Chapter 88
Cyber Warfare

Ralph D. Berenger
American University of Sharjah, UAE

ABSTRACT

This entry explores the difficulty of defining precisely cyber warfare, of determining the motives behind cyber attacks, and reviews the history of cyber warfare that extends back to the creation of cyberspace itself, while looking at future international research and policy implications. The introduction grapples with defining cyber warfare and its distinction from cyber war. It traces the etymology of the concept to the unlikely confluence of science fiction writers, 1960's radicals, and current experts in the field, many of them former anti-establishment cyber warriors themselves. The next section synthesizes the literature and highly publicized examples of cyber warfare in recent years. The following segment reviews the responses of governments to cyber warfare, and finally, it looks at future implications for policymakers.

INTRODUCTION

Cyber warfare. The phrase evokes computer board games displayed on a massive screen where outcomes are settled, not by the most blood and materiel shed over geo-strategic superiority, but by which side or ideology grabs and holds a tactical advantage over information in the fifth domain. It's the stock and trade of science fiction writers about how future civilizations and its disaffected populations will settle disputes and secure power over the other. The future is now. In response to accelerating anonymous computer-based attacks on business and governmental facilities from 2003-2011, the U.S. military, in a mid-2011 policy shift, now considers cyber attacks on America's infrastructure as *jus ad bellum* (the right to wage war). Left unclear, perhaps purposefully, was exactly how that "right" would be exercised.

Like "democracy" and "terrorism," "cyber war" is an abstraction that is difficult to define precisely. Some authors try to narrow the phrase's meaning to "actions by a nation state to penetrate another nation's computers for the purpose of

DOI: 10.4018/978-1-4666-0315-8.ch088

causing damage or disruption" (Clarke & Knake, 2010), but that definition does not consider rogue players representing non-governmental interests.

The Economist (2010) called cyber warfare aggression in the "fifth domain"—the others being land, sea, air and space—which the U.S. Defense Department formally recognizes. Others have acknowledged in their definition the role of unsophisticated amateurs, non-state actors and mischief-makers, who can do as much harm and cause sufficient chaos to be taken seriously as unaligned cyber warriors (U.S. Joint Forces Command, 2010). Many authors and scholars lean toward an "I-know-it-when-I-see-it" stance. In this entry, cyber warfare is defined as the asymmetrical aggressive actions to exploit existing digital communication technology in the fifth domain to illegally and surreptitiously access, record, or modify computer programs, systems or networks for surveillance, disruption, disarmament, or destruction of critical information for political or military reasons. Note that prosecuting warfare by a machine in a language recognized only other machines in an unseen place with unlimited space sounds like science fiction, and that is where the ideas that spawned a generation of hackers evolved.

Early experts in the field of cyber warfare and digital disruption of information flows were science fiction writers, principally William Gibson and Bruce Sterling, along with Pat Cadigan, Rudy Rucker, Lewis Shiner, and John Shirley created the cyberpunk culture in their writings, and developed neologisms such as *cyberspace*, *cyber war* and *cyber warfare*. But the antecedent of those expressions—*cyber*—has origins that can be traced to at least the 18th Century and has Greek roots. The use of machines and the imagined dependency on computers was also a recurring theme of the late Kurt Vonnegut, an anti-establishment icon, whose writing career overlapped the counter-culture movement of the 1960's. The merger of man and machine, *cybernetics*, was defined by Norbert Wiener of Harvard University, in his 1948 book of that title, as the study of control and communication (Wiener, 1948).

The current leading researchers in cyber warfare include Richard Clarke, co-author of *Cyber War: The next threat to national security and what to do about it* (Clarke & Knake, 2010), a former national security official in the White House for three administrations, and chairman of Good Harbor Consulting, a security and risk management consultancy for governments and corporations; William J. Lynn III, deputy secretary of defense, and author of a number of position papers on the U.S. cyber defense status (Lynn, 2010, 2011); Marcus Ranum, an early innovator in Internet security technology and chief security officer for Tenable Network Security, a faculty member of the Institute for Applied Network Security and author of *The Myth of Homeland Security* (Ranum, 2003); Jeffery Carr, founder and CEO of Taia Global, advisor on security to the U.S. Defense Department and NATO, and author of *Inside Cyber Warfare* (Carr, 2010); Raymond C. Parks and David P. Duggan, senior members of the technical staff of Sandia National Laboratories in Albuquerque, New Mexico, whose *Principles of Cyber-Warfare* (Parks & Duggan, 2001), is required reading at the U.S. Military Academy at West Point; and Charles G. Billo, senior research associate, at the Institute for Security Technology Studies at Dartmouth College, who studied the motivations of selected nation states in cyber warfare (Billo & Chang, 2004).

OVERVIEW

Unlike *cyber warfare*, which is a continual an ongoing threat, the concept of *cyber war* is a topic of debate. Part of the problem of defining cyber war comes from a mish-mash of other terms such as cyber terrorism, hacking, cyber espionage, cyber crime, cyber identity theft, phishing and so forth. When does a hacker become a cracker—someone who electronically breaks into a supposedly