Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Redefining the Role of Information Warfare in Chinese Strategy

Information warfare is generally understood as "actions taken to affect adversary information and information systems, while defending one's own information and information systems."2 In this paper, a theory is introduced that China is currently executing a patient and deceptive form of information warfare that redefines the boundaries of Western definitions of the concept. China's efforts are designed to advance its economic state, maintain its national unity, significantly improve its technological and military capab...

Copyright SANS Institute
Author Retains Full Rights

AD

Entrust
< Let's Talk

Edward Sobiesk
GSEC Practical Assignment 1.4b, Option 1
March 1, 2003

Redefining the Role of Information Warfare in Chinese Strategy

> The record of Americans' ability to predict the nature of the next war (not to mention its causes, location, time, adversary or adversaries, and allies) has been uniformly dismal.[1]
>
> -- Charles Heller and William Stofft, *America's First Battles*

Abstract

Information warfare is generally understood as "actions taken to affect adversary information and information systems, while defending one's own information and information systems."[2] In this paper, a theory is introduced that China is currently executing a patient and deceptive form of information warfare that redefines the boundaries of Western definitions of the concept. China's efforts are designed to advance its economic state, maintain its national unity, significantly improve its technological and military capabilities, and increase its regional and global influence -- all with minimal or no fighting and without alarming the West. This theory is supported by diverse sources that relate directly to China's grand strategy and strategic heritage.

China is emerging as the United States' primary rival in the 21st Century. In spite of this formidable competitor, American comprehension of China's strategic heritage, grand strategy, and the role of information warfare in support of that strategy is gravely insufficient. This work presents summaries of China's strategic heritage and grand strategy, and then proposes how China is currently using information warfare based on its strategic heritage to achieve its national interests. China's view of America as an adversary and appropriate comparisons to America's strategic heritage and America's information warfare doctrine are also included. It is stressed throughout the paper that American analysis does not fully comprehend the strong impact that Eastern strategic heritage is having on China's actions.

Introduction

As the 21st Century begins, the future of world relations is very uncertain. Whether the United States will gradually decline in global influence and the world become multi-polar is unclear. In the upcoming decades, the nation that appears to hold the greatest potential for developing into a true rival with the United States is China. This turn of events is somewhat disturbing since currently China's non-democratic government retains strict central control over its society, economy, and military. As China continues to grow in economic, military, and political strength, it is essential that American strategists devote greater study to understanding this possible adversary.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The ancient Chinese strategist Sun Tzu said, "One who knows the enemy and knows himself will not be in danger in a hundred battles."[3] In this Information Age, though, with American military doctrine relying on numerous high tech means to maintain almost perfect information and military situational awareness, America is neglecting to study potential adversaries' strategic cultures. America's Vietnam War showed that having a technically superior force is not enough. In the end, warfare is about breaking the other nation's will to fight. This is a key aspect of the domain of information warfare. With the line between war and peace now very blurry, the field of information warfare warrants even more careful study.

Cultural Perspectives – East vs. West

Before discussing China's overall strategy, and the role information warfare plays, it is critical to understand the strategic cultural differences between the East (China) and the West (United States). These cultural perspectives dramatically impact the strategies employed by each country. Perhaps even more importantly, though, the United States' cultural perspective could cause it to misread, or even miss, what China's strategic aspirations are and what methods are being employed to achieve them.

An excellent illustration of the differences between the two cultures is given by Mark McNeilly is his book *Sun Tzu and the Art of Modern Warfare*. Mr. McNeilly explains that the differences between the classic board game of each culture, chess for the West and Go for the East, show the dissimilarities in strategic thinking. Chess starts with a board full of pieces – a complete Army on each side. A battle takes place, and in the end, both Armies are generally destroyed (the board is almost empty) and the winner has captured the opponent's king. Contrast this with Go, where one starts with an empty board, and the players take turns placing pieces (black or white stones) on the board in an effort to gain control of as much territory as possible. Although capture of opponent's stones is possible, it is secondary to controlling territory. To play well, one must balance defending one's own territory and attacking the vulnerable pieces of the opponent. The game of Go ends with the board filled with pieces and the winner controls the greatest amount of territory.[4] Mr. McNeilly, whose book advocates the teachings of Sun Tzu, believes in the Eastern attitude used in Go over the Western attitude used in chess,

> In strategy, one should seek to exert the most influence with the smallest investment, not to destroy one's opponent and one's own nation in endless fighting. It is best not to win by wiping out one's enemy but by avoiding fighting and moving strategically to achieve relative dominance, survival, and prosperity. This approach leaves the nation intact, allowing it to dominate a healthy peace rather than one which fosters resentment and poverty.[5]

A second example of the cultural differences between East and West was inadvertently given in a footnote inside the 2002 Report to Congress on *The Military Power of the People's Republic of China* by the United States Secretary of Defense. The Report

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

stated that China has not officially published a "grand strategy," but China's two strategic objectives can be identified as (1) developing "comprehensive national power" and (2) maximizing "strategic configuration of power" called "*shi*" to maintain independence and create momentum for national power. China's overall strategy will be covered shortly, but the point of interest here involves a footnote for the term "*shi.*" The first two sentences of the footnote state, "There is no Western equivalent to the concept of '*shi*.' Chinese linguists explain it as 'the alignment of forces,' the 'propensity of things,' or the 'potential born of disposition,' that only a skilled strategist can exploit to ensure victory over a superior force."[6] This indicates that the United States does not think in the same manner as China and even begs the question: does the United States understand how China thinks?

Is the United States an Adversary?

This paper does not intend to definitively claim that China views the United States as an adversary. In fact, based on cultural differences, it is possible that China would not view the term adversary in the same manner as the United States. If one expands upon the Go strategic analogy presented above, China most likely sees the United States as an obstacle to achieving control and influence over territory. This proposition is supported by the 2002 Report to Congress on *The Military Power of the People's Republic of China* which states:

> While seeing opportunity and benefit in interactions with the United States -- primarily in terms of trade and technology -- Beijing apparently believes that the United States poses a significant long-term challenge. China's leaders have asserted that the United States seeks to maintain a dominant geostrategic position by containing the growth of Chinese power, ultimately "dividing" and "Westernizing" China, and preventing a resurgence of Russian power.[7]

This Report also indicates that China has a negative view toward United States relationships with Japan and Taiwan, especially involving any East Asian regional theater missile defense system or a "rebirth of Japanese militarism." In general, China will seek to reduce the United States' Asia-Pacific regional influence.[8]

Additional evidence on China's attitude towards the United States can be found in a magazine article and another Report to Congress. An August 2002 article in *Jane's International Defense Review* notes that based on the United States' reaction to the 1996 Taiwan Strait crisis, the Chinese military decided that any outbreak of conflict in the Taiwan region would result in United States intervention. Based on this judgment, Chinese military strategists have increased their study of the United States armed forces and advocate using the United States as the target of military exercises.[9] The 2002 Report to Congress on *The National Security Implications of the Economic Relationship Between the United States and China* by the U.S. - China Security Review Commission substantiates this by identifying that one of China's six military modernization focuses is, "Acquiring the capability to sink an American aircraft carrier."[10]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

In defense of China's attitude, many Chinese strategists might argue that the United States, other Western nations, and Western non-state organizations have, at a minimum, been waging non-violent financial and trade war within Southeast Asia for the past decade. As example, PLA Colonels Qiao Liang and Wang Xiangsui, in their 1999 book *Unrestricted Warfare*, describe the financial crisis that took place in Southeast Asia in the mid 1990s, "A surprise financial war attack that was deliberately planned and initiated by the owners of international mobile capital ultimately served to pin one nation after another to the ground . . . ."[11] They further describe financial war as "a form of non-military warfare which is just as terribly destructive as a bloody war, but in which no blood is actually shed."[12] If feelings such as these exist within the Chinese culture, it is easy to understand why the West may be viewed as an adversary. It also provides insight into how China views strategy and information warfare.

China's Grand Strategy

A preponderance of literature reviewed indicates that as China enters the Information Age, it is strategically falling back upon the 2000-year-old teachings of Sun Tzu's *The Art of War*. The following two Sun Tzu quotations best sum up current Chinese strategy:

> Therefore, to gain a hundred victories in a hundred battles is not the highest excellence; to subjugate the enemy's army without doing battle is the highest of excellence.[13]
>
> Warfare is the Way of deception. Therefore, if able, appear unable, if active, appear not active, if near, appear far, if far, appear near.[14]

Compare these sayings with the frequently quoted Deng Xiaoping (a key 1970-80's Chinese leader) 24-character strategy: "Keep cool-headed to observe, be composed to make reactions, stand firmly, hide our capabilities and bide our time, never try to take the lead, and be able to accomplish something."[15]

Toshi Yoshihara, in his monograph *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*, identifies that Sun Tzu is strongly influencing Chinese strategic culture. Based on China's perceived "position of weakness" relative to the United States, the concept of winning without fighting holds great appeal. Mr. Yoshihara states, "In a hypothetical confrontation between China and the United States, the backwardness of Chinese forces would undoubtedly invite defeat. Since the Chinese cannot possibly hope to fight on American terms, they must therefore find other means to deter or defeat the United States."[16] In other words, they must win without fighting.

The 2002 Report to Congress on *The Military Power of the People's Republic of China* lists comprehensive national power (evaluated based on China's national standing compared to other nations) and "strategic configuration of power" as China's grand strategic objectives. It emphasizes, however, that China views "strategic ambiguity,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

including strategic denial and deception," as a method to influence the public and government opinions of other countries.[17] This Report also stresses "China's leaders believe that three essential 'conditions' – national unity, stability, and sovereignty – must exist if China is to survive and develop as a nation."[18]

The 2002 Report to Congress on *The National Security Implications of the Economic Relationship Between the United States and China* states similar, but more foreboding, findings: "China's leaders view the United States as a partner of convenience, useful for its capital, technology, know-how, and market. They often describe the United States as China's long term competitor for regional and global military and economic influence."[19] This Report indicates China is implementing this strategy with ". . . well established policies and a broad-based program (including both legal and illegal methods) to acquire advanced Western technologies for its industrial development, military programs, espionage capabilities and intelligence gathering and surveillance."[20]

China isn't adopting the above strategy and taking the above actions in anticipation of World War III with the United States. Rather, China is strengthening itself during peace and prosperity so it can increase its regional and global power without fighting the United States in a major war. Because China's strategy utilizes peacetime to expand its influence and accomplish the actions necessary to ensure success with little or no fighting, the concept of Chinese information warfare takes on an entirely new light.

The Role of Information Operations (Information Warfare) in U.S. Doctrine

In understanding how China approaches and conducts information warfare, it is valuable to first review the information warfare doctrine of the United States. The United States uses the term "information operations" during peacetime and reserves the term "information warfare" exclusively for times of conflict.[21]

The U.S. military's *Joint Vision 2020*, the guidance for transforming America's armed forces, states the overall goal of transformation is ". . . the creation of a force that is dominant across the full spectrum of military operations – persuasive in peace, decisive in war, preeminent in any form of conflict."[22] It identifies information superiority as its key enabling concept which achieves, "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[23] Information superiority is only of value, though, when it fosters decision superiority, defined as, ". . . better decisions arrived at and implemented faster than an opponent can react . . . ."[24] Information superiority is ". . . created and sustained by the joint force through the conduct of information operations."[25]

The U.S. military *Joint Doctrine for Information Operations* states, "Information operations are actions taken to affect adversary information and information systems, while defending one's own information and information systems."[26] The scope of information operations applies "across all phases of an operation, the range of military operations, and at every level of war."[27] The major capabilities used for information

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

operations consist of operations security, psychological operations, military deception, electronic warfare, physical attack/destruction, and may include computer network attack. Information operations activities also encompass public affairs and civil affairs. Offensive information operations capabilities target "the human decision making processes" and ". . . must be permissible under the law of armed conflict, consistent with applicable domestic and international law, and in accordance with applicable rules of engagement."[28] Joint doctrine defines information warfare as, "information operations conducted during time of crisis or conflict . . . ."[29] The United States does not conduct information operations or information warfare against the American public.

Although these quoted U.S. documents claim information operations look beyond the military and conflict domains, their entire flavor is, not unexpectedly, military and conflict-oriented. U.S. doctrine appears to seek information superiority over an enemy through using high tech means such as satellites, maintaining elaborate electronic command and control systems, degrading or denying an enemy their command and control systems, and using precision weapons to destroy desired targets. Information operations are often waged by the U.S. military in support of kinetic weapons. U.S. commanders try to stay several moves ahead of their opponent(s) in the decision cycle while maintaining close to perfect information, denying the enemy insight into U.S. actions, and striking quickly with surgical precision. Returning to the chess vs. Go board game analogy, U.S. doctrine appears to be just another way of describing how to win at chess.

Chinese Information Warfare: It's not about Fighting

This paper theorizes that China is currently executing a patient and deceptive form of information warfare designed to advance its economic state, maintain its national unity, significantly improve its technological and military capabilities, and increase its regional and global influence all with minimal or no fighting and without alarming the West. Everything presented thus far in this paper – from the analogy of Go vs. chess to the relationship between the United States and China to America's view on how information warfare should be waged – has been designed to place the reader in a position to appreciate what China is attempting to accomplish. As shall be seen in subsequent paragraphs, China's information warfare actions go beyond the military boundaries that are more traditional in the West. They are methodically based on China's desired ends instead of available technological means or current U.S. technological infrastructure vulnerabilities. China's objectives are more likely measured in decades as opposed to the U.S. tendency towards immediate or short-term accomplishments. Because of the central control China's government maintains over its society, China's pursuits spanning the economic and military domains hold the potential to be more integrated than America's open economy allows. Finally, China's central control and closed society may also allow it to hide its true intentions until significant progress has been made toward their completion.

The theory that China is currently executing a non-Western form of information warfare assumes a very broad definition, or at least application, of the information warfare

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

concept. China is attempting to accumulate as much meaningful information (as well as capital and military equipment) as possible and to protect its information, decision-makers, and national unity. They are exploiting their adversary's information systems and open societal structures and are attempting to influence their adversary's decision-making process. Throughout these efforts, China is trying to conceal its intentions from the West because the opportunity of exploitation is much greater when the target is unaware of, or not sensitive to, the exploitation. Examples of what China is attempting to accumulate include Western science and technology techniques and capabilities, Western capital, cutting edge military technology, and sophisticated nuclear technology. Example elements of the Western decision-making process that China is trying to influence include Western military, government, and business leaders, the Western media, and the Western public. If China intends to win without fighting, then it will carefully walk the line of buying, bullying, borrowing, and stealing every possible advantage that it can without placing its current position of power in jeopardy. China's current position of power should be interpreted as its strong central control of its nation and its regional influence.

Some Western readers may think this broad definition of information warfare is "beyond the boundaries of information warfare," or "not warfare." This is exactly what China wants the West to think.

The much-discussed 1999 book *Unrestricted Warfare* by PLA Colonels Qiao Liang and Wang Xiangsui has been internally criticized for possibly divulging "too much information on Chinese thinking to the outside world."[30] However, much in this book supports this paper's theory on Chinese information warfare and actually had a significant impact in forming that theory. As example, it states, "Obviously, warfare is in the process of transcending the domains of soldiers, military units, and military affairs, and is increasingly becoming a matter for politicians, scientists, and even bankers. How to conduct war is obviously no longer a question for the consideration of military people alone."[31] In a different section of the book, it expresses similar sentiments, ". . . we acknowledge that the new principles of war are no longer 'using armed force to compel the enemy to submit to one's will,' but rather are 'using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests.' "[32] In fact, the very title *Unrestricted Warfare* captures the position of the authors as illustrated, "When we suddenly realize that all these non-war actions may be the new factors constituting future warfare, we have to come up with a new name for this new form of war: Warfare which transcends all boundaries and limits, in short: unrestricted warfare."[33] In transcending all boundaries, the authors include those, "lying between the two worlds of war and non-war, of military and non-military."[34]

Unrestricted Warfare also points out the Western media's ability to influence the Western public and Western decision-makers during conflicts. A salient example is America's withdrawal from Somalia in 1993. The authors query, "Did CNN's broadcast of an exposed corpse of a U.S. soldier in the streets of Mogadishu shake the determination of the Americans to act as the world's policeman, thereby altering the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

world's strategic situation?"[35] They argue that Western media impacted the end of Operation Desert Storm also,

> . . . the reason that the ground war abruptly came to a halt after 100 hours was actually because Bush, influenced by a hasty assessment of the course of the war that was issued on television by a battlefield news release officer, later came to a similarly hasty decision of his own, "dramatically shortening the time from strategic decision-making to concluding the war."[36]

These two media related incidents are exactly the sort of effects information warfare is trying to accomplish. *Unrestricted Warfare* even surmises that media influence might be purchased saying, "could buying or gaining control of stocks be used to turn another country's newspapers and television stations into the tools of media warfare?"[37]

In his article "Threat Kingdom," Lieutenant Colonel Bill Flynt of the Foreign Military Studies Office at Ft. Leavenworth, KS extracted important insights into the book *Unrestricted Warfare* through the use of a technique called "text-mining." Text-mining will identify ". . . the language of a document, summarize and categorize a document, extract key words, proper names and multiword phrases, report frequency of word and phrase occurrence, statistically rank a document's relevance to a specific topic and glean other information."[38] The application of this technique revealed the five most often described means in the book *Unrestricted Warfare* are: cyber strikes, information operations, economic attacks, bombing, and direct action. Text-mining identified the five most often described ends as: national security advantage, economic advantage, financial gain, political influence, and political change.[39] Discussing the most often described ends, Lieutenant Colonel Flynt summarizes, "The ends emphasized in this red perspective overlap all four instruments of power: military (national security advantage), economic (economic advantage/financial gain), diplomatic/political (political change) and informational (political influence). From this red perspective, any end that increases power is worth pursuing."[40]

Based on a literature review, it appears that when evaluating China's information warfare strategy, American analysis usually focuses on available means and American vulnerabilities instead of China's desired ends. Many excellent papers exist on the asymmetric threat of cyber attack and on the vulnerabilities of America's infrastructure to such an attack. The on-line SANS Reading Room, for instance, has a paper by Charles Bacon entitled "The China Syndrome" which explores the possible use of Chinese civilians to launch massive information warfare attacks against the United States, as well as the potential use of information warfare techniques by China to target United States military and civilian information systems and infrastructure. The paper also addresses the legal issues involving the Articles of the Geneva Convention if civilian infrastructure is targeted or if uncontrolled means such as computer viruses or worms are used.[41]

The vulnerability of America's infrastructure is certainly very high, and the threat of an electronic Pearl Harbor-like attack, especially by a non-state organization that would be

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

difficult to retaliate against, must not be ignored. In the case of China, though, with the exception of a possible attack to seize Taiwan, China's long term ends focus far more on its economy and regional influence. The five most often described ends in the book *Unrestricted Warfare* support this position. Additionally, Toshi Yoshihara's monograph *Chinese Information Warfare: A Phantom Menace or Emerging Threat?* observes that for China, ". . . economic development remains its highest national priority . . . ."[42] Likewise, the 2002 Report to Congress on *The National Security Implications of the Economic Relationship Between the United States and China* cites ". . . rapidly growing economic interactions that have muted political differences."[43] This Report further concludes that China's ". . . military derives extensive financial and technological benefits from the growth and modernization of the domestic economy, which is designed to serve it."[44] A final sobering comment from this Report deals with China's methods: "China is covertly acquiring the more sensitive technologies it cannot buy on the open market through a targeted collection program and espionage initiatives."[45]

The American perspective on information warfare is generally too limited. For instance, it may restrict itself too much to the military domain, or to the prospect of armed conflict, or to a computer-centric vision. Perhaps, though, American perspectives and assumptions continue to flourish as a result of Chinese efforts. China's information warfare strategy is shrouded in secrecy and confusion as the following paragraphs make clear.

The most comprehensive work found on the subject of Chinese information warfare is Toshi Yoshihara's U.S. Army War College monograph *Chinese Information Warfare: A Phantom Menace or Emerging Threat?* Despite Mr. Yoshihara's extensive, intelligent coverage of the subject, he found identification of China's information warfare doctrine to be "frustratingly elusive." The lack of any official national policy or meaningful taxonomy, the "opaqueness of China's defense community," the gaps in analytical writings and "between theory and practice," the ongoing debates and lack of consensus, the absence of evidence on future direction, and the unique influence of Chinese strategic tradition all result in his assessment that China's attitudes on information warfare are "evolving" and "could pose an increasingly daunting and unpredictable challenge for American policymakers."[46]

Mr. Yoshihara points out that in a significant portion of their literature, the Chinese dovetail, or even plagiarize, American information warfare concepts. For example, he describes how the Chinese concept of information dominance is remarkably similar to America's information superiority. He notes, though, that while this copying may be legitimate, much of China's public debate might be designed to "further obscure China's real intentions and capabilities" and could conceivably be "an extensive deception campaign."[47] Mr. Yoshihara warns that the United States must be careful not to believe that Chinese views on information warfare mirror those of the United States. He repeatedly emphasizes that "Sun Tzu's influence as a strategic tradition" remains strong. Sun Tzu's notion of "winning without fighting through superior knowledge" is especially appealing as compared to fighting a mid-intensity conflict against America's high tech military.[48] Mr. Yoshihara summarizes:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

> . . . American understanding of China's approaches to IW within the academic and defense communities remain shallow. This lack of understanding, both stemming from the extreme secrecy surrounding China's military programs in general and the nascent stage of development in IW in particular, could invite ugly strategic and operational surprises for the United States.[49]

Conclusion

It is not the intent of this paper to claim definitive understanding of China's information warfare strategies and programs. A theory was proposed, and evidence was presented in support of that theory. A more significant concern is opening a greater Western dialogue on Chinese information warfare techniques including scope, threats, and desired ends. A key second objective of this paper was to repeatedly point out the vast differences in strategic heritage between China and the United States, and how these effect the actions of each country. If America doesn't fully address these differences, it may result in significant long-term strategic disadvantage.

As a final thought, Winston Churchill, in a 1939 radio address, said, "I cannot forecast to you the action of Russia. It is a riddle wrapped in a mystery inside an enigma: but perhaps there is a key. That key is Russian national interest."[50] In the 21st Century, Western strategists must use Chinese national interest as the starting point for analysis.

Notes

---

[1] Charles Heller and William Stofft, *America's First Battles*, Lawrence, Kansas: University Press of Kansas, 1986, p. xii.

[2] U.S. Department of Defense, *Joint Doctrine for Information Operations*, 9 October 1998, URL: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (21 February 2003), pp. I-9 and I-11. The U.S. military uses the term information operations for "actions taken to affect adversary information and information systems, while defending one's own information and information systems." The term information warfare is reserved for information operations conducted during a time of conflict.

[3] Sun Tzu, *The Art of War*, translated in 2000 by Sonshi.com, URL: http://www.sonshi.com/sun-tzu_all.html (20 February 2003), Chapter 3.

[4] Mark McNeilly, *Sun Tzu and the Art of Modern Warfare*, New York: Oxford University Press, 2001, pp. 22-23.

[5] Ibid., p. 23.

[6] Office of the Secretary of Defense of the United States of America, Report to Congress on *The Military Power of the People's Republic of China*, 12 July 2002,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

URL: http://www.defenselink.mil/news/Jul2002/d20020712china.pdf (17 February 2003), pp. 5-6.

[7] Ibid., p. 8.

[8] Ibid., p. 10.

[9] Yihong Zhang, "China's Rising Forces," *Jane's International Defense Review*, Volume 35 (August 2002): p. 36.

[10] U.S. – China Security Review Commission, Report to Congress on *The National Security Implications of the Economic Relationship Between the United States and China*, July 2002, URL: http://www.uscc.gov/anrp02.htm (20 February 2003), Chapter 10.

[11] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, translated by Foreign Broadcast Information Service (Beijing, China: PLA Literature and Arts Publishing House, February 1999), URL: http://www.terrorism.com/documents/unrestricted.pdf (21 February 2003), p. 51.

[12] Ibid., p. 51.

[13] Sun Tzu, *The Art of War*, translated in 2000 by Sonshi.com, URL: http://www.sonshi.com/sun-tzu_all.html (20 February 2003), Chapter 3.

[14] Ibid., Chapter 1.

[15] Deng Xiaoping, as quoted in Office of the Secretary of Defense of the United States of America, Report to Congress on *The Military Power of the People's Republic of China*, 12 July 2002, URL: http://www.defenselink.mil/news/Jul2002/d20020712china.pdf (17 February 2003), p. 7.

[16] Toshi Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*, November 2001, URL: http://www.carlisle.army.mil/ssi/pubs/2001/chininfo/chininfo.pdf (21 February 2003), pp. 6, 24-28.

[17] Office of the Secretary of Defense of the United States of America, Report to Congress on *The Military Power of the People's Republic of China*, 12 July 2002, URL: http://www.defenselink.mil/news/Jul2002/d20020712china.pdf (17 February 2003), pp. 5, 6, and 8.

[18] Ibid., p. 6.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[19] U.S. – China Security Review Commission, Report to Congress on *The National Security Implications of the Economic Relationship Between the United States and China*, July 2002, URL: http://www.uscc.gov/anrp02.htm (20 February 2003), Executive Summary.

[20] Ibid., Chapter 10.

[21] U.S. Department of Defense, *Joint Doctrine for Information Operations*, 9 October 1998, URL: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (21 February 2003), p. I-11.

[22] U.S. Chairman of the Joint Chiefs of Staff, *Joint Vision 2020*, June 2000, URL: http://www.dtic.mil/jv2020/jv2020.doc (22 February 2003), p. 1.

[23] Ibid., p. 10

[24] Ibid., p. 11.

[25] Ibid., p. 11.

[26] U.S. Department of Defense, *Joint Doctrine for Information Operations*, 9 October 1998, URL: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (21 February 2003), p. I-9.

[27] Ibid., p. vii.

[28] Ibid., pp. I-9, I-10, and II-1.

[29] Ibid., p. I-11.

[30] Toshi Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*, November 2001, URL: http://www.carlisle.army.mil/ssi/pubs/2001/chininfo/chininfo.pdf (21 February 2003), p. 22.

[31] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, translated by Foreign Broadcast Information Service (Beijing, China: PLA Literature and Arts Publishing House, February 1999), URL: http://www.terrorism.com/documents/unrestricted.pdf (21 February 2003), p. 221.

[32] Ibid., p. 7.

[33] Ibid., p. 12.

[34] Ibid., p. 12.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[35] Ibid., p. 12.

[36] Ibid., p. 76.

[37] Ibid., p. 191.

[38] Bill Flynt, "Threat Kingdom," July 2000, URL: http://call.army.mil/fmso/fmsopubs/issues/threatkingdom/threatkingdom.htm (23 February 2003), p. 3.

[39] Ibid., p. 8-9.

[40] Ibid., p. 9.

[41] Charles Bacon, "The China Syndrome," July 2001, URL: http://www.sans.org/rr/infowar/china.php (22 February 2003).

[42] Toshi Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*, November 2001, URL: http://www.carlisle.army.mil/ssi/pubs/2001/chininfo/chininfo.pdf (21 February 2003), p. 6.

[43] U.S. – China Security Review Commission, Report to Congress on *The National Security Implications of the Economic Relationship Between the United States and China*, July 2002, URL: http://www.uscc.gov/anrp02.htm (20 February 2003), Executive Summary.

[44] Ibid., Executive Summary.

[45] Ibid., Chapter 10.

[46] Toshi Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*, November 2001, URL: http://www.carlisle.army.mil/ssi/pubs/2001/chininfo/chininfo.pdf (21 February 2003), pp. 2, 3, 5, 18, 24, 30, 35, and 36.

[47] Ibid., pp. 12, 19, and 21.

[48] Ibid., pp. 6, 20, 23, and 24.

[49] Ibid., p. vi.

[50] Winston Churchill, "Quotation from Radio Address," 1939, URL: http://www.quotationspage.com/quotes/Sir_Winston_Churchill/31 (23 February 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Bibliography

Bacon, Charles. "The China Syndrome." July 2001. URL: http://www.sans.org/rr/infowar/china.php (22 February 2003).

Churchill, Winston. "Quotation from Radio Address." 1939. URL: http://www.quotationspage.com/quotes/Sir_Winston_Churchill/31 (23 February 2003).

Flynt, Bill. "Threat Kingdom." July 2000. URL: http://call.army.mil/fmso/fmsopubs/issues/threatkingdom/threatkingdom.htm (23 February 2003).

Heller, Charles and Stofft, William. *America's First Battles*. Lawrence, Kansas: University Press of Kansas, 1986.

Liang, Qiao and Xiangsui, Wang. *Unrestricted Warfare*. Translated by Foreign Broadcast Information Service (Beijing, China: PLA Literature and Arts Publishing House, February 1999). URL: http://www.terrorism.com/documents/unrestricted.pdf (21 February 2003).

McNeilly, Mark. *Sun Tzu and the Art of Modern Warfare*. New York: Oxford University Press, 2001.

Office of the Secretary of Defense of the United States of America. Report to Congress on *The Military Power of the People's Republic of China*. 12 July 2002. URL: http://www.defenselink.mil/news/Jul2002/d20020712china.pdf (17 February 2003).

Sun Tzu. *The Art of War*. Translated in 2000 by Sonshi.com. URL: http://www.sonshi.com/sun-tzu_all.html (20 February 2003).

U.S. Chairman of the Joint Chiefs of Staff. *Joint Vision 2020*. June 2000. URL: http://www.dtic.mil/jv2020/jv2020.doc (22 February 2003).

U.S. – China Security Review Commission. Report to Congress on *The National Security Implications of the Economic Relationship Between the United States and China*. July 2002. URL: http://www.uscc.gov/anrp02.htm (20 February 2003).

U.S. Department of Defense. *Joint Doctrine for Information Operations*. 9 October 1998. URL: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (21 February 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Yoshihara, Toshi. *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*. November 2001. URL: http://www.carlisle.army.mil/ssi/pubs/2001/chininfo/chininfo.pdf (21 February 2003).

Zhang, Yihong. "China's Rising Forces." *Jane's International Defense Review*. Volume 35 (August 2002).

© SANS Institute 2003, Author retains full rights

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**