SOCIETY FOR APPLIED PHILOSOPHY
Annual Conference 2013
28-30 June, University of Zurich

Location: SOE E-1
11.30-1.30pm
Saturday 29 June 2013
20 min talk (10 mins questions)

Ethics, Cybersecurity and the Military

Abstract

In this paper I examine the issue of cybersecurity in the context of the conventionally understood ends of the military. I start out by demonstrating that the use of military capabilities to deal with cyberthreats creates a number of headaches for conventional ethical approaches to conflict, especially just war theory. I describe a number of cases that give us cause to question the validity of cyberweapons as a legitimate military capability. And I argue that the current development of cyberweapons, and their emerging use, is a significant challenge for conventional military ethics.

Then I describe three specific moral problems for the military when it comes to using cyberweapons. First is the 'threshold' problem which is the concern that cyber weapons will lower the threshold for resorting to war. Second is the 'collateral harm' problem which is the concern that cyberweapons increase the likelihood of civilians being deliberately targeted and/or becoming victims of disproportionate attacks on dual-use infrastructure. Third is the 'accountability' problem because of the difficulty of holding accountable military personnel or their governments for the use or misuse of a weapons system.

Next I argue that conceptions of the military as an institution whose sole purpose is to 'kill people and break things' acts to compound the moral problems as I outline them above. This approach fails to acknowledge the necessary peacetime role played by military capabilities, gives insufficient ethical guidance for the use of these capabilities in non-war contexts and increases the risk of unnecessary collateral harm.

Consequently, I suggest that the purpose of the military should be conceived more broadly.   I argue that the conventional conception of the military as merely a ‘blunt instrument’ of the state whose sole purpose is to engage in hostile force against belligerents during war is too narrow in scope. I conclude by arguing that the military have a responsibility to protect and preserve the “life” of the political community it serves. I argue that the central aims for using the military’s ‘cyber-capabilities’ should be revised toward that end. I then highlight the types of cyberthreats to which this applies in order to shed light on the permissibility and obligations on the military when dealing with issues of cybersecurity.

Background

<Slide One>

Currently, I'm a Researcher with the Centre for Applied Philosophy and Public Ethics (CAPPE) where I manage the Ethics of Cybersecurity project.

I worked in Australia's Department of Defence for ten years.

- *Deputy Director, Strategic Assessments, Strategic Policy Division (2005-2008)*.
- *Assistant Director, Information Strategy and Futures, Chief Information Office (2004-2005)*.
- *Intelligence Analyst, Defence Intelligence Organisation (1999-2004)*.

I'm also working on finishing my Doctorate with CAPPE.

- Justifying Killing by the Police and Military: The Ethics of Institutionalised Lethal Force.

Introduction

In this paper, I argue that the current development of cyber-capabilities, and their emerging use, is a significant challenge for conventional military ethics.

First, I start out by giving a brief description of the Ethics of Cybersecurity project.

Second, I outline three specific moral problems for the military when it comes to using cyberweapons. This includes giving brief descriptions of: the 'threshold problem,' the 'collateral harm problem,' and the 'attribution problem.'

Third, I argue that conceptions of the military as an institution whose sole purpose is warfighting acts to compound these moral problems.

A. The Joint CAPPE-NSC Ethics of Cybersecurity Project

<Slide Two>

As I mentioned above, I manage the Ethics of Cybersecurity Project.

Cybersecurity (or the systemised protection of individuals and states against cyberwarfare, cyberespionage and cybercrime) is an increasingly prominent feature of international and national security.

An effective response to emerging threats to cybersecurity, however, requires a comprehensive understanding of the problem and its potential solutions. The potential for a serious attack on Australia's cybersecurity is a growing reality, but many of the important theoretical, ethical and policy aspects of cybersecurity remain unexamined.

<Slide Three>

Our project proposes to develop an ethical framework for guiding cybersecurity decision-making, especially in the Australian context.

It will describe the cyberthreats to Australia's national security and then explore the ethical and theoretical issues that arise from dealing with them, resulting in a general set of advice for practitioners and policy-makers in a National Security College (NSC) Occasional Paper.

The NSC is a specialist graduate studies school, offering graduate studies and professional courses aimed at enhancing the functioning of the national security community, strengthening networks of cooperation between practitioners and non-government experts, and achieving effective outreach to business and the wider community.

The National Security College was announced as a joint venture between the Commonwealth Government and ANU by current Prime Minister Kevin Rudd and former Vice-Chancellor Professor Ian Chubb in December 2009.

Therefore, our research project aims to contribute to this comprehensive understanding by examining the key:

1) Cyberthreats confronting Australia's national security;

2) Tensions between the rights of citizens and the responsibilities of national security institutions; and
3) Mechanisms by which security can be achieved.

In short, we aim to develop an ethical framework that provides the opportunity to bring together disparate elements of the issue, including military, law enforcement, and intelligence aspects. This then will provide the basis for a general set of guidance options that can anticipate future developments in a way that is transparent, accountable and responsive.

<Slide Four>

Activities

Consultations/Discussions:

- Delft visit and colloquium: 18-20 June 2013
- Zurich Panel: 29 June 2013
- Computer Ethics (CEPE) Lisbon, Portugal: 1-3 June 2013
- Society for Philosophy of Technology (SPT): 3-6 July 2013

Workshop (Cyberwar, Cyberterrorism and Cybercrime: Mapping the Ethical Terrain)

- In Canberra: 5-6 August
- Public seminar: 7 August
- People: George Lucas Jr, Pano Yannakogeorgos, Don Howard, Gary Waters, John Blackburn, Tobias Feakin, Alastair MacGibbon.

Edited Book for 2014

Journal Special Edition

Occasional Paper (Cybersecurity: Mapping the Ethical Terrain)
Final Submission due: December 2013

B. Using Military Cyber-capabilities

<Slide Five>

In this first section, I start out by demonstrating that the use of military cyber-capabilities, especially those dealing with cyberthreats, creates a number of headaches for conventional ethical approaches to conflict, especially just war theory.

<I will discuss the conceptualisation of Cybersecurity in more detail at the Society for Philosophy of Technology conference next week in Lisbon, Portugal>

Cybersecurity is used in the broad sense to capture everything that is happening in the cyber domain.

Many states have national Cybersecurity centres to coordinate government policy on this issue. For example, Australia is in the process of setting up the Australian Cyber Security Centre (ACSC).

But Cybersecurity can also be used in the more narrow sense as protecting cyber-infrastructure from threats to its trustworthiness *(Adam Henschke will talk more about "trust" in his talk)*.

Either way, the range of cyberthreats is radically diverse.

Cybersecurity encompasses a range of conceptual axes: private and public infrastructure; threats against information or harms to or through physical devices.

Cyberthreats may be isolated to single machines, distributed attacks against large numbers of machines at once, or mimetic in nature, such as computer viruses and worms.

Cyberthreats can be personal in nature, such as identity fraud, or lead to massive and widespread harms, such as attacks on critical infrastructure such as power plants. The intersections between these different ways of understanding cyberthreats create a startling number of ways to secure against malevolent actors in cyberspace.

The important area of focus for this talk, however, is the debate surrounding cyberwar and, in particular, the use of “cyberweapons.”

According to Rowe (2010)[1], Cyberweapons are software used to attack other software or data within computer systems. He distinguishes cyberweapons and cyberattacks (attacks using cyberweapons) from “information warfare”, a more general term that includes propaganda, electronic surveillance, cyber-espionage, and defensive information operations. That is, he focuses on "information attack" and not "information exploitation" or "information defense".

But the problem with Rowe’s approach to cyberweapons is that he does not explicitly include damage within his definition (though it might be considered implicit since he is talking about weapons).

Dipert suggests that cyber attacks are (2010: 398) “intentional cyberharms that are instigated or controlled by political organizations (or their military services) on other political organizations or services.”

<Example of Stuxnet? As Seumas mentioned in his talk>

According to Dipert,[2] cyberwar is the first major new form of warfare since the development of nuclear weapons.

Second, it is difficult to determine the source of cyberattacks.

Third, many cyberattacks will not be lethal and will not even result in permanent damage to physical objects.

Fourth, the necessary components of cyberwarfare (i.e. a laptop and an internet connection) are readily available to most people.

So what are the moral problems for the military when it comes to using cyberweapons?

First, the ‘threshold’ problem is the concern that cyber weapons will lower the threshold for resorting to war.

Second, the ‘collateral harm’ problem is the concern that cyberweapons increase the likelihood of civilians being deliberately targeted and/or becoming victims of disproportionate attacks on joint-use infrastructure.

Third, the ‘attribution’ problem is the difficulty of identifying the source of a cyberattack with sufficient certainty to respond.

Attributing a cyberattack to a specific party is notoriously difficult. To be morally justified in using a forceful response that causes significant harm to another party, a necessary condition is that the defender knows the alleged attacker intended to harm in some way.

<Slide Six>

In short, cyberweapons damage software in a variety of ways. But this damage to software also has the potential to harm physical infrastructure and humans.

There are, however, also non-damaging cyber-attacks.
1) Theft of information
2) Espionage
3) Control of systems

We could also talk about offensive and defensive cyberweapons but I won’t do that here.

The important point is that there is a distinction between “cyberweapons” (which do damage and sometimes harm) and “cyber-capabilities” (which are the military’s full suite of cybertools).

As Dipert points out, “Cyberattacks belong to a large genus of all kinds of attacks on information systems. Such attacks include traditional counterespionage and disinformation campaigns, old-fashioned destruction of telephone lines, jamming of radio signals, killing of carrier pigeons, and so on.”[3]

C. The Inadequacy of the 'Warfighting' paradigm

<Slide 8>

Having briefly describe the way in which the use of military cyber-capabilities create unique moral problems for the military, I now argue that conceiving of the military as an institution whose sole purpose is warfighting acts to compound these moral problems.

The conventional warfighting context presupposes that a particular act of violence is part of a larger struggle between two or more political communities engaged in armed conflict.

Importantly, the conventional understanding of violent conflict as part of a war fighting effort assumes three basic contextual conditions for the military use of lethal force.

First, the conflict originates in an international dispute rather than being a domestic issue. This means that the conflict occurs outside of the legal jurisdiction of the state itself. There is no overarching independently-enforced criminal justice system to which they are subject.

Second, the main parties to the conflict are both state actors.

Third, the incident is classifiable as an armed conflict and part of a war fighting effort. All this means that the individual soldier's use of lethal force occurs within, and must be judged in terms of, an environment vastly different to what we would expect within, say, the conventional law enforcement context.

But military cyber-capabilities have a necessary peacetime (or non-war role).

The military's peacetime role has often been neglected in discussions relating to military ethics.

For example, Dipert suggests, that "espionage is not usually an activity that has been considered part of the moral considerations in regarding going to war or conduct in war. The ethical considerations in espionage and other intelligence-gathering operations are but one of the several traditionally neglected aspects of the morality of war (although there has been growing interest in this field)."[4]

Now it is the ethicist's role to ensure that the (*in bello)* criteria are understood by users of cyber-weapons, and to insist that users are duly diligent in ascertaining technical capabilities and relevant aspects of situations in which they are used.[5]

But, as a consequence of Just War Theory's failure to acknowledge the peacetime role of the military, I argue that the 'warfighting' approach to judging the use of military 'cyber-capabilities' increases the risk of unnecessary collateral harm.

It does this because the "tight linkages between legitimate and illegitimate targets, will combine to frequently render internet-delivered cyber-attacks indiscriminate."[6]

And

"Even if cyber-weapons are discriminate, questions of unnecessary harm to combatants and disproportionate harm to civilians remain."[7]

<Slide 9>

For example, generally speaking,

"Targeting joint-use industries and systems in a lawful military conflict is generally permitted by international law and Just War Theory."[8]

Whereas,

"Targeting primarily civilian structures and networks is prohibited by international law and by almost all theories of morality in warfare."[9]

So,

"Cyberweapons could target joint-use infrastructure, that is, systems and structures for both civilian and military uses, or even civilian targets with the goal of demoralising, weakening, or confusing an enemy's military of civilian leadership."[10]

But the distinction between joint-use and civilian information systems is meaningless in cyberwarfare when the military use of civilian cyber infrastructure is ubiquitous.

<Slide 10>

This issue is compounded by the absence of agreement regarding the best actors to manage cyberthreats. Cyberwarfare, in being compared to kinetic attacks, is typically thought of in militaristic terms.

Yet cyberthreats do not need large numbers of willing actors to occur and do massive amounts of damage to information or infrastructure—dealing with small groups of autonomous actors is typically the purview of counterterrorism and counterinsurgency operations.

Furthermore, most existing cyberthreats are more mundane than ruining power supplies or hijacking drones—cyberthreats at present take the form of spam rings, extortion, money laundering, and other organized criminal activity.

So law enforcement becomes an attractive paradigm for conceptualizing cybersecurity; but this involves again different actors with different reach, jurisdictional boundaries, and purposes.

Conclusion

In conclusion, Cybersecurity is an increasingly prominent feature of the security landscape

A number of ethical questions arise between:
1) the diversity of threats to cybersecurity
2) the tradeoffs required to manage cyberthreats
3) lack of agreement about who is best positioned to secure cyberspace

And when it comes to the use of military cyber-capabilities, the 'warfighting' approach fails to acknowledge:
1) the necessary peacetime role played by military cyber-capabilities; and
2) gives insufficient ethical guidance for the use of these capabilities in non-war contexts.

OTHER POTENTIAL POINTS

The Conventional Law Enforcement context

The conventional law enforcement context describes an environment where a sovereign state (or similar political community) is reasonably effective at managing violent conflict within its own jurisdiction using a common body of law. It presupposes at least a basic form of government with functioning law-making body, criminal justice system and policing institutions. It also means the absence of serious armed conflict, especially recurring violent incidents between large politically-motivated groups. Within the law enforcement context, belligerents who are party to a conflict are treated as suspected criminals and not as combatants.[11]

The conventional understanding of violent conflict within the law enforcement context assumes three basic environmental conditions (or contextual conditions).

First, the conflict is a domestic rather than an international issue. This means that any given state is responsible for resolving a violent conflict that occurs within its own jurisdiction.

Second, it is generally assumed that the parties to a violent conflict are non-state actors and the role of the state is to adjudicate fairly between them.

Third, the incident is not classifiable as an armed conflict or part of a war fighting effort.

Notes

Barrett, Edward T. "Warfare in a New Domain: The Ethics of Military Cyber-Operations." *Journal of Military Ethics* 12, no. 1 (2013): 4-17.

Dipert, Randall R. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9, no. 4 (2010/12/01 2010): 384-410.

Maxwell, Mark. "Rebutting the Civilian Presumption: Playing Whack-a-Mole without a Mallet?". In *Targeted Killings: Law and Morality in an Asymmetrical World*, edited by C. Finkelstein, J.D. Ohlin and A. Altman. Oxford: Oxford University Press, 2012.

Rowe, Neil C. "The Ethics of Cyberweapons in Warfare." *International Journal of Technoethics* 1, no. 1 (2010): 20-31.

[1] Neil C Rowe, "The ethics of cyberweapons in warfare," *International Journal of Technoethics* 1, no. 1 (2010): 21.

[2] Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (2010): 385.

[3] Ibid., 386.

[4] Ibid., 389.

[5] Edward T. Barrett, "Warfare in a New Domain: The Ethics of Military Cyber-Operations," *Journal of Military Ethics* 12, no. 1 (2013): 10.

[6] Ibid.

[7] Ibid.

[8] Dipert, "The Ethics of Cyberwarfare," 390.

[9] Ibid.

[10] Ibid.

[11] Mark Maxwell, "Rebutting the Civilian Presumption: Playing Whack-a-Mole without a Mallet?," in *Targeted Killings: Law and Morality in an Asymmetrical World*, ed. C. Finkelstein, J.D. Ohlin, and A. Altman (Oxford: Oxford University Press, 2012), 36.