Hackers and Cyber Terrorists

M. J. Warren
Deakin University, Australia

INTRODUCTION

Many aspects of our modern society now have either a direct or implicit dependence upon information technology (IT). As such, a compromise of the availability or integrity in relation to these systems (which may encompass such diverse domains as banking, government, health care, and law enforcement) could have dramatic consequences from a societal perspective.

In many modern business environments, even the short-term, temporary interruption of Internet/e-mail connectivity can have a significantly disruptive effect, forcing people to revert to other forms of communication that are now viewed as less convenient. Imagine, then, the effect if the denial of service was over the longer term and also affected the IT infrastructure in general. Many governments are now coming to this realization.

This article sets out to consider the scenario in which technology infrastructures or services are targeted deliberately, examining the issue in relation to two categories of computer abuser: 'hackers' and 'cyber terrorists.'

The Computer Hacker

The definition of the 'computer hacker' has been the subject of much debate in computing circles. Caelli, Longley, and Shain (1989) provide two definitions of the term:

1. In programming, a computing enthusiast. The term is normally applied to people who take a delight in experimenting with system hardware (the electronics), software (computer programs) and communication systems (telephone lines, in most cases).
2. In data (information) security, an unauthorized user who tries to gain entry into a computer, or computer network, by defeating the computers access (and/or security) controls.

In mass media terms, the latter interpretation is by far the more common (although persons belonging to the former category of hacker would seek to more accurately define the latter group, particularly those with a malicious intent, as 'crackers').

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 '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 naïve 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) (Parker, 1976). 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 (1994) book *Hackers: Heroes of the Computer Revolution 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 Authority:** Promote decentralization. This element of the ethic shows its strong anarchis-

tic, 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. It was certainly true that at this time hackers certainly saw themselves as cyber Robin Hoods whose motives for hacking certainly outweighed any law that they may have been breaking.

Mizrach (1997) states that the following individuals currently 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.
- **Virus Writers** (also, creators of Trojans, worms, logic bombs): These are people who write code which (a) attempts to reproduce itself on other systems without authorization and (b) often has a side effect, whether that be to display a message, play a prank, or destroy a hard drive.
- **Pirates:** Originally, this involved breaking copy protection on software. This activity was called 'cracking'. Nowadays, few software vendors use copy protection, but there are still various minor measures used to prevent the unauthorized duplication of software. Pirates devote themselves to thwarting these and sharing commercial software freely.
- **Cypherpunks** (cryptoanarchists): Cypherpunks freely distribute the tools and methods for making use of strong encryption, which is basically unbreakable except by massive supercomputers. Because American intelligence and law enforcement agencies, such as the NSA and FBI, cannot break strong encryption, programs that employ it are classified as munitions—thus, distribution of algorithms that make use of it is a felony.
- **Anarchists:** They are committed to distributing illegal (or at least morally suspect) information, including but not limited to data on bomb making; lock picking; pornography; drug manufacturing; and radio, cable, and satellite TV piracy.
- **Cyberpunk:** Usually some combination of the above, plus interest in technological self-modification, science fiction, and interest in hardware hacking and 'street tech'.

Mizrach (1997) determined that new groupings with cyberspace had altered the initial code of ethics, and that the code of ethics in the 1990s was more concerned with:

- **"Above all else, do no harm":** Do not damage computers or data if at all possible.
- **Protect Privacy:** People have a right to privacy, which means control over their own personal (or even familial) information.
- **"Waste not, want not":** Computer resources should not lie idle and wasted. It is ethically wrong to keep people out of systems when they could be using them during idle time.
- **Exceed Limitations:** Hacking is about the continual transcendence of problem limitations.
- **The Communication Imperative:** People have the right to communicate and associate with their peers freely.
- **Leave No Traces:** Do not leave a trail or trace of your presence; do not call attention to yourself or your exploits.
- **Share:** Information increases in value by sharing it with the maximum number of people. *Don't hoard, don't hide!*
- **Self-Defense Against a Cyberpunk Future:** Hacking and viruses are necessary to protect people from a possible Orwellian *1984* future.