Chapter 11
Social Dynamics and the Future of Technology-Driven Crime

Max Kilger
Honeynet Project, USA

ABSTRACT

The future paths that cybercrime and cyber terrorism take are influenced, in large part, by social factors at work in concert with rapid advances in technology. Detailing the motivations of malicious actors in the digital world, coupled with an enhanced knowledge of the social structure of the hacker community, will give social scientists and computer scientists a better understanding of why these phenomena occur. This chapter builds upon the previous chapters in this book by beginning with a brief review of malicious and non-malicious actors, proceeding to a comparative analysis of the shifts in the components of the social structure of the hacker subculture over the last ten years, and concluding with a descriptive examination of two future cybercrime and national security-related scenarios likely to emerge in the near future.

INTRODUCTION

Some Opening Comments on the Future of Cybercrime and Cyber Terrorism

The future of cybercrime and cyber terrorism is not likely to follow some monotonic, simple deterministic path. The complex interplay of technology and social forces, as demonstrated in the previous chapters, reveals that this outcome will be anything but straightforward. However, this reality does not mean that through a better understanding of the social relationships between technology and humans, we cannot influence, at least partially, that future. In particular, social scientists have accumulated a significant body of knowledge on how various types of social processes--such as sentiment, status, social control and distributive justice, just to name a few – operate and interact to form our social world. We are now just beginning to gain a better understanding of how these processes are altered through the catalyst of digital technologies.

DOI: 10.4018/978-1-61692-805-6.ch011

It is hoped that through this understanding, we will build a better foundation from which to suggest how cybercrime and cyber terrorism may evolve over time. As social scientists, we have an obligation to share this understanding with others and, in particular, with our counterparts in the computer science and Information Technology (IT) security fields. These scientists and professionals approach the issues of cybercrime and cyber terrorism from a technological perspective, attempting to devise algorithms, encryption, authentication techniques, and strategic security platforms to protect networks and information systems from intrusion, data theft, and intentional damage. While many of these IT security researchers were initially resistant to considering bodies of knowledge outside of the traditional hard sciences, in the past five years there has been a shift in thought, reflecting a willingness to bring social science knowledge and research into consideration in their thinking. This recent change has also benefited social science researchers interested in people, technology, and issues such as cybercrime and cyber terrorism, because it has purposely exposed social scientists to IT scientists and their knowledge of technical systems and strategies.

Historically, the landscape of the IT security battlefield has been filled with technological weapons and defenses. Computer network defenders typically deploy a panoply of software and hardware tools--including (i) firewalls that restrict and control TCP/IP address and port traffic, (ii) intrusion detection systems that look for suspicious network traffic and unexpected program behavior, and (iii) anti-viral/spyware applications that scan files and memory for known virus signatures and exploits. IT security professionals spend a good deal of their time conducting very technical forensic analyses of compromised computer systems and attempting to reverse- engineer worms and other malware to see what their purpose and intended actions might be. The strategic nature of these efforts to defend computer networks and servers has typically almost always been reactive and from a temporal aspect, post hoc. IT security professionals normally have to wait until an exploit or threat has been uncovered before they can examine the threat and take preventative action.

The most common exception to this situation is when a security vulnerability in an application or operating system component is uncovered by IT security professionals, and a preventative patch is created and applied to the appropriate systems before individuals with malicious intent discover the vulnerability and take advantage of it.

It is evident from the current state of the IT security environment that there are a number of serious deficiencies in the current strategies used to combat cybercrime and cyber terrorism. Continuously fighting malicious actors and agents from what is mostly a post hoc, defensive posture is likely neither the most desirable nor optimal arrangement. Developing a more theoretical understanding of the reasons why individuals or groups develop and deploy exploits and malware, on the other hand, is one important pathway likely to enable IT security researchers and professionals to begin to emerge from their historically defensive posture.

This Chapter's Approach

The theoretical and empirical lessons learned from the previous chapters of this book are both relevant and valuable components of this strategy. This chapter builds upon those chapters by beginning with a brief review of the motivations of malicious and non-malicious online actors, then proceeding to a comparative analysis of the shifts in the components of the social structure of the hacker subculture over the last decade. This chapter concludes with a descriptive examination of two future cybercrime and national security-related scenarios likely to emerge in the near future. It is hoped that by providing a better understanding of the social-psychological and cultural forces at work within the hacking community, a more forward-looking and proactive strategy toward