CHAPTER 1

INTRODUCTION

The Birth of Cyber Warfare

Cyber warfare did not begin with the construction of the Internet. Cyber warfare (CW) really finds its roots in hacking. To understand CW, hacking must be understood first. “Hacking” and “hacker” have become terms that most people associate with talented computer programmers who have learned to exploit systems that the average person does not completely understand. But, the term hacker pre-dates the emergence of the silicon chip based computers most people are currently familiar with.

> In the late 1950s, the MIT model railroad club was given a donation of parts, mostly old telephone equipment. The club’s members used this equipment to rig up a complex system that allowed multiple operators to control different parts of the track by dialing in to the appropriate sections. They called this new and inventive use of telephone equipment *hacking*; many people consider this group to be the original hackers. (Erickson 2008, 2)

The hacker culture stayed with telephone equipment as their medium of choice through the 1980s. The Bell phone networks became a target for hackers who specifically called themselves phone phreaks (Goldstein 2009, xxxvii). Early phone phreaks would whistle a sound at 2600 hertz into a telephone, which the system would recognize and allow access to the long distance phone network (Goldstein 2009, xxxvii). The phone phreak would then have access to the entire system the way an operator would (Goldstein 2009, xxxvii). This iconic frequency has become the title of one of the more influential hacker publications titled simply: 2600. Steve Jobs and Steve Wozniak were some of these early hackers exploring the phone networks and tricking the system into doing what they wanted (Wozniak 2006, 103).

As home computers began to emerge in the 1980s, hackers began to explore their potential and possibilities. The most recognizable early instance of this in popular culture was the movie “War Games.” In this movie, the main character uses his computer and the phone networks to enter into a military computer and wreak havoc. There is also a scene in this movie where the main character hacks a pay phone to make a free long distance call.

With the advent of the computer in homes, hackers began to learn more and more about computer code. This is essentially where the skill of the hacker lies today. The concept of modern hacking is quite simple. Exploit errors or loopholes in a computer system’s operating code thus allowing access to and manipulation of the system. Early hackers seemed more concerned with what could be done rather than hacking a system to get something from that system (Erickson 2008, 1). The possibilities of hacking became obvious very quickly as government, financial, educational, and security systems became more connected in the 1980s to promote efficiency of information transfer. In the 1990s the Internet granted the public unprecedented access to a variety of networks for financial transactions, communication, and commerce. Hackers quickly began to categorize themselves into different groups based on different goals. Hackers who are oriented towards increasing security and testing systems so that they might be strengthened called themselves White Hat Hackers. Those more criminally minded were termed Black Hat Hackers. And, of course those that dabble in both became Grey Hat Hackers.

The hacker community continued to grow throughout the 1980s and 1990s. Hacking became more public with the advent of malicious code in the form of viruses and software (malware). As people began to use the Internet more and more, personal

CYBER WARFARE: ARMAGEDDON IN A TEACUP?

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

BRADLEY L. BOYD, MAJOR, USA
B.A., University of California, Irvine, California, 1996

Fort Leavenworth, Kansas
2009-02

Approved for public release; distribution is unlimited.

computers began to be affected. Self Replicating Computer Viruses had been present since the early 1970s, but mainstream citizens did not take notice until the Happy99 worm and the ILOVEYOU worm appeared in the 1990s. These worms had global effects that reached the lives and systems of everyday citizens. This self replicating global reach signals the start of real concern about a strategic level attack capable of striking throughout the globe, paralyzing systems, and preventing the flow of accurate information. People and governments started to fear computer hackers and their potential to disrupt systems that governments and economies relied on. Governments started to worry that if a single hacker can wreak havoc with an ILOVEYOU worm, then what could a nation accomplish with the full weight of national spending. In the late 1990s CW appeared to be a viable way to disrupt other nations, though how and to what extent were unclear.