Chapter 15
China's Cyber Tool:
Striving to Attain Electronic *Shi*?

Timothy L. Thomas
United States Armed Forces (Retired), USA

ABSTRACT

This chapter analyses how China is using cyber reconnaissance to achieve electronic shi, defined as strategic advantage. It examines China's cyber strategy and information age advantages; Chinese financial and military cyber threats; China's hacker population; and Chinese organizations devoted to cyber defense. Once attained, electronic shi allows a country to "win victory before the first battle."

1. INTRODUCTION

Shi is an important strategic Chinese concept with roots as far back as Sun Tzu's classic *The Art of War*. One US source defines *shi* as the strategic configuration of power or advantage (Sawyer, 1994). A retired Chinese General, Tao Hanzhang, defines *shi* as "the strategically advantageous posture before a battle that enables it to have a flexible, mobile, and changeable position during a campaign" (Tao, 2007, 124). Another Chinese source, the book *Campaign Stratagems*, defines *shi* as the combination of the friendly situation, enemy situation, and the environment; as the sum of all factors impacting the performance of the operational efficiency of both sides; and as the key factor determining the rise and fall of operational efficiency (Zhang and Zhang, 2002).

The attainment of a strategic advantage is directly stated or implied in all of these definitions. Electronic *shi*, then, is the attainment of an electronic strategic advantage via cyber reconnaissance. US Defense Officials recognize Chinese attempts to realize electronic *shi* in

DOI: 10.4018/978-1-61520-831-9.ch015

today's digital environment. The US deputy undersecretary of defense for Asia-Pacific affairs, Richard Lawless, told Congress in 2007 that the Chinese military's "determination to familiarize themselves and dominate to some degree Internet capabilities—not only of China and that region of the world—provide them with a growing and very impressive capability that we are very mindful of and are spending a lot of time watching" (Tkacik, 2007).

Chinese computer specialists, primarily civilian hackers, have developed cyber tools to enhance their Internet capabilities to recon and attack foreign networks and websites. For the purposes of this chapter, the term "cyber tools" refers to software tools of a malicious nature, to include scanners, viruses, botnet controllers, and Trojans among other network reconnaissance and attack mechanisms (author's definition).

US analyst Phillip Saunders, who specializes in Chinese affairs, believes China uses its cyber tools to accomplish the following goals: secure inputs for its economy; protect against US containment strategies; expand China's political influence; and pursue commercial interests (Saunders, 2006). Like Saunders, other US analysts also believe the cyber tool has become an attractive option for Chinese security experts.

Chinese officials recognize the importance of attaining electronic *shi*. Xiong Guangkai, chairman of the China Institute for International Strategic Studies, stated in March 2009 that information and financial security are key elements of China's contemporary non-traditional security thinking (Liu, 2009). Xiong's comments are important. He was once the deputy chief of the People's Liberation Army (PLA) General Staff and a senior consultant to those making national policy. His inside knowledge of the Chinese system enables him to ascertain the national security issues of most probable concern to China's Communist Party leaders. Without control over these two elements, electronic *shi* will be difficult to attain.

1.1 Cyber Tools as a Means to Attain Strategic Advantage

China's cyber tools enable it to work toward attaining a strategic advantage or *shi*. Cyber, or computer-related, tools can deceive, influence, attack, defend, and conduct reconnaissance activities anonymously from strategic distances. They perform activities over the Internet as forces do on the ground but from distances and surreptitious postures that actual forces cannot achieve. To use the cyber tool effectively, China must conceive ways to manipulate cyberspace just as regular forces manipulate the military thought of opposing commanders. Cyber tools help uncover vulnerabilities in the digital files of other nation-states, vulnerabilities that could be manipulated in times of crises. Spotting vulnerabilities now could lead to China's "winning victory before the first battle" through the attainment of electronic *shi*.

Financial, economic, and information security issues have received increased attention from China's cyber personnel, and not in just a domestic sense. Chinese cyber reconnaissance personnel have allegedly been conducting very active searches in the financial and information files of several foreign governments. Attaining control over the levers of financial and information security would enable China to attain strategic cyber and perhaps overall strategic advantage without fighting.

China's use of its cyber tools during this historic opportunity differs from the US approach in several ways. First, Chinese strategists are investigating ways to integrate cyber tools with military concepts such as the thirty-six stratagems of war (Chinese Hacker Alliance, 2008). Packets of electrons, strategists recognize, can serve as stratagems that deceive or influence another country's cyber-event interpretations and responses. Take, for example, the stratagem "rustle the grass to startle the snake." China's strategists might want to use this stratagem to ascertain what type