Chapter XI
Hacker Wars:
Cyber Warfare Previews

Richard Baskerville
Georgia State University, USA

ABSTRACT

This chapter develops an analytical framework for new forms of information warfare that may threaten commercial and government computing systems by using e-collaboration in new ways. The framework covers (a) a strategic model, (b) a strategic arena, (c) e-collaboration, and (d) ethics and law. The framework is then used to compare two recorded instances of major hacker wars that erupted in the shadow of kinetic conflicts. In both cases, the hacker war appears to have been a grassroots collaborative enterprise led by loosely organized civilians, with neither government control nor permission. Collaborating across networks to coordinate their attacks, such hacker wars can attack both government and commercial computer networks without warning. The analysis shows how hacker wars demonstrate characteristics found in the frameworks, and that there are forms of e-collaboration that represent a potentially difficult new source of threat for globalized information systems.

INTRODUCTION

The collaborative use of computing, or e-collaboration, uses computers to support the coordination and cooperation of groups of people in order to perform a task or solve a problem (Bafoutsou & Mentzas, 2002). Building on work in virtual teams, the development of e-collaboration represents advances in virtual reality in the sense that virtual workplaces for work groups are often involved (Rutkowski, Vogel, Genuchten, Bemelmans, & Favier, 2002). The application of e-collaboration in most circumstances is a constructive activity: Teams of people using technology to develop work products, coordinate their activities, and communicate their knowledge. The use of information and communications technologies for e-collaboration extends beyond the workplace and into the public arena.

The widespread public availability of ICT makes it possible for grassroots and voluntary e-collaboration to make myriad positive contributions to the welfare of people anywhere in the world. Some computer conferencing tools are widely and near-freely available, such as NetMeeting and BSCW. Trends to make this technology available for public service are in sight. For example, organizations and the general public used ICT in many formal and informal ways to coordinate the relief efforts for the tsunami disaster of 2004 (Hempel, 2005).

We should not overlook, however, the dark-side potential of voluntary and public e-collaboration when used, however well intentioned, for coordinating and collaborating in attacks upon computing resources belonging to others. There are myriad sources of threats for commercial information systems today. These wellsprings of hazards include natural disasters, criminals, vandals, and that most human of all threats, human error (Baskerville, 1996; Im & Baskerville, 2005). With the advent of widespread public networking (the Internet), all of these threat sources have become real-time threats. Many, if not most, information systems are vulnerable through their network connections to all of these threat sources. Information security risk managers must appraise the risks to their systems from each of these sources. The task is growing more complex and extensive as our networks and computer systems grow more complex and extensive (Cronin & Crawford, 1999).

The value of information within the context of warfare is certainly nothing new, and has been recognized for millennia:

Thus, what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge. (Sun Tzu, 1995, p. 90)

However, electronic improvements to the use of information within warfare have been evolving over the past century. The original version was known as electronic warfare and regarded the control of the electromagnetic spectrum in military action (Armistead, 2004). To a degree, information warfare arises from electronic warfare and entails actions to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage over an adversary (Alger, 1996). Information warfare may be critical in the opening phases of any military offensive (Bishop, 2006). Because information warfare encompasses perception management, it is closely related to the struggle to win the hearts and minds of the population. Brutal experience has shown that the information war can be more significant for victory than the armed confrontation that accompanies it (Sturges, Katjihingua, & Mchombu, 2005).

Warfare and terrorism currently lie on the distant horizon as a source of threat to commercial information systems. The central focus of concern for warfare as a source of risks for commercial systems have been directed mostly at those commercial systems concerned with national critical infrastructures. Risk planners are assuming that warfare or terrorist strategies would attack commercial computer systems only as a means to disrupt essential services such as energy, transportation, communications, and so forth (The President's Commission on Critical Infrastructure Protection, 1997). Little concern has been expressed for warfare or terrorism strategies directed at the destruction or disruption of commercial computing per se (Furnell & Warren, 1999).

In this chapter, we explore risks that arise from the use of e-collaborative technologies for the purposes of warfare and terrorist strategies aimed at disrupting or destroying commercial computing capacity as an end rather than as a means. We will explore cases that involved both random and strategically formulated attacks on widespread commercial and government computing facilities. We select perhaps the most interest-