Security in knowledge

Analytic of China Cyber Warfare
中國網絡戰之分析

Robert Lai

CISSP-ISSAP, ISSEP, CAP, CEH, CSSLP, C|CISO

RSA®CONFERENCE2013

Session ID: PNG-R32A

Session Classification: Intermediate

Analytic of China Cyber Warfare

- Introduction
  - The enlightened cyber power—China
  - What are the characteristics of China cyberattack?
  - What is China's advantage?

Analytic of China Cyber Warfare

- Comprehensive view of China cyberattack
  - Cyber espionage
  - Cyberattack for political and military goals
  - Cyber assaults
  - Hidden dragon—invisible capabilities
  - Emerging cyberpower

Analytic of China Cyber Warfare

- Cyber espionage
  - China is the most active nation-state on cyber espionage activities
  - Grain of sands approach
    - Steals as much data as possible
    - Infers the data for valuable information later
  - Use stolen military and industry secrets to aid future cyberattack

Analytic of China Cyber Warfare

- Cyberattack for political and military goals
  - Advocates of human rights in China and overseas are targets
  - Cyber-spies target Dalai Lama
  - Military and defense industry personnel are primary targets

Analytic of China Cyber Warfare

- Cyber Assaults
  - In Nov 2006, Chinese hackers prompted Navy college site closure
  - In 2007, the office of Dept of Defense Secretary, Robert Gates, was hacked

Analytic of China Cyber Warfare

- Hidden Dragon—Invisible Capabilities
  - GhostNet
    - 1,000 compromised computers in 103 countries
    - targeted a network of high-value targets
    - has a covert design with advanced botnet capabilities
  - Operation Shady RAT
    - undetected for over five years
    - old malware still matters
  - L7DA (Layer 7 DDoS Attack)
    - CSFI discovered China's advanced technique in 2009

Analytic of China Cyber Warfare

- China as an Emerging Cyberpower
  - A high political, informational, military, and economic (PIME) rating
  - Closing the C4ISR gap
    - Advance in UAV development
    - Advance in space domain
  - First cyberpower with a preemptive strategy

Analytic of China Cyber Warfare

- The Art of China Cyber Warfare
  - Extreme Information Warfare
  - Asymmetric Attack
  - Dynamic Strategic Advantages
  - Critical Competitive Advantages

Analytic of China Cyber Warfare

- Extreme Information Warfare
  - China's People Liberation Army (PLA) has engaged in information warfare (IW) development two decades ago
  - In 1996, Wei Jincheng, a military strategist wrote to use the Internet as a platform to engage in warfare without stepping out of the door in the Liberation Army newspaper
  - China has incorporated IW as an integral part of Revolution in Military Affairs (RMA)
  - People's war concept to leverage the pool of IT experts
  - Active psychological operations
  - 5,000-year-old stratagems plus modern technology

Analytic of China Cyber Warfare

- Asymmetric Attack
  - Asymmetric warfare strategies and capabilities are the core elements in PLA's RMA
  - The conflict of the Taiwan Strait is the best scenario of asymmetric warfare with cyber operations to deter or delay U.S. involvement
  - Higher ROI on using a low-tech method or device to attack a high-tech system

Analytic of China Cyber Warfare

- Dynamic Strategic Advantages
  - Sun Tzu's Art of War
  - Mao's theory of strategy and tactics
  - Go (Wei-Ch'i)—a Chinese strategic game
  - Chinese martial arts—the Tao (way) of fighting
  - Abductive reasoning—smart thinking

Analytic of China Cyber Warfare

- Sun Tzu's Art of War
  - A body of knowledge on strategic and tactical planning
  - Suitable for conventional and un-conventional warfare
  - Key principles
    - Best defense is offense
    - Know your enemy
    - Know yourself

Analytic of China Cyber Warfare

- Mao’s theory of strategy and tactics
  - Mao’s people’s war is famous in guerrilla warfare on attack
    - Holistic and agile
  - Oppose fixed battle lines and positional warfare, and favor fluid battle lines and mobile warfare
  - Oppose keeping the Red Army at its old stage, and strive to develop it to a new stage
  - Avoid or by-pass a strong defense and to assault a weak spot
  - PLA strategy and doctrine are influenced by Mao

Analytic of China Cyber Warfare

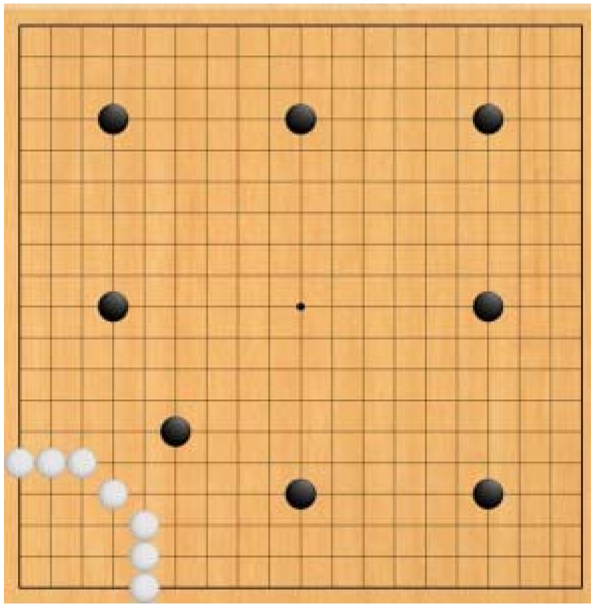
- Go (Wei-Ch'i)—a Chinese strategic game
  - A strategic skill game on a 19x19-grip board to train analytic skill
  - Requires analytical thinking to contemplate means to end using nested loop evaluation
  - The best of Go masters play multiple strategies on multiple boards—all at the same time
  - Military strategy planners (masters of Go) can plan simultaneous attack like multi-threading on a supercomputer
  - The handicapping system of Go permits a weaker player to play with a strong player as a way to practice asymmetric attack

Analytic of China Cyber Warfare

- Go (Wei-Ch'i)—a Chinese strategic game…con't
  - Concept of *Shi* (勢)
    - Like the flow of water that can wash away anything standing in its way
    - Strong *Shi*: most likely to win
    - Weak *Shi*: most likely to lose
    - *Shi* is future-oriented
    - Chapter 5 of Art of War covers *Shi*

Analytic of China Cyber Warfare

- Go (Wei-Ch'i)—a Chinese strategic game…con't
  - An example of weak player of white stone even there is solid strong defense
  - Good *Shi* to black stone player than white stone player



http://blogs-images.forbes.com/johntamny/files/2012/07/GoBoard.jpeg

Analytic of China Cyber Warfare

- Chinese martial arts—the Tao (way) of fighting
  - A full contact combat technique with unrestricted rule
  - It is analogous to asymmetric attack
  - A Chinese martial artist with knowledge of acupuncture points can bring an opponent to his knees with a minimum of movement
    - same analogy on exploitation of vulnerabilities in an information system
  - Martial arts train the minds and bodies of practitioners to cultivate concentration, patience, persistent, focus, and agility
  - The martial arts' qualities are the characteristics of Chinese war-fighters including the cyber warriors

Analytic of China Cyber Warfare

- Abductive reasoning—smart thinking
  - Most people reason with either inductive or deductive logic
  - Chinese reason like abductive logic
  - A good tool to formulate strategy
    - Assumption to be proved in the future
  - China's IW stratagems make the correct assumption about cyber war twenty years ago

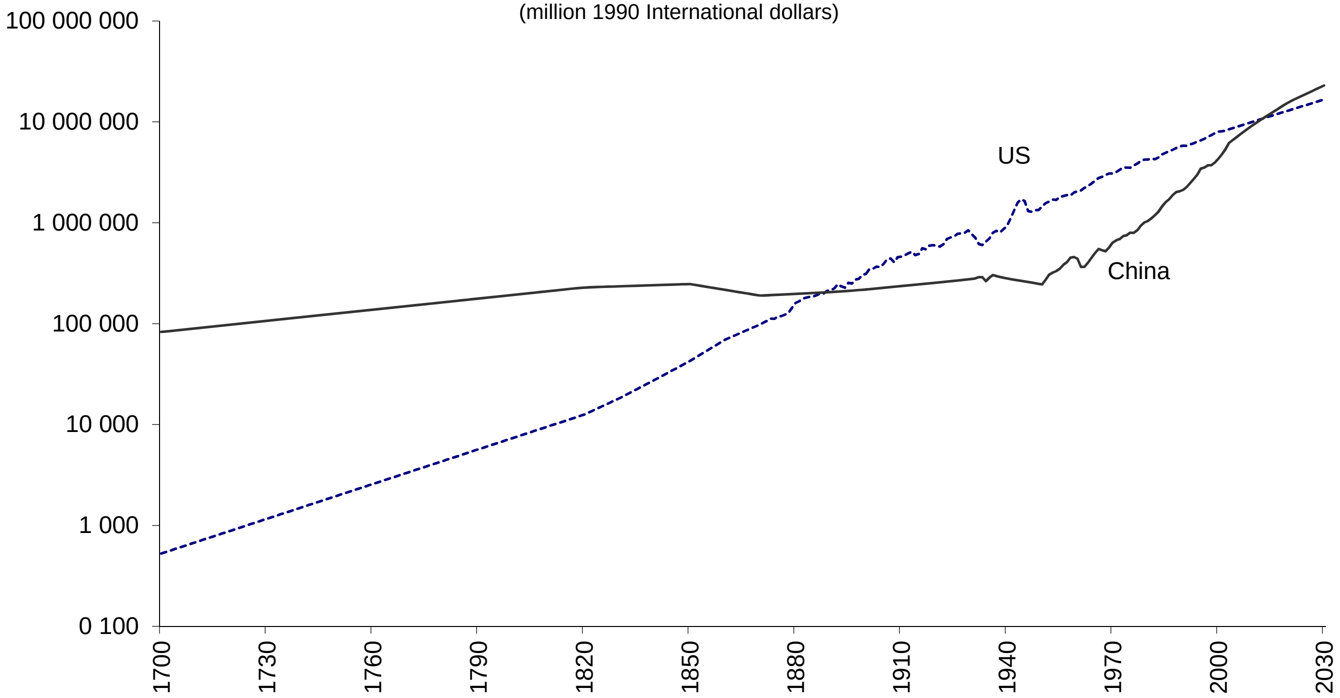
Analytic of China Cyber Warfare

- Critical Competitive Advantages
  - Economic power
  - Demographics
  - Anti-Satellite Program
  - Cryptanalysis
  - High Performance Computers (HPC)
  - Sophisticated Filtering System
  - Red Hackers
  - Soft Power—Knowledge

Analytic of China Cyber Warfare

- Economic power
  - China was a global economic power in 1800
  - China is re-emerging as a global economic power

Comparative Levels of GDP, China and the United States, 1700-2030
(million 1990 International dollars)



Source: www.ggdc.net/Maddison and Maddison (2007)

Analytic of China Cyber Warfare

- Anti-Satellite (ASAT) Program
  - Successful ASAT missile test on Jan 17, 2007
    - Using ballistic missile to shoot down a satellite in low earth orbit
  - A military hedge to the U.S. space dominance

Analytic of China Cyber Warfare

- Demographics
  - Over 500 million Internet users
  - Home to 120 million managerial, professional, and skilled workers at the end of 2010
    - 30 million managerial personnel
    - 55.5 million technical professionals
    - 28.6 million highly skilled personnel
    - 10.5 million rural staff with practical skills

Analytic of China Cyber Warfare

- Cryptanalysis
  - Prof. Wang Xiaoyun 王小云 at Shandong University led a research team to
    - break MD5 by collision attack
    - do the same for SHA1
    - apply subkey recovery attack on ALPHA-MAC, MD5-MAC and PELICAN
    - give the distinguishing attack on HMAC-MD5

Analytic of China Cyber Warfare

- High Performance Computers (HPC)
  - China’s Tianhe-1A supercomputer was the most powerful computer in the world with 2.57 petaflops performance in 2010
  - Military purposes:
    - Nuclear weapons development
    - C4ISR capabilities
    - Cryptography
    - Combat simulation

Analytic of China Cyber Warfare

- Sophisticated Filtering System
  - Advance content filtering capability
    - Multi-layer, multi-channel, and distributed content monitor system
    - Can be a defense
  - Chinese characteristics of Internet Censorship
    - Combination of universal filtering and manual spot-check
    - The criterion for "harmful information," "sensitive information" and "subversion behavior" is not defined within the 50 plus law-cases
    - Inefficient administration and dismayed legal system
    - Scouting and banning protest activities and the political movements supported by oversea forces
  - The most complex, advanced, and pervasive in the world

Analytic of China Cyber Warfare

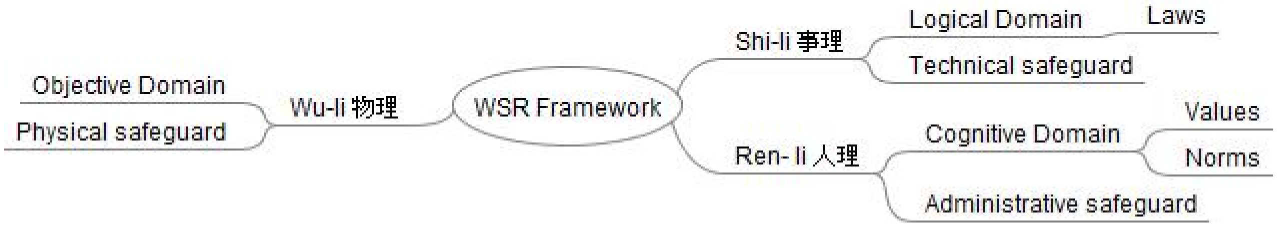
- Red Hackers
  - Ad-hoc
  - Patriotic
  - Hackers for hire
  - Advance in custom malware coding
  - Mao’s doctrine on people’s war works well for the Chinese hackers

Analytic of China Cyber Warfare

- Soft power—knowledge
  - Knowledge is power
  - Rapid progress in systems engineering (SE), and information and communication technology (ICT)

Analytic of China Cyber Warfare

- Soft power—knowledge…con’t
  - China’s SE is augmented by the Oriental systems methodology—”Wu-li Shi-li Ren-li” approach (WSR)
  - WSR doctrine
    - Knowing Wu-li 物理 (relation with the world)
    - Sensing Shi-li 事理 (relation with the mind)
    - Caring Ren-li 人理 (relation with others people)
  - WSR Framework



Analytic of China Cyber Warfare

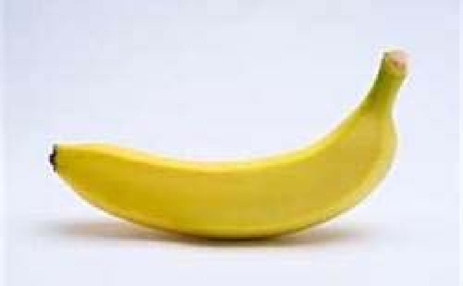
- Cognitive domain
  - National interest
  - Cultural Intelligence
  - Intelligence diversity
  - Worldview

Analytic of China Cyber Warfare

- National interest
  - World power
    - China is challenging the unipolar world order of the U.S.
    - Multipolar world order is the new order
  - Three major objectives
    - To change the sociopolitical order
    - To accelerate economic growth
    - To improve geopolitical standing and restore national dignity

Analytic of China Cyber Warfare

- Cultural Intelligence
  - Select two from the following:



Analytic of China Cyber Warfare

- Cultural Intelligence…con’t
  - Most likely result
    - Western thinkers: choose panda and monkey
    - Asian thinkers: choose monkey and banana
  - Reason
    - Western thinker: panda and monkey are animals
    - Asian thinker: monkey eats banana

Analytic of China Cyber Warfare

- Worldview
  - Occidental vs. Oriental
    - Individualism vs. Collectivism
  - China's participation in the World Trade Organization (WTO)
    - a world factory instead of a world market
  - China plays by its own rules
    - Currency
    - Military spending

Analytic of China Cyber Warfare

- Conclusions
  - Cyber war: it is China's game for now
  - China has dynamic strategic advantage and critical competitive advantages
  - China has the attacker advantage on asymmetric warfare
  - Knowledge is the best weapon to cyber warfare since one of the Sun Tzu's Art of War principles is "know your enemy"
  - An analytic of China cyberattack must scrutinize the national interest, goals and philosophies, culture, worldview, and behavioral phenomena of China

Analytic of China Cyber Warfare

Acknowledgments

I would like to thank Dr. Toshi Yoshihara, John A. van Beuren Chair of Asia-Pacific Studies Strategy and Policy, and professor at the U.S. Naval War College, for his valuable inputs to this capstone project. Ten years ago, Dr. Yoshihara wrote a monograph "Chinese Information Warfare—A Phantom Menace or Emerging Threat" that has been the primary inspiration to lead my interest in researching cyber warfare particularly related to China.

I would like to thank Dr. David Lai, a research professor of Asian Security Studies at the Strategic Studies Institute of the U.S. Army War College, to share his viewpoints with me on U.S.-China security policy, and China's Strategic Concept—Shi.

Their insights provided me the direction to ponder the patterns on China cyber war strategy and tactic.

Analytic of China Cyber Warfare

- My contact info
  - Email: sysgate@gmail.com
  - Twitter: rcklai

Security in knowledge