# Book Review: *Cyber Bytes: Chinese Information-War Theory and Practice* by Timothy Thomas

## *Strategic Insights*, Volume VI, Issue 3 (May 2007)

by MAJ Eric Oliver



*A review of Timothy L. Thomas, Dragon Bytes: Chinese Information-War Theory and Practice (Ft. Leavenworth, KS: Foreign Military Studies Office, 2004).*

## Introduction

Drawing on almost ten years of open source research at the Foreign Military Studies Office at Fort Leavenworth, Timothy Thomas' book *Cyber Bytes: Chinese Information-War Theory and Practice* provides an exceedingly thorough review of the Chinese literature on their development of Information-War (IW) both as a concept and as a capability.

Although Chinese approaches to IW have significant similarities to American ones, his book clearly highlights the differences in motivation, technique, and philosophy which are uniquely Chinese. By understanding these differences, the reader will be able to make reasonable predictions how the Chinese may confront (and may already be confronting) adversaries and potential adversaries in the 21st century. As Dr. Jacob Kipp, Director of the Foreign Military Studies Offices says in the book's foreword: "The findings will prove to be slightly alarming to those who believe that the Chinese are years behind other nations in information age developments."

## Toward an 'Informationalized Force'

The author begins by highlighting the fact that Chinese writings on IW first began to appear in the middle of the 1980s, but notes there really wasn't much advancement of the idea. That changed dramatically after the first Gulf War. Having seen the power of an "informationized force" (as the Chinese referred to it), military and other prominent theorists began looking at new IW concepts with a focus on preparing for what they referred to as "People's war under modern conditions." As a result, the first three chapters of Mr. Thomas' book provide a review of key Chinese writings from 1995-2003. Those writings look similar to early U.S. Command and Control and IW theories, but it appears the Chinese came into their own around the 1997-1998 time frame.

The author provides ample evidence that, since that time, the Chinese are diligently transitioning from a mechanized force to an informationized one:

- They are developing concepts similar to the United States' network-centric warfare—integrating sensors and shooters via a network to increase accuracy and pace of operations.
- They are cultivating theories and capabilities for attacking and defending military and civilian networks—the author discusses open source accounts of Chinese successes against the United States.
- They are creating and leveraging high-technology training and research institutes—the author discusses at least five of them.
- They are thinking about how to attack and defend command, control, communications, computer systems, and intelligence (C4I) systems.
- They are preparing for electronic warfare.
- They are changing their command structures.
- They are developing and exercising means of using networks to rapidly mobilize the entire nation.
- They are discussing means to target public opinions—both domestic and foreign.
- They are pondering approaches to psychological operations.
- They are investigating better ways to leverage their reserves' civilian information technology expertise to support their active forces.
- They are securing their "information borders" and reinforcing their "spiritual defense line" against propaganda and other attacks using "false information."

The list seemingly goes on forever as the Chinese discuss ways to use "information systems, sound, light, electronics, magnetism, heat, and so on as carriers of strategy."

## Strategic Philosophy

So what is the significance of it all? Isn't the United States doing many of the same things? The answer is "yes." However, the Chinese have different philosophical underpinnings that inform their approach. Seemingly in homage to Sun Tzu, the Chinese are not simply looking at IW as a means to improve their performance in conflict: they have set their sights on "forcing enemy troops to surrender without a fight" or as General Wang Baocun put it in 1999, to "force the enemy side to regard their goal as our goal." In a word, the Chinese are thinking "preemption." Chapters 4 and 5 are indispensable for getting inside the Chinese psyche on these points.

Chapter four is dedicated to the traditional Chinese concept of 'stratagems' and how they can be adapted for IW. One of Mr. Thomas' quotes from Major General Li Bingyan says it best:

While we are inheritors of our own outstanding cultural tradition, we should be boldly collecting cultural genes from Western military science and its emphasis on technology. We should make traditional strategy merge with modern science and technology and scientific methods, so as to restore the original intent of 'Sun Tzu strategy.'

The chapter offers many examples of how the Chinese are acting on this concept, but one particularly interesting case was quoted by the author. He cited the writings of Maj General Niu Li (a professor), Col Li Jiangzhou (an associate professor), and Maj Xu Dehui (a lecturer) from the Communications and Command Institute.

Their writings have laid out and explained ten specific stratagems: thought-directing, intimidation through momentum building, information-based capability demonstrations, prevailing over the enemy with extraordinary means, using fictitious objects to hide the true picture, all-encompassing deceptions, prevailing over the enemy with all-round strength, going with the flow, releasing "viruses" to muddy the flows, and controlling the time element. Reading this list and their accompanying explanations, I was struck with the similarity between these notional

stratagems and some of the actual events we see emanating from China. To offer just one example, the stratagem of Information-based Capability Demonstrations seems to become reality in reports of Chinese anti-satellite activities such as the destruction of a satellite on January 11, 2007.

Chapter 5 is dedicated to PSYOP. Having 4,000 years of experience, the Chinese should be well-prepared. With the emergence of information technology, Chinese leaders realize people will be exposed to new ideas, and the power of ideas cannot be ignored. As a result, this chapter includes a fascinating discussion of "Psychological Security." In the Chinese view PSYOP is not only about projecting destabilizing ideas into an adversary's population or forces, but is also about "inoculating" one's own population or forces against such ideas—'defensive PSYOP' if you will. Here again, the theories seem to become reality when one looks at Chinese efforts to discredit or disallow outside information from reaching their population.

Chapters 6 and 7 review Chinese writings analyzing the war in Iraq up through August of 2003. After reading these chapters, it is clear the Chinese were once again surprised by the effectiveness of the coalition. Based upon the literature Mr. Thomas has explored, it appears the Chinese have a renewed respect for the efficacy of information technology in support of traditional combat. It also appears they were impressed by U.S. psychological operations units—the 4th Psychological Operations Group in particular. Their overall assessment of the PSYOP campaign led them to highlight five noteworthy lessons learned:

- China should strive for advantage in future conflicts by demonstrating they are fighting a just war;
- China must provide better psychological training to decisionmakers because psychology can impact the progress or outcome of conflict;
- China must build up its PSYOP forces at the state and military levels;
- China must build a propaganda system including modern mass communications, cultural awareness, and psychology and behavioral science understanding; and
- China must respect foreign PSYOP capabilities and increase PSYOP defense efforts.

These chapters lead inexorably to the conclusion that the Chinese are preparing their forces to be able to fight first in the so-called cognitive domain, but they are also preparing to back it up with full-scale information-empowered, kinetic conflict if necessary.

In China, as in the United States, IW is a very broadly defined term, but Mr. Thomas' book does an exceptional job of collecting all the various interpretations and activities that correlate to the Chinese IW effort. His book also does an excellent job discussing the meaning of those interpretations and activities through the minds of the Chinese themselves. He concludes that "China intends to use IW in one of three ways: as a tool of war, as a way to achieve victory without war, or as a means to enhance stability." Based upon the evidence provided, there is no doubt China is organizing, training, and equipping to succeed.

The only criticism I offer of this book is readability. Trying to collapse ten-plus years of nationwide writing by hundreds of authors into a relatively compact 162 pages is a tough task to be sure, but the ideas seem to flow in stream-of-consciousness fashion at some points. As a result, it is sometimes very tough reading. Nevertheless, *Cyber Bytes* is still well worth the effort. Having been involved in U.S. IW theory and practice for almost five years now, I have seen numerous intelligence briefings on Chinese IW, but this book was better than the sum of all of them. If the reader only has time to read one chapter, be sure to read Chapter 4 to get a feel for the Chinese concept of IW stratagems. If the reader wants a thorough understanding of the state of IW in China, but doesn't have the time to read ten years worth of Chinese writing, read this book in its entirety.

## About the Author

Eric Oliver is a Major in the U.S. Air Force. He was one of the principal authors of the AF's Information Operations (IO) Concept of Operations and contributed extensively to the AF's current IO Doctrine publication. He also served as the first Director of Operations at the Air Force's Network Operations and Security Center. He brought that organization to its initial operational level, successfully commanding and controlling the daily defense of AF computer networks against a full spectrum of active threats.

*The views expressed here are those of the author(s) and do not necessarily represent the views of NPS, the Department of Defense, or the U.S. Government.*