IDEA GROUP PUBLISHING **ITJ3014**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This chapter appears in the publication, *International Jouranl of e-Collaboration*
edited by Ned Kock © 2006, Idea Group Inc.

Hacker Wars:
E-Collaboration by Vandals and Warriors

Richard Baskerville, Georgia State University, USA

ABSTRACT

This article 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 (1) strategic model, (2) strategic arena, (3) e-collaboration, and (4) ethics and law. The framework then is 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 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.

Keywords: electronic collaboration; globalization of IS; hacker; IS risk management; IS security; security management; security risk

INTRODUCTION

Collaborative use of computing, or e-collaboration, uses computers to support 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 often are 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 (ICT) for e-collaboration extends beyond the work place 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 almost 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 the dark-side potential of voluntary and public e-collaboration when used, however well-intentioned, for coordinating and collaborating in attacks on 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 human error, the most human-of-all threats (Baskerville, 1996). 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).

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 risk for commercial systems has been directed mostly at those commercial systems concerned with national critical infrastructures. Risk planners are assuming that warfare or terrorist strategies will attack only commercial computer systems 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 article, we explore risks that arise from the use of e-collaborative technologies for the purpose 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 interesting and well-known cases of such destruction — the eruption of hacking warfare among nations in the shadow of military confrontations, shooting wars, and other material conflicts. For our purposes, we will distinguish between cyber wars and kinetic wars. We will define cyber wars as computer and computer