Chapter 9
Cyber Conflict as an Emergent Social Phenomenon

Dorothy E. Denning
Naval Postgraduate School, USA

ABSTRACT

This chapter examines the emergence of social networks of non-state warriors launching cyber attacks for social and political reasons. It examines the origin and nature of these networks; their objectives, targets, tactics, and use of online forums; and their relationship, if any, to their governments. General concepts are illustrated with case studies drawn from operations by Strano Net, the Electronic Disturbance Theater, the Electrohippies, and other networks of cyber activists; electronic jihad as practiced by those affiliated with al-Qa'ida and the global jihadist movement associated with it; and operations by patriotic hackers from China, Russia, and elsewhere.

INTRODUCTION

Warfare is inherently social. Soldiers train and operate in units, fighting and dying for each other as much as for their countries. Cyber conflict is also social, but whereas traditional warriors work and socialize in physical settings, cyber warriors operate and relate primarily in virtual space. They communicate electronically and meet in online forums, where they coordinate operations and distribute the software tools and knowledge needed to launch attacks. Their targets are electronic networks, computers, and data.

DOI: 10.4018/978-1-61692-805-6.ch009

The Emergence of Cyber Conflict, or Hacking for Political and Social Objectives

Although conflict appears throughout human history, its manifestation in cyberspace is a relatively recent phenomenon. After all, digital computers did not appear until the 1940s, and computer networks until the 1960s. Attacks against computers and the data they held emerged in the late 1950s and early 1960s, but they were perpetrated more

for money and revenge than as an instrument of national and international conflict. Typical crimes included bank fraud, embezzlement, information theft, unauthorized use, and vandalism (Parker, 1976). Teenage hacking arrived on the scene in the 1970s, and then grew in the 1980s, as young computer users pursued their desire to explore networks, have fun, and earn bragging rights. By the end of the decade, the single biggest attack on the Internet was a computer worm launched by a college student simply as an experiment. Within this mix of playful hacking and serious computer crime, cyber conflict, or hacking for political and social objectives, emerged, taking root in the 1990s and then blossoming in the 2000s. Now, it accounts for a substantial share of all cyber attacks, as well as some of the highest profile attacks on the Internet, such as the ones perpetrated by patriotic Russian hackers against Estonia in 2007 and Georgia in 2008.

The Hacker Group Phenomenon

From the outset, hackers and cyber criminals have operated in groups. In his examination of early computer-related crime, Donn Parker found that about half of the cases involved collusion, sometimes in groups of six or more (Parker, 1976, p. 51). Youthful hackers met on hacker bulletin boards and formed clubs, one of the earliest and most prestigious being the Legion of Doom (Denning, 1999, p. 49), while serious criminals formed networks to traffic in cyber crime tools and booty, such as stolen credit cards. Today, there are perhaps tens or hundreds of thousands of social networks engaging in cyber attacks. While many of these networks were formed for fun or financial gain, others arose for the purpose of engaging in cyber conflict. Individuals, often already connected through hacker groups or other social networks, came together to hack for a cause.

The Purpose of This Chapter

This chapter examines the emergence of social networks of non-state warriors launching cyber attacks for social and political reasons. These networks support a variety of causes in such areas as human and animal rights, globalization, state politics, and international affairs. This chapter examines the origin and nature of these networks; their objectives, targets, tactics, and use of online forums. It also describes the relationship, if any, to their governments.

THE NATURE OF NON-STATE NETWORKS

Unlike states, non-state networks of cyber soldiers typically operate without the constraints imposed by rigid hierarchies of command and control, formal doctrine, or official rules and procedures. Instead, they operate in loosely-connected networks encouraging and facilitating independent action in support of common objectives--what is sometimes characterized as "leaderless resistance."

However, while the networks are decentralized, they are not actually leaderless. A few individuals, often already connected outside cyberspace or from previous operations, effectively take charge, or at least get things started. They articulate goals and strategy, plan and announce cyber attacks, encourage people to participate, and provide instructions and tools for participating. They manage the online forums--websites, web forums and groups, discussion boards, chat rooms/channels, email lists, and so forth--supporting network activities. They also develop or acquire the automated software tools used by the group. Often, the tools themselves give the leaders some control over the conduct of cyber attacks (e.g., selection of targets and rate of attack), compensating for the lack of a hierarchical command structure over the network players.