INFORMATION WARFARE: BACK TO THE FUTURE

Chitra Kaul*
Research Scholar-Singhania University
chitrakaul@rediffmail.com

Dr. (Prof) BMK Prasad
Principal
(Dronacharya College of Engineering)

Divyanshu Sinha
Asstt Prof (Dronacharya College of Engg)
Divv4u@gmail.com

Abstract

"…attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence." The famous quote finds its roots to the celebrated text from ***Sun Tzu, written in 400-320 B.C.,with the apt title - The Art of War.*** *The most revered tactician of the world, Sun Tzu in his famous words in the China's most profound military classic quoted above, seems to be making a prophecy, which seems turning almost true in the present era. In tune with Sun Tzu's philosophy of winning without fighting, of destroying the enemy through tactical manipulation, and enlightened exploitation of strategic power, the People's Republic of China is a frontrunner in the arena of Cyber warfare. The Chinese were first to use cyber attacks for political and military goals, the reports date back to year 1997 and they undoubtedly are the first nation to leapfrog into the 21st century cyber warfare technology.[6]*

Keywords : Art of War, 36 Stratagems, Information Warfare, Cyberwar.

INTRODUCTION

Cyber-warfare, Also known as *cybernetic war* [1], or *cyberwar* is the use of computers and the Internet in conducting warfare in cyberspace [2].

The strategy of "avoiding fighting" dates back over 2000 years to the famous Chinese tactician, Sun Tzu. Still revered by Chinese military and political leaders alike, Sun Tzu advocated, **"To subdue the enemy without fighting is the acme of skill"**. Since China's military will take decades to match the US military in terms of technology and training, the concept of using information and cyber warfare to 'win without fighting' is quite appealing. Since the Chinese cannot possibly hope to fight on American terms, they must therefore find other means to deter or defeat the US."

The Chinese theory of non-contact warfare "seeks to attain a political goal by looking for auxiliary means beyond military boundaries or limits." Cyber warfare against civilian and military networks, particularly communications and logistics nodes, and information Computer network attacks include not only on disabling computer networks but also on corrupting information, sabotaging data, inserting false data, delaying the decision cycle, and convincing the adversary to doubt the security of the network. Thus, by a deliberate effort to penetrate a network (and allow the penetration to be discovered), the target may disable the network of their own accord to conduct security countermeasures and install upgrades. This effectively disables the network and conveniently makes use of the "killing with a borrowed sword" stratagem as well. By inserting false data or 'disinformation' into the network, the opponent will doubt the accuracy of all information and thus

will slow the decision cycle or stop using automated command and control tools altogether.

THE STRATAGEMS REDEFINED

A significant way the information age has affected China's attitude toward warfare is that China's 36 stratagems may find new meaning and application. Some 300 years ago an unknown scholar decided to collect and record China's stratagems. *The Thirty-Six Stratagems: The Secret Art of War* emphasizes deception as a military art that can achieve military objectives [15]. In the information age, which is characterized by anonymous attacks and uncertainty, the stratagem just might be revitalized as a tactic. It should be easier to deceive or inflict perception-management injuries (guidance injuries in Chinese) as a result. The information age is developing into the anonymous persuaders' age.

Some argue that in today's high-tech world, these ancient stratagems no longer apply. However, a look at just the first five stratagems shows otherwise. Strategy one is "fool the emperor to cross the sea"[16]. Lowering an enemy's guard must be an open act, hiding true intentions under the guise of everyday activities. An IW application would be using regular e-mail services or Internet business links to mask insertions of malicious code or viruses. Strategy two is "besiege Wei to rescue Zhao": when the enemy is too strong to attack directly, attack something he holds dear. Today's IW implication is that if you cannot hit someone with nuclear weapons because of catastrophic effects on your own country, then attack the servers and nets responsible for Western financial, power, political and other systems' stability with electrons. Strategy three is "kill with a borrowed sword": when you do not have the means to attack the enemy directly, attack using another's strength. The IW application is simple—sends viruses or malicious codes through a cutout or another country.

Strategy four is "await the exhausted enemy at your ease": choosing the time and place for battle is an advantage. Encourage the enemy to expend his energy in futile quests while you conserve your strength. When he is exhausted and confused, attack with energy and purpose. The IW application here is to use the people's war theory to send out multiple attacks while saving the significant attack until all the West's computer emergency response teams (CERTs) are engaged. Finally, strategy five is "loot a burning house": when a country is beset by internal conflicts, it will be unable to deal with an outside threat. The IW application is to put hackers inside the West under the guise of a student or business and attack from the inside. While chaos reigns, steal from information resources.

GLOBAL CONCERN

Jeff Green the senior vice president of McAfee Avert Labs was quoted as saying "Cybercrime is now a global issue. It has evolved significantly and is no longer just a threat to industry and individuals but increasingly to national security." They predicted that future attacks will be even more sophisticated. "Attacks have progressed from initial curiosity probes to well-funded and well organized operations for political, military, economic and technical espionage." [5] On first week of September 2007, The Pentagon and various French, German and British government computers were attacked by hackers of Chinese

origin. The Chinese government denies any involvement. [7] In the second week of April hackers hacked the Indian MEA computers. [8]

The report from McAfee says that China is at the forefront of the cyber war. China has been accused of cyber-attacks on India and Germany and the United States. China denies knowledge of these attacks. Arguments have been expressed regarding China's involvement indicating, in the methods of computer Hackers who use zombie computers; it only indicates that China has the most amounts of computers that are vulnerable to be controlled. [3]

In activities reminiscent of the Cold War, which caused countries to engage in clandestine activities, intelligence agencies are routinely testing networks looking for weaknesses. These techniques for probing weaknesses in the internet and global networks are growing more sophisticated every year. [4]

Cyber counterintelligence are measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions. [11]
The intelligence community is coming to grips with the challenge of cyber warfare intelligence. Much of the advanced infrastructure used in traditional warfare, like satellite imagery, is ineffective in the realm of cyber. New techniques and technologies are required for intelligence agencies to operate in this field. [12]

CASE STUDY – TITAN RAIN

A serious FBI and US army network compromise, involving customized Trojans to access highly classified data, was code named TITAN RAIN by US government. In Washington, officials remained tight-lipped about **Titan Rain**, insisting all details of the case are classified. But high-level officials at three agencies told TIME **the penetration was considered serious.** A federal law-enforcement official familiar with the investigation says the FBI "aggressively" pursued the possibility that **the Chinese government is behind the attacks.** Yet they all caution that they don't yet know whether the spying is official, a private-sector job or the work of many independent, unrelated hands. The law-enforcement source says **China has not been cooperating with U.S. investigations of Titan Rain**. China's State Council Information Office, speaking for the government, told TIME the charges about cyberspying and Titan Rain are "totally groundless, irresponsible and unworthy of refute." [14]

Despite the official U.S. silence, several government analysts who protect the networks at military, nuclear-lab and defense- contractor facilities tell TIME that **Titan Rain is thought to rank among the most pervasive cyberespionage threats that U.S. computer networks have ever faced**.

FUTURE TRENDS

To ascertain the seriousness of the issue, consider the following scenario. "The nuclear command systems today operate in an intense information battleground, on which more than 20 nations including Russia, China, and North Korea have developed dedicated computer attack programs. **These programs deploy viruses to disable**,

confuse, and delay nuclear command and warning processes in other nations. At the brink of conflict, nuclear command and warning networks around the world may be besieged by electronic intruders whose onslaught degrades the coherence and rationality of nuclear decision-making. The potential for perverse consequences with computer-launched weapons on hair-trigger is clear." [13]

CONCLUSION

The primary conclusion from a review of Chinese IW stratagems is that strategy, the military art and science of conducting campaigns on a broad scale, has undergone a transformation. Concentrations of forces will be replaced by striking efficacy with information and energy, and lines between front and rear will blur. Operations will switch from firepower to detecting, concealing, searching and avoiding, making long-range combat replace hand-to-hand fighting. A core issue will be the fight for network supremacy, which will be necessary to win in strategy and battle simultaneously.

REFERENCES

[1] Jonathan V. Post, "Cybernetic War," *Omni*, May 1979, pp.44-104, reprinted *The Omni Book of Computers & Robots*, Zebra Books, ISBN 0-8217-1276

[2] DOD, Cyberspace, http://www.dtic.mil/doctrine/jel/doddict/data/c/01473.html

[3] "China 'has 75M zombie computers' in U.S., http://www.upi.com/International_Security/Emerging_Threats/Briefing/2007/09/17/china_has_75m_zombie_computers_in_us/7394/

[4] Griffiths Peter, "World faces "cyber cold war" threat", Reuters, http://ca.news.yahoo.com/s/reuters/071129/tecnology/tech_britain_internet_col

[5] "Cyber Crime: A 24/7 Global Battle", Mcafee, http://www.mcafee.com/us/research/criminology_report/default.htm

[6] Cyber warfare resources and reference materials for Washington authorities, http://staff.washington.edu/dittrich/cyberwarfare.html

[7] Chinese Official Accuses Nations of Hacking, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/12.html

[8] MEA Computer Network Hacked, http://www.india-server.com/news/mea-computer-network-hacked-172.html

[11] DOD - Cyber Counterintelligence, http://www.dtic.mil/doctrine/jel/doddict/data/c/01472.html

[12] World Wide War 3.0, http://www.the-diplomat.com/article.aspx?aeid=3301 7-9 Oct 2008

[13] "A Succinct Cyber Crime Tour Meant To Illustrate By Way of Assorted Examples The Sort of Online Crimes Which Are Occurring -- And Why We Need More Cyber Crime-Trained Attorneys,"

http://www.uoregon.edu/~joe/tour/cybercrime.pdf

[14] "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)," Monday, **Aug. 29, 2005** http://www.time.com/time/magazine/article/0,9171,1098961,00.html

[15] Wang Xuanming, *The Thirty-Six Strategems: The Secret Art of War* (China Books and Periodicals, December 1992).

[16] http://www.chinastrategies.com