CYBER-TRACKING: INTERPRETING A FIVE LEVEL MODEL OF BEHAVIOR IN CYBERSPACE

Charles W. Jaeger, Southern Oregon University, Ashland OR 97520, 541-552-6714, jaeger@sou.edu

ABSTRACT

The Internet extends human communication to almost everywhere, 24/7, and the variety of content is astonishing. Ordinary Internet users are in the majority, but hackers, crooks, bullies, criminals, and terrorists all share time in cyberspace. This paper discusses models that attempt to make sense of it all, including a five-level model designed to capture all activity in cyberspace.

INTRODUCTION

The model is designed to help us think systematically about the seemingly chaotic world around us. A model's value is determined by how much it explains, how precisely, and how well we can interpret operational direction with validity and reliability. Can we make a model that captures all activity in cyberspace? Yes. Will it be precise? Maybe. Will it be useful? Yes, if it explains more than we knew before.

The five-level model presented in this paper interprets behavior in cyberspace, providing a means to count events, analyze them, and form a basis to plan productive interventions through decision science. Other models may not capture as much. Thus, we can benefit from considering a more complete model.

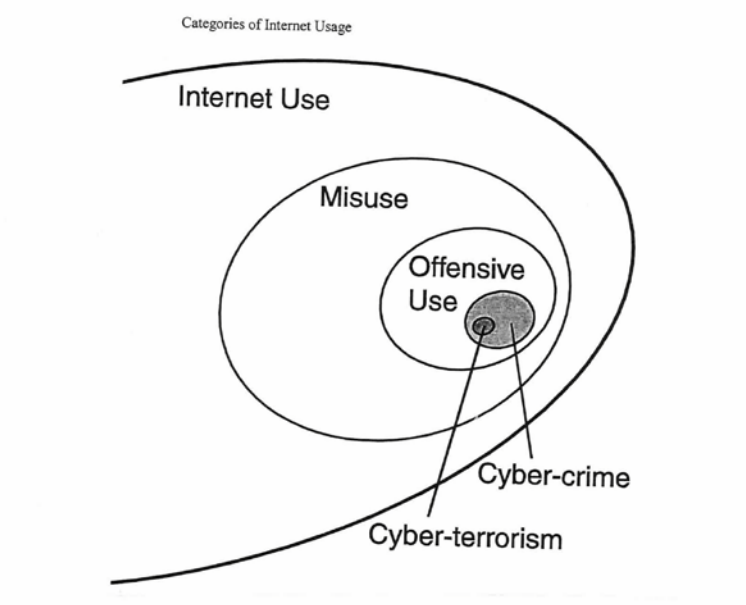
MODEL DEVELOPMENT

Tavari [5], Spinello [4], Denning [2], and others have separated cyberspace activities into variations of subsets from a philosophical, ethical, or moral problems perspective. Activities include cybervandalism, cybertrespass, and cyber-piracy, or activism, hacktivism, and cyberterrorism. However, these are not complete in pursuing ways to formulate marketing questions. Conway [1] formulated a three level model designed to capture "fringe" activity on the Internet, and included normal usage as the baseline measurement. Other categories were misuse, and offensive use. Jaeger [3] expanded this general schema to include cybercrime and cyberterrorism in a complete five-level model that can be the basis for counting, analyzing, and interpreting reasoned decisions about activities in cyberspace.

Table 1: interpreting behavior in cyberspace

Category	Description	Examples
Use	normal and legal Internet usage	surfing; email; messaging; e-commerce
Misuse	acts that disrupt or otherwise compromise other sites, including protests and vandalism	hacking pornography onto an enemy's Web site; adding political slogans
Offensive use	actual damage, theft, fraud, extortion, or commercial espionage that are not crimes or that cannot practically be prosecuted	hacking into celebrities' medical records for curiosity and public dissemination
Cybercrime	criminal acts that can be prosecuted	hacking bank databases to commit identity theft for profit
Cyberterrorism	crimes with political motivations	hacking SCADA systems (supervisory control and data acquisition) to open dam spillways or disable electrical grids

(see Figure 1 for a graphic model)



The five-level model has been useful in teaching about activity in cyberspace. Are there instances where the model definitions cannot precisely place an act in a category? Yes, but that is the nature of behavioral models. Does that make the model bad? No—as long as the model is helpful in interpreting reasoned decisions.

For example, unauthorized entry into a Web site, depending on what comes next, could be categorized as misuse (malicious but harmless), or offensive (damaging, but not prosecutable), or criminal, or it could be a terrorist act. The model categories help us count them, analyze them, and develop strategies for appropriate action.

In addition to teaching about behavior in cyberspace, Internet service providers, security software developers, and other Internet watchdog organizations may benefit from the five-level model. For example, Carnegie Mellon's CERT® facility studies internet security vulnerabilities, researches network changes in security systems, and develops information and training to help improve security. Additional levels of behavior would add richness.

The five-level model raises other interesting questions. For example, is it something more than ordinary use if you are not actively engaged in misuse or offensive use, but you are communicating with others with the intent to help them plan and coordinate misuse or offensive use? Those two distinct types of behavior merit further discussion.

REFERENCES

[1] Conway, M. (2002). Reality bytes: Cyberterrorism and terrorist "use" of the Internet. *First Monday, 7(11).* Retrieved December 20, 2002, from http://firstmonday.org/issues/isssue7_11/conway.

[2] Denning, D. (1999). "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy." Retrieved September, 2004. Denning's work can be found at: http://www.cs.georgetown.edu/~denning/publications.html

[3] Jaeger, C. (2006). "Cyberterrorism and Information Security." *The handbook of Information Security.* Hoboken, NJ: John Wiley & Sons.

[4] Spinello, R. (2010). *Cyberethics: Morality and Law in Cyberspace,* 4th Edition. Burlington, MA: Jones and Bartlett Publishers, Inc.

[5] Tavani, H. (2004). *Readings in CyberEthics,* 2nd Edition. Burlington, MA: Jones and Bartlett Publishers, Inc.