Chapter XXXIV
The Ethics of Deception in Cyberspace

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

ABSTRACT

We examine the main ethical issues concerning deception in cyberspace. We first discuss the concept of deception and survey ethical theories applicable to cyberspace. We then examine deception for commercial gain such as spam, phishing, spyware, deceptive commercial software, and dishonest games. We next examine deception used in attacks on computer systems, including identity deception, Trojan horses, denial of service, eavesdropping, record manipulation, and social engineering. We then consider several types of deception for defensive purposes, less well known, including honeypots, honeytokens, defensive obstructionism, false excuses, deceptive intelligence collection, and strategic deception. In each case we assess the ethical issues pro and con for the use of deception. We argue that sometimes deception in cyberspace is unethical and sometimes it is ethical.

INTRODUCTION

Deception is a ubiquitous human phenomenon (Ford, 1996). As the Internet has evolved and diversified, it is not surprising to find increasing deception in cyberspace. The increasing range of Internet users in particular, and the development of Internet commerce, has provided many opportunities and incentives.

Deception is a technique for persuading or manipulating people. We will define deception as anything to cause people to have incorrect knowledge of the state of the world. This includes lying but also misleading. Deception in cyberspace can be used both offensively (to manipulate or attack computer systems, networks, and their users) or defensively (to defend against manipulations or attacks). Most ethical theories proscribe most forms of deception while permitting some kinds (Bok, 1978). Deception smooths social interactions, controls malicious people, and enables doing something for someone's unrecognized benefit

(Nyberg, 1994). The harms of deception are the failure to accomplish desired goals, and the often long-term damage to the trust necessary to sustain social relationships, without which much human activity could not be accomplished.

(Quinn, 2006) provides a useful categorization of ethical theories applicable to computer technology. He identifies subjective and cultural relativism, divine-command theory, Kantian rule-based ethics, social-contract theory, and act and rule utilitarianism. Subjective relativism, cultural relativism, and divine-command theory do not fit well with cyberspace because cyberspace is a social resource that spans diverse cultures with diverse opinions, and it needs cooperation to work properly. Kantian rule-based ethics is difficult to apply in general, though it helps resolve specific issues. Social-contract theory is useful but may not provide specific enough guidance to resolve a particular ethical dilemma. Alternative formulations to cyberethics such as the "disclosive" approach of (Brey, 2000) can also be explored but they are relatively new.

That leaves utilitarianism, which attempts to decide ethical questions by assessing the net benefit to society of a particular act or ethical rule. So we will follow a utilitarian approach here, and rule utilitarianism in particular. We shall say a particular policy of deception is ethical if its net of benefits minus costs, in general to a society in the long term, exceeds that of not deceiving, else it is unethical (Artz, 1994). Benefits include achieving the goals of the deceiver and the value of those goals. Costs include the direct damage caused by the deception as when its goals are malicious, direct costs of the deception being discovered such as retaliation, and indirect costs of discovery such as increased distrust of the parties. In cyberspace for instance, if someone is attacking your computer, a deception that could make them go away could be justified if the cost of a successful attack on the computer is hours of work to reinstall the operating system and damaged files. Both benefits and costs must be multiplied by probabilities to obtain expected values when they are uncertain due to such factors as whether the deception will succeed or whether it will be discovered.

BACKGROUND

Deception can be verbal or nonverbal (Vrij, 2000). Verbal methods include outright lying, equivocation, failing to state key information, false claims, and false excuses. Nonverbal methods include mimicry, decoying, and various nonverbal forms of pretense. People use deception everyday without being aware of it, and many areas of human activity could not function without deliberate deception such as police work, law, politics, business negotiation, military actions, and entertainment. Much deception as practiced is unjustified, however. Hence there is an extensive literature on detection of deception (Vrij, 2000). Human deceivers try to control the information they reveal, but it is hard to control all the channels of communication, and the truth often "leaks out" through secondary channels. For instance, people who lie tend to fidget, hold their bodies rigidly, and use an unusual tone of voice. Deception can also be detected in verbal utterances from the use of vagueness, exaggeration, high frequency of negative terms, and especially inconsistency between different assertions. But deception detection is difficult in general, and attempts to build automated "lie detectors" have not been very successful.

Cyberspace is well suited for many forms of deception because of the difficulty of obtaining collaborating information when assertions are made (Fogg, 2003). For instance, a policeman can pretend to be a 14-year-old girl online to entrap pedophiles. At the same time, a "phisher" can pretend to be a bank by implementing a fake Web site to steal personal data from victims. In addition, the connectivity of the Internet enables social interactions over long international distances,