Chapter 15
The Ethics of Cyberweapons in Warfare

Neil C. Rowe
U.S. Naval Postgraduate School, USA

ABSTRACT
The author discusses the ethical issues of using cyberweapons, software that attacks data and other software during warfare. Many people assume these are relatively benign weapons, but we argue that they can create serious harms like any weapon. He defines cyberweapons and describes them in general terms, and survey their status as per the laws of war. He then discusses the unreliability of cyberweapons, the problem of collateral damage, and the associated problems of damage assessment, maintenance of secrecy, and mounting cyber-counterattacks. He examines some possibilities for creating more ethical cyberweapons and discusses the alternative of cyber-blockades. He concludes that cyberattacks should generally be outlawed by international agreement.

INTRODUCTION
Cyberweapons are software used to attack other software or data within computer systems (Bayles, 2001). We distinguish cyberweapons and cyberattacks (attacks using cyberweapons) from “information warfare”, a more general term that includes propaganda, electronic surveillance, cyber-espionage, and defensive information operations (Jones, Kovacich, & Luzwick, 2002). That is, we will focus on “network attack” and not “network exploitation” or “network defense”. Like conventional weapons, cyberweapons can be used against a variety of targets in a variety of circumstances with a wide range of lethality (White Wolf Security, 2009). Often cyberweapons exploit flaws or errors in software. Proponents have cited these as “clean” weapons that are safer than conventional weapons since they do not dam-
The Ethics of Cyberweapons in Warfare

unlike chemical, biological, and nuclear weapons, people have no visceral fear of cyberweapons for reasons like health consequences. But maybe they should. All weapons can have serious harms by virtue of their being weapons. The public is unaware of the degree to which they depend on computer systems and the information they store, and thus weapons targeting them can have many unforeseen consequences. For instance, targeting a country’s Internet service providers can prevent goods from being delivered, and cause people to starve or die from lack of necessary medical supplies.

There are several schools of ethics. In this article we will follow a pragmatic approach derived from utilitarian ethics in which we argue that a technology is unethical if it has a significant net harm to world society (“negative utilitarianism”). We would also like to derive ethical principles of using cyberweapons, so we will follow “rule utilitarianism”. Such principles can then be codified in laws of warfare. However, we do not need an elaborate ethical foundation here because most of the ethical issues with cyberattacks seem similarly problematic under any ethical framework.

THE STATE OF THE ART IN CYBERWEAPONS

Military organizations have noted the success of amateur attackers (“hackers”) in damaging computer systems, and have hoped to use these techniques or “exploits” for military advantage, much as they seek a wide variety of ways to gain advantage in warfare (Denning, 1999). Many of these techniques exploit flaws in software. Certain kinds of errors such as failure to check for buffer overflows in loops or failure to properly label data on Web sites can lead to granting of unauthorized special privileges to users of a system. Cyberweapons are programs that package a set of such exploits against a computer system and its data. Cyberweapons can be launched or controlled either externally, from another computer or the Internet, or internally, by spies and saboteurs (Knapp & Boulton, 2007).

Cyberattackers can use their access and privileges to destroy the data and software on a computer system or network, but that is pretty obvious and tells the victim they have been attacked. Cyberattackers can modify the data on a victim system to impede military operations, but that requires a good deal of contextual knowledge about the data. So a better goal for cyberweapons is to take control of a system without the knowledge of the system’s owner so it can be used for the attacker’s purposes. This technology is called “rootkits” (Kuhnhauser, 2004). Sets of such remotely controlled computers can be used to create “botnets”, networks of slave computers under the control of a single user (Bailey et al., 2009).

Hacker botnets have been used to earn money by sending spam or phishing email from the slave computers, have been used for denial-of-service attacks against organizations the attacker does not like, have been used for blackmail of organizations by threatening malicious mischief, and have been used for espionage. Botnets developed for military purposes could stop an adversary’s military organization from communicating or defending itself.

Cyberweapons can be an innocent-looking software module. Running them to see what they do is not easy because many require passwords to run and their effects may be very subtle. Thus it is difficult to identify cyberweapons within a computer system. Cyberweapons are easy to transport because they are just bit patterns that can be easily copied, or they can even wander autonomously as mobile “agents” (Ceruti, 2001). And when they have served their purpose, they can be deleted. This makes it considerably harder to police cyberweapons than nuclear, chemical, and biological weapons. Nonetheless, traces of a