Contribution to Panel on Cyberwarfare

ISME 2011

Randall R. Dipert

University at Buffalo

rdipert@buffalo.edu

As with autonomous and non-lethal weapons, EMP, and other technological advances in weaponry, the single main question about cyberwarfare is whether it presents truly new ethical issues.

There is at this point remarkably little philosophical literature on ethical issues in cyberwarfare and little on information warfare[1] generally: there is Dr. Steck's paper[2], my own presentation here last year, subsequently published in the Dec. 2010 issue of the *Journal of Military Ethics*,[3] Col. James Cook's contribution to the same volume[4], and now Dr. Don Howard's presentation yesterday[5]. There is a great deal of other literature, but it is from a policy, legal, or computer-science perspective.[6]

The past year has seen several widely publicized developments in cyberwarfare. These have included the approval and subsequent formation of a centralized US Cyber Command, the appearance of Stuxnet, increased warnings of the dangers of cyberattacks on infrastructure, public discussion of Richard Clarke's book, and the release of several major policy studies. The news-cycle has also seen several debunking essays in the last 6 months

[1] Other than espionage, disinformation campaigns, etc.
[2] "Cyber Attacks and Non-combatant Immunity," ISME, Jan. 2011.
[3] "The Ethics of Cyberwarfare" ISME 2010 and JME, Dec. 2010.
[4] "Cyberation and Just War Doctrine: A Response to Randall Dipert," JME: 411-423.
[5] "Cyberwarfare and its Challenges to the Laws of Armed Conflict," ISME Jan. 2011.
[6] See my bibliography in JME Dec 2010.

arguing that the dangers of cyberwarfare are overblown, that its issues and terminology are confused, and even that the buzz around cyberwarfare is a public-relations attempt by various military organizations to increase funding. These have included an essay by Seymour Hersh in *The New Yorker*[7], an article in the New York Times,[8] and Col. Cook's essay. I think these critics need to be taken seriously, and that there is some confusion among journalists and the general public.

I myself had tried to avoid sensationalizing the dangers of nation-on-nation cyberattacks and argued only that there were now scattered, low-level cyberattacks, but that this level will probably slowly increase. I carefully defined my terms, differentiating cyberattacks (which could be done by hackers) from cyberwarfare (nation-on-nation cyberattacks) and cyberwar (extensive cyberwarfare with considerable damage or deaths). I think largescale, highly destructive cyberattacks by nations or stateless political organizations are not in the future, except possibly as part of a fullblown conventional war.

What then might be ethically new and interesting in cyberwarfare? I think there are five points that can be made. Some of these parallel Ed Barrett's concise summary of issues in cyberwarfare yesterday morning[9].

First, many nation-on-nation cyberattacks will not fit precisely into the paradigm cases of just war theory and existing international law. Namely, they will likely <u>not</u> be invasions of sovereign territory that bring destruction of physical facilities and the large-scale casualties of traditional warfare.

---

[7] Nov 1, 2010.
[8] "Apaocalypse in Cyberspace? It's Overdone," by Eric Pfanner, *NY Times* Jan. 16, 2011.
[9] His Powerpoint at ISME 2011 and his "Executive Summary and Command Brief" in JME Dec. 2011.

Instead, in the likely worst cast there would by extensive, but diffuse, damage to industry, infrastructure, and command and control's functioning. I call this the "ontological" problem of cyberwarfare: physical entities aren't killed or damaged. The total quantity of intentional harm may nevertheless fall within consequentialist or other thresholds for acts of war that morally permit counterattack. In some rare cases they may even justify a conventional counterattack.[10]

Second, there will be a necessity of ever increasing enhanced government cybersecurity measures now costing in the tens, and soon in the hundreds, of billions of dollars per year.[11] Because of the "attribution problem" of identifying the sources of attacks with certainty, and because of a lack of a common understanding over what would trigger a fighting war, most efforts and costs in the near future costs will be in the realm of defensive cyberwarfare, cybersecurity. Martin Libicki of Rand, Richard Clarke, and I all see an urgent need for the development of a substantial offensive cyberwarfare capacity that would serve as a deterrent. For there to be deterrence there would also have to be the demonstration of this capacity and announced policies for counterattack, possibly massive counterattack. (Stuxnet might have been partly intended as a demonstration of an ability to make such attacks.) There has been as yet no hint of an announced policy, despite the urgent need for one.

---

[10] When, as an example, the first attack was intentionally severely damaging, and when such an attack cannot be otherwise blocked or deterred

[11] The increased cybersecurity costs for repairing damage and purging malware cost the Pentagon over $100 million over only 6 months. (Internetnews.com April 8, 2009) The latest estimate I have seen for the protection of US government computers is $17 billion/per year, but this surely doesn't track the need to upgrade programs and operating systems, and amount of time wasted because of the threat. (nextgov.com May 19, 2008).

To make an analogy with the cold war, the U.S. has so been far been mostly in the business of building bigger and better bomb shelters. This despite the now well-understood folly of civil defense efforts in the nuclear past. These costs are likely to escalate to the point of being outrageous, eventually necessitating deterrence strategies, in what I call the coming Cyber Cold War.

Third, there is likely to be a long period of skirmishing at low levels with new cyberweapons, including testing and developing of targeting and insertion tools, and means of cyberdamage assessment. These cyberattacks on another state will also come from government-tolerated "patriotic" hackers and group and corporate proxies for governments. This will likely reach a game-theoretic equilibrium if sensible deterrent strategies are consistently followed.

Fourth, there are an array of possible technical and policy developments that may change this dynamic. These include reversible-damage cyberweapons[12], increasingly sophisticated forensic tools and better intelligence on potential enemies cyber capabilities, and even changes to the internet protocol that reduce anonymity--perhaps only at the level of national identification. Some have suggested a need, especially of military organizations, to move to alternative and even proprietary operating systems and productivity tools[13]. Even open-source operating systems (e.g., Linux)

---

[12] Proposed by Neil Rowe of the U.S. Naval Postgraduate School, Monterey CA.

[13] In the early days of apolitical hackers' attacks, attachments to emails, with macros in Microsoft Word, were a major source of mischief in DoD. Recently, flaws in Adobe Acrobat created vulnerabilities.

One proposal to changing operating systems is in Jeffrey Carr's *Inside Cyber Warfare*, 2010). His specific proposal is for critical infrastructure to switch to Linux, whose code is public and much simpler. This book is on Stratcom Commander Kevin Chilton's suggested reading list (http://www.stratcom.mil/reading_list/). My son, a computer professional, has convinced me that Carr's argument that, since there are fewer serious attacks on Mac

and tools would be easier to protect because of the relative simplicity and accessibility of the underlying code. To limit the botnet threat, and serve as an early-warning system for suspicious code sequences, Internet Service Providers (ISPs) and LANs could require recent application of the latest anti-malware tools before a computer can be connected to the network. Commercial cybersecurity corporations could be licensed and required to forward suspicious code to a central government clearing house. (Government cybersecurity experts would not be required immediately to report malware intrusions and reports to commercial cybersecurity organizations, although they should generally do so as soon as possible when it is compatible with national security.) To forestall hackers in our own country from attacking other countries, but being perceived by them as proxies for our own government, we will probably eventually need to apply the Neutrality Law (of 1794, with many alterations and now in U.S. C. Title 18 I.45 par 960) that forbids attacks on other nations by private American citizens. For a variety of reasons, existing international law is insufficient and it is likely that treaties banning or limiting varieties of cyberweapons are not feasible.

Finally, because of what appears to be the ability to narrowly target a facility or capability, without loss of life or collateral damage,[14] it may be that sophisticated cyberattacks (possibly Stuxnet) are an alternative to the usually ineffectual sanctions and diplomatic activity against rogue nations that do not risk a "shooting war." This may increase cyberweapons' use by

---

OS and Linux, they are therefore less vulnerable. (Carr, p. 193), is unconvincing: Microsoft Windows and products have simply made much more attractive targets.

[14] Rowe and others had quite reasonably argued that cyberweapons will actually be *more* prone than conventional weapons to unexpected and undesired side-effects and collateral damage.

technologically advanced nations against rogue states that are less advanced, but this seems like a good thing—no babies die from malnutrition as they sometimes do by sanctions.[15]

[15] Although their protests have been ignored, pariah nations subjected to sanctions have correctly argued that in the past blockades and embargos were treated as legitimate *casus belli*. There is a growing understanding of, and conceptual distinctions among, levels of force (see the preface to the 4th edition of Walzer's *Just and Unjust Wars*), "hard" force being a shooting war typically physically intrusive and that results in permanent damage or deaths, while "soft" force (force "short-of-war") consists of embargos, sanctions, other economic measures, moral pressure, and threats of soft or hard force. There are fine moral distinctions to be made even among the application of different kinds of soft force. Soft force has received fairly little attention in moral philosophy and in international law, and this is one cause for the moral and legal vacuum concerning cyberwarfare.