and the saboteur. Although the exact nature of what cyberwarriors do is shrouded in mystery, most evidence points to their having two major roles (at least offensively): the gathering of information, and the infiltration and damaging of enemy infrastructure and systems. The former role pertains to espionage, and the latter to sabotage. Note, importantly, that neither involves killing (at least as an a priori function of the roles, although, of course, physical spies and saboteurs may be forced to kill in carrying out their duties). The virtues of the cyberwarrior, therefore, will be some kind of synthesis of the virtues of the spy and the saboteur.

Spies, or “intelligence officers,” deal not only in obtaining information, but in discriminating between information that is relevant and useful, and information which is useless or false. Thus, the good spy is discerning and prudent. He is able to identify relevant information quickly and use it to the benefit of his nation. However, spies are usually sent to extract information from sources which have already been identified (by other spies and intelligence) as having a high chance of possessing valuable information. Tony Pfaff and Jefferey R. Tiel argue that “the feature that will make persons subject to espionage operations is that they possess or are likely to possess secrets that threaten national security.” This is often not the case in cyber espionage, where – as the Snowden case has demonstrated – security operatives have access to huge amounts of information that has been gathered indiscriminately. However, rather than undermining the need for virtues of discernment, this fact makes them all the more pressing. The good cyberwarrior will be able to determine what, from a huge array of information, is worth pursuing in depth, and what is worth setting aside.

Discernment also touches on another virtue of the good cyberwarrior: discretion. Within their work, cyberwarriors are likely to come across a host of sensitive information of little relevance to their purposes. Cyberwarriors must consider it a matter of honour never to disclose any information that they do not judge explicitly relevant to national security. This includes, I would argue, at least some forms of personal information that can be used to blackmail people into becoming “false-flag” agents (agents working against their own nation). The reason why blackmail and coercion should not be justified under a cyberwarrior code is because it, like the warrior code, is subject to universally applicable moral laws (such as, for example, the Laws of Armed Conflict). If coercion and exploitation are unjustifiable under broader moral principles, they should not be lauded by a code of honour. Furthermore, this discernment and discretion should not be made solely by balancing the probability of success against the cost (in terms of employee hours, cost, etc.), but also against the moral costs of potentially invading the privacy of someone who has done nothing wrong. Privacy is perhaps the key value at stake in discussions of espionage, so key in fact

---

6 Enemark, *Armed Drones and Military Virtue*, p. 80
that Anita L. Allen argues that “[e]ven wrongdoers’ expectations of privacy matter prima facie when selecting the means of information gathering.” Because of their ready access to information, cyberwarriors should pride themselves on being secret-keepers, who only violate privacy in extreme circumstances, rather than Orwellian observers with the private information of civilians at their fingertips.

The other central role of cyberwarriors is their use in undermining cyber systems of their enemies. These can be used to cripple an opponent’s own ability to launch cyberattacks, disrupt enemy communications before one’s own (physical) military strike, and so on. Here, the function of the cyberwarrior is to sabotage the infrastructure of an enemy nation. Like physical saboteurs, the primary moral concerns here are ones that warriors share: that civilian harms from such attacks are minimised, and that the damage is proportionate to the offence committed by the target. However, to be excellent the cyberwarrior is required to do more than simply adhere to laws of (cyber) conflict like discrimination and proportionality, as Mark Osiel notes:

By taking seriously [...] internal conceptions of martial honor, we may be able to impose higher standards on professional soldiers than the law has traditionally done, in the knowledge that good soldiers already impose these standards on themselves.

What makes cyberwar more appealing than conventional war? Simply, the fact that less people are killed in conducting cyberwar. The entire justification of the cyberwarriors existence is the reduction of casualties and thus, although every cyberwarrior is bound not to directly target civilians, and minimize the effect of his attacks on civilians, the excellent cyberwarrior will direct his ends toward the prevention of all casualties, and minimising his collateral damage from “proportional” to “none.” Just as an excellent saboteur will aim to do his job and leave without being noticed or destroying anything other than the target, the cyberwarrior will aim to keep his job as “clean” as possible, minimising casualties as a matter of pride and honour, as well as from commitment to the laws of war.

Conclusions

As is necessary in so short a piece, I have not been able to speculate very deeply regarding the possibly “points of honour” for cyberwarriors. This would require a more engaged study and more familiarity with what cyberwarriors actually do. However, it does seem to me (i) crucial that cyberwarriors develop a code of honour; and (ii) that the source of that code will be more akin to that of non-killing operatives than warriors, whose code is largely derived from the need to justify the killing done by warriors. Not only is this important as a source of identity and moral conduct for cyberwarriors but if principles underpinning the profession are identified, they may help to ensure cyberwarriors do what is right in areas that the laws of conflict have not yet considered; as French notes, “[a] code that encompasses all of what it is to be a particular kind of warrior may help the warrior who has internalized it determine the proper course of action in a situation the rule writers could never have foreseen.”

If modern wars are to be increasingly conducted by non-

---

11 French, The Code of the Warrior, p. 16
physical combatants, then the development of a code that reconciles the moral excellence of the agent with his profession must be a central priority for military ethicists and practitioners.