Cybersecurity Threats – The Red Dragon Rising
Understanding and Assessing the Chinese Cyber Threat

William Hagestad II
Lieutenant Colonel (RET) USMCR
www.red-dragonrising.com
21st Century Chinese Cyber Warfare

Today’s presentation is an appetizer of the content which will be included in a new book titled

“21st Century Chinese Cyber Warfare”

Published by IT Governance, London, UK

In January 2012
Presentation Agenda

- Learning objectives
- Statement of the Issue
- Origins of Chinese Information Warfare (IW)
- People’s Liberation Army Organization
- History of Chinese IW
- Conclusions
Learning Objectives

- Understanding Chinese warfare history and culture that influence today’s reality
- Chinese Communist Party cyber initiatives that threaten your organization
- People’s Liberation Army (PLA) information warfare capabilities
- What you can expect to face in the next decade
What’s the Issue?

Threat of cyber attacks against;

- Corporations;
- Research institutes;
- Militaries;
- International organizations; and,
- Governments...

But not the 中国人民共和国...why?
How are the Chinese doing it?

• Calculated, precise use of hacking methodologies to gain unauthorized access to a network;
  – Via brute force attacks, Distributed Denial of Service (DDoS);
  – Trojans, viruses and malware; or a combination of both methods also known as a....
Advanced Persistent Threat (APT)
So, who is behind these... cyber attacks?

- The People’s Republic of China for starters...
- But it cannot be... there is no evidence pointing to the Chinese Government....
- Who are the attackers then?

1) Yes, the government!
2) The People’s Liberation Army (PLA)
3) State Owned Enterprises
4) Hacktivists
However....Current Events!

• “Slip-Up in Chinese Military TV Show Reveals More Than Intended”¹

• “Chinese Military Slips Up And Broadcasts Cyberwar Campaign Against U.S. Targets”²


Now the Smoking Mouse...

- A Six second screenshot on Chinese Television
- PLA propaganda + unedited TV = proof positive!
- 6-seconds of fame for the PLA demonstrating organic hacking software capability
- Falun Gong Censorship
- Hacked IP @ University of Birmingham, AL
What is the Chinese motivation?

- Fear of foreigners...
- Self-preservation and,
- Hegemony (霸权).....what?
  - A perfect description of the Communist Party of China (CPC).....implied power of the Chinese state subordinates every element of modern Chinese Society......including threats of religion Falun Gong.....
It cannot be that simple?

Other reasons for PRC motivated cyber-attacks....

• Frenzied Chinese economy
• Strategic advantage over regional and international affairs
• CPC mandated...2010
• PLA mission statement....1995!
The Rise of Digital China....

• Significant educational Internet connectivity...since 1987

• Centuries old warfare doctrine Sun Tzu’s Art of War....孙子的战争艺术

• Net Centric Warfare –
Chinese style.....
Tell me more about these Chinese hackers....

Who are they?

• Communist Party of China (CPC)
• People’s Liberation Army (PLA)
• State Owned Enterprises (SOE)
• Civilian Hackers (Hacktivists)
中共共产党 - CPC

• Communist Party of China codified cyber warfare in 2010
• “protect national infrastructure from external cyber threats” – President Hu Jin tao
• President Hu’s successor Xi Jin ping .... CPC + PLA x information technology superiority = China’s worldwide dominance
人民解放军 - PLA

- Sun Tzu’s ‘The Art of War’ 孙子的战争艺术 – 500B.C.
- 1995 - Father of Chinese Information Warfare – Major General Wang Pu feng
国有企业 - State Owned Enterprises

- China Telecom – owned by the CPC, operated by the PLA
- Huawei – owned by former PLA officer direct links to the PLA however NOT the CPC
- ZTE – based in Shenzhen, Guangdong
- China Petroleum & Chemical Corp
- SinoChem
- China National Petroleum Corp
- China National Pharmaceutical Group
Hacktivists

• Originally supported by CPC & PLA
• Reinforce the PRC’s nationalism via the web
  — Taiwan, the renegade Chinese Province
  - Punishing Japan for WWII war crimes
  - Codera’s anti-Chinese web rhetoric
Origins of Chinese IW

• Sun-Tzu’s Art of War – basis
• Sun Ping’s Military Methods
• Major General Wang Pufeng – founding father of Chinese Information Warfare (IW)
• PLA's IW strategy spearheaded by Major General Dai Qingmin,
• War Without Limits – Senior Colonel’s Qiao Liang & Wang Xiangsui
Official Statement of Chinese IW

- 20 JUL 2010 – ‘ordered by President Hu Jintao to handle cyber threats as China enters the information age, and to strengthen the nation's cyber-infrastructure’³

- The Cyber Warfare ‘Princelings’
  General Zhang Qinsheng 章沁生
  General Chen Bingde 陈炳德
  General Ma Xiaotian 马晓天
  Vice Admiral Sun Jianguo 孙建国
  Major General Hou Shu sen 侯树森

³ PLA Daily, July 20, 2010; [Online] Available at:
http://english.peopledaily.com.cn/200007/21/eng20000721_46068.html
Current Tacticians

• Major General Hu Xiaofeng, Deputy Director for the National Defense University Department of Information Warfare and Training Command

• Professor Meng Xiangqing, National Defense University Institute for Strategic Studies

“goal is to achieve a strategic objective”

“You have to meet my political conditions or your government will be toppled, or you promise to meet some of my political conditions.”

4 The Dark Visitor, 2010; [Online] Available at: http://www.thedarkvisitor.com/category/uncategorized/
Chinese Cyber Warfare History

- May 03, 2001 China warns of massive hack attacks
- 2002 - “informatization”信息化 Chinese Communist Party (CCP) General Secretary and Central Military Commission (CMC) Chairman Jiang Zemin, a speech before the 16th Party Congress
- 2007 – GhostNet 幽灵网
- 2007 - Titan Rain 泰坦雨
- 2008 - Asian web surfers top for time spent online
- 2009 - Operation Aurora 操作极光
- 2009 – Night Dragon 夜龙
- 2010 - Should we be afraid of Chinese hackers?...Or lost cyber war
- 2011 - US needs to get better at preventing foreign access to advanced technology
  - GAO watchdogs find holes in high-tech access, licensing rules

Conclusions

Conclusions include the following:

1) The hegemony of the People’s Republic of China drives the intent to use information warfare in the cyber realm;
2) The use of cyber-warfare is state sponsored;
3) The People’s Liberation Army has a unit assigned to carry out cyber-warfare, known as the ‘Blue Army’
4) There is a significant cultural, economic, historical and linguistic thread throughout the decade plus history of Chinese cyber-warfare;
5) The CPC, although advocating citizen hacking, can no longer control it;
6) Commercial enterprises worldwide are permeable to Chinese cyber hacking in all its form and methods;
7) Similarly, and in particular, the United States Department of Defense cannot defend itself adequately from the various alleged Chinese information warfare threats in the 5th domain of warfare;
8) The composite alleged People’s Republic of China cyber-warfare threat is serious and will only become much worse.....
9) Diplomatic initiatives should be seriously considered in tandem with a show of U.S. military force in ASIA PAC
Who owns the US?
偉大的中國防火牆

• The Great Firewall of China –
  – No one gets out, and no one gets in........
你會說中國普通話……嗎？

看看發生了什麼事！
謝謝您

謝謝您的時間今天
有沒有問題？
Event Description

The Chinese Cyber Threat is becoming synonymous with the Advanced Persistent Threat (APT). Your reality is, or will be very soon, learning how to operate in a compromised state, always vigilant to ferret out the stealthy intruder. The InfoSec professional needs to have a working knowledge of the threat community they are facing in order to accurately assess the risk and advise senior leaders on the proper course of action. This briefing will provide you with the information necessary to assess the risk posed to your organization by the Rising Red Dragon.

The People’s Republic of China, also known as the Middle Kingdom, has a very developed and mature information warfare capability. This fifth dimension of warfare is also known as a cyber warfare capability and includes such acronyms as computer network attack (CNA), computer network exploit (CNE) and computer network vulnerability (CNV).

During this presentation of the Chinese Cyber Warfare phenomena, attendees will receive an introduction to Chinese Warfare, Culture and History. A rapid progression towards the recent decades long development of ‘informatization’ of Sun Tzu’s ancient warfare methodologies will be mapped to Western military principles of war. Present day Communist Party of China (CPC) cyber initiatives, the People’s Liberation Army (PLA) information warfare capabilities and organization will be analyzed. The introduction of civilian hacktivists and Chinese ‘corporations’ into the inculcation of the cyber realm and what it all means to the outside world.

Attendees should consider attending this Chinese Cyber Warfare presentation to better understand the facts vs. the folklore about China and her rather developed cyber and information warfare capabilities.