IRM PRESS
701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com
ITB7698

Chapter 11

Cyberspace Ethics and Information Warfare

Matthew Warren
Deakin University, Australia

William Hutchinson
Edith Cowan University, Australia

INTRODUCTION

We have seen a rise in computer misuse at a global level and also the development of new policies and strategies to describe organized computer security attacks against the information society–these strategies are described as being "information warfare." This is very different from the traditional view of attack against computers by the individual, determined hacker, a cyber warrior with a code of conduct to follow. Today the threats come from individuals, corporations, government agencies (domestic and foreign), organized crime and terrorists. This new world of conflict in the electronic ether of virtual cyberspace has brought with it a new set of ethical dilemmas.

COMPUTER HACKERS

In the beginning, there were hackers. A group of what seem now to be a simple case of technocentric juveniles out to challenge their wits against the system. The term "computer hacker" usually denotes those who try to gain entry into a computer or computer network by defeating the computers' access (and/or security) controls. Hackers are by no means a new threat and have routinely featured in news stories during the last two decades. Indeed, they have become the traditional

Previously Published in *Social Responsibility in the Information Age*, edited by Gurpreet Dhillon, Copyright © 2002, Idea Group Publishing.
This chapter appears in the book, Ethical Issues of Information Systems by Ali Salehnia. Copyright © 2002, IRM Press, an imprint of Idea Group Inc.

"target" of the media, with the standard approach being to present the image of either a "teenage whiz kid" or an insidious threat. In reality, it can be argued that there are different degrees of the problem. Some hackers are malicious, while others are merely naive and hence do not appreciate that their activities may be doing any real harm. Furthermore, when viewed as a general population, hackers may be seen to have numerous motivations for their actions (including financial gain, revenge, ideology or just plain mischief making). However, in many cases it can be argued that this is immaterial as, no matter what the reason, the end result is some form of adverse impact upon another party.

Steven Levy's book *Hackers: Heroes of the Computer Revolution* (1984) suggests that hackers operate by a code of ethics. This code defines main key areas:

- Hands-on imperative: Access to computers and hardware should be complete and total. It is asserted to be a categorical imperative to remove any barriers between people and the use and understanding of any technology, no matter how large, complex, dangerous, labyrinthine, proprietary, or powerful.
- "Information wants to be free." This can be interpreted in a number of ways. Free might mean without restrictions (freedom of movement = no censorship), without control (freedom of change/evolution = no ownership or authorship, no intellectual property), or without monetary value (no cost).
- Mistrust of authority. Promote decentralization. This element of the ethic shows its strong anarchistic, individualistic, and libertarian nature. Hackers have shown distrust toward large institutions, including, but not limited to, the state, corporations, and computer administrative bureaucracies.
- No bogus criteria: Hackers should be judged by their hacking, not by "bogus criteria" such as race, age, sex, or position.
- "You can create truth and beauty on a computer." Hacking is equated with artistry and creativity. Furthermore, this element of the ethos raises it to the level of philosophy.
- Computers can change your life for the better. In some ways, this last statement really is simply a corollary of the previous one. Since most of humanity desires things that are good, true, and/or beautiful.

During the 1980s and 1990s this pure vision of what hackers are was changed by the development of new groups with various aims and values. Mizrach (1997) states that the following individuals exist in cyberspace:

- Hackers (Crackers, system intruders)–These are people who attempt to penetrate security systems on remote computers. This is the new sense of the term, whereas the old sense of the term simply referred to a person who was capable of creating hacks, or elegant, unusual, and unexpected uses of technology.
- Phreaks (phone phreakers, blue boxers)–These are people who attempt to use technology to explore and/or control the telephone system.