3-2012

The Advanced Persistent Threat and the Role of Cybersecurity Education

Gary C. Kessler
Embry-Riddle Aeronautical University, kessleg1@erau.edu

EMBRY-RIDDLE Aeronautical University

The Advanced Persistent Threat and the Role of Cybersecurity Education

Gary C. Kessler

March 2012

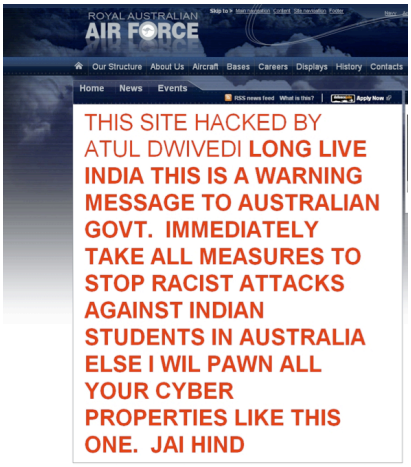
Overview

- The changing face of infowar
- The Advanced Persistent Threat
- Examples of recent cyber attacks
- Mitigation and preparation
- Formalizing the response
- The role(s) of education

The Scope of the Problem

The New Face of Infowar

- Today's information warfare is
  - No longer about pedestrian hackers and Web defacement
  - Being performed by professionals for monetary, political, or ideological gain
  - Not aimed at "crashing the Internet"
  - Designed to use information in an optimal way at the convenience of the attacker
  - Persistent, targeted, adaptable



A Snapshot of Cyber Threats...

- Network Intrusion Of Western Retailer By 'Warcraft,' Resulting In Unauthorized Use Of Customer Credit Cards
- Identification Of Internet Protocol Addresses In A Secure Shell Brute Force Attack On A Nevada-Based Personal Internet Server
- Attempted Recruitment of Money Mules Using Web Sites Registered in China and Hosted in Russia or Ukraine
- Compromise of Identified U.S. Bank Account Via Keylogger, Resulting In Fraudulent Automated Clearing House Transfers Laundering Funds to Ukraine
- Email Solicitation of At-Home Workers Linked to Russian Wire Transfer Service
- Integration of Denial of Service Attacks and Computer Intrusions to Facilitate Unauthorized Wire Transfers from the Account of the Customer of an Internet-Based Business in October 2009
- Malware Worm Infection of Ten Host School Computers
- Theft of Trade Secrets 2009: Potential Targeting by Chinese Actors
- Money Mule Recruitment Using Website Miraclad.com Hosted in Russia, Registered in India, and Exfiltration of Funds to Persons in Poland
- Identification of User Names Exploiting Vulnerability in Microsoft Frontpage to Obtain Personal Information

Source: FBI, March 2010

...And Who's Online

WORLD INTERNET USAGE AND POPULATION STATISTICS
December 31, 2011

World Regions	Population (2011 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2011	Users % of Table
Africa	1,037,524,058	4,514,400	**139,875,242**	13.5 %	2,988.4 %	6.2 %
Asia	3,879,740,877	114,304,000	**1,016,799,076**	26.2 %	789.6 %	44.8 %
Europe	816,426,346	105,096,093	**500,723,686**	61.3 %	376.4 %	22.1 %
Middle East	216,258,843	3,284,800	**77,020,995**	35.6 %	2,244.8 %	3.4 %
North America	347,394,870	108,096,800	**273,067,546**	78.6 %	152.6 %	12.0 %
Latin America / Carib.	597,283,165	18,068,919	**235,819,740**	39.5 %	1,205.1 %	10.4 %
Oceania / Australia	35,426,995	7,620,480	**23,927,457**	67.5 %	214.0 %	1.1 %
WORLD TOTAL	**6,930,055,154**	**360,985,492**	**2,267,233,742**	**32.7 %**	**528.1 %**	**100.0 %**

NOTES: (1) Internet Usage and World Population Statistics are for December 31, 2011. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau and local census agencies. (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local Regulators and other reliable sources. (5) For definitions, disclaimers, and navigation help, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com. Copyright © 2001 - 2012, Miniwatts Marketing Group. All rights reserved worldwide.

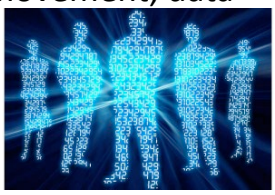
The Advanced Persistent Threat

Advanced Persistent Threat

- An entirely different class of infowar attack
- These attacks may be targeted...
  - They can be deflected for a time, but the attackers do not go away
  - Combine social engineering, technical vulnerabilities, phishing, spearphishing, and other tools in the hacker toolkit
- ...or exploit popular software of no particular value to the attackers
  - Except to spread the fog of war

APT Life Cycle

- Standard intel gathering/exploitation cycle:
  1. Reconnaissance
  2. Initial intrusion into the network
  3. Establish a backdoor into the network
  4. Obtain user credentials
  5. Install various utilities
  6. Privilege escalation, lateral movement, data exfiltration
  7. Maintain persistence



Source: MANDIANT

The Role of the PRC

Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation

Prepared for

The US-China Economic and Security Review Commission

Project Manager
Steve DeWeese 703.556.1086 steve.deweese@ngc.com

Principal Author
Bryan Krekel

Subject Matter Experts
George Bakos
Christopher Barnett

Northrop Grumman Corporation
Information Systems Sector
7575 Colshire Drive
McLean, VA 22102
October 9, 2009

NORTHROP GRUMMAN

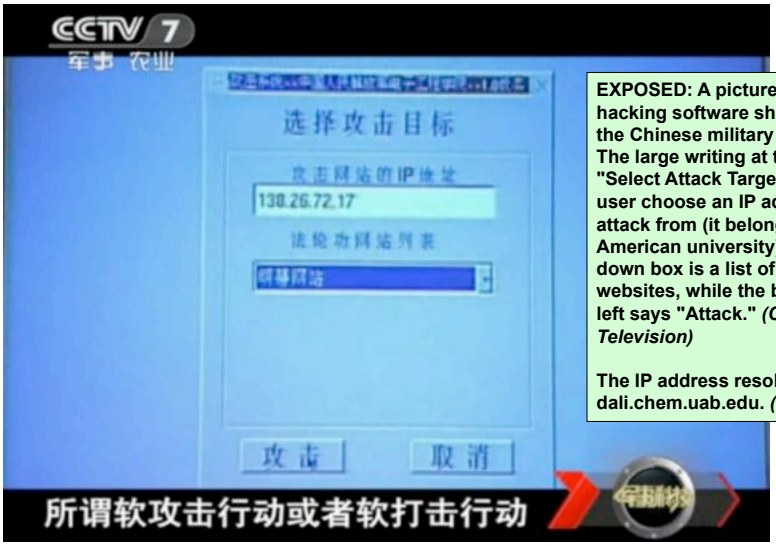
The APT is not a group of rogue hackers; it is state-sponsored information warfare

- The Aurora attack did not target Google's Beijing employees; it targeted the U.S. employees because they had access to the source code

There is evidence that China is developing an Integrated Network Electronic Warfare capability comprising computer network exploitation and attacks, and electronic warfare

- Underground hacker listserves are a recruiting ground

Film at Eleven...



EXPOSED: A picture of the hacking software shown during the Chinese military program. The large writing at the top says "Select Attack Target." Next, the user choose an IP address to attack from (it belongs to an American university). The drop-down box is a list of Falun Gong websites, while the button on the left says "Attack." *(China Central Television)*

The IP address resolves to dali.chem.uab.edu. *(GCK)*

Source: *The Epoch Times*

But is *Everything* an APT?

- Mid-December 2009 cyber attack
  - Disclosed by Google in January 2010, although there are reportedly dozens of other targets (including Adobe Systems and Juniper Networks)
  - Originated in China
    - Google stated that its IP had been stolen and the accounts of Chinese dissidents targeted
  - MacAfee reported attack exploited zero-day vulnerability in Internet Explorer
    - Although not publically disclosed, the vulnerability had been known by Microsoft since September 2009
  - VeriSign reports that attacks launched by "agents of the Chinese state or proxies thereof"

Stuxnet

- Discovered June 2010
  - A computer worm exploiting a flaw in Windows but targeting Siemens supervisory control and data acquisition (SCADA) systems
    - A programmable logic controller (PLC) rootkit
  - Primary target was specific centrifuge models at Iranian nuclear research facilities
    - 59% of victims were in Iran, 18% in Indonesia
  - Highly-specific attack, probably state-sponsored
    - First variant appeared in June 2009
    - Second variant appeared in early 2010
    - Speculation that the discovery was inadvertant and that Stuxnet was supposed to remain covert until needed

HBGary
Detecting Tomorrow's Threats Today

- Reported February 2011
  - WikiLeaks posts *Collateral Murder* video, 260K U.S. diplomatic cables, *Afghan War Diary* (92K documents), and *Iran War Logs* (400K documents) (Jan.-Oct., 2010)
  - Many sites halt all dealings with WikiLeaks
  - *Anonymous* hacker group launches DoS attacks on anti-WikiLeaks offenders
  - HBGary Federal announces that they know the identity of *Anonymous* members
  - *Anonymous* launches social engineering attack, coupled with SQL injection, on HBGary Federal, eventually acquiring ~70K corporate and customer e-mail messages

RSA

- Reported March 2011
  - Phishing e-mails sent to low-level employees

  - Attachment contained a zero-day exploit in Adobe Flash, allowing installation of Poison Ivy RAT
  - Accessed corporate network, escalated privileges, acquired information, and compromised RSA SecureID tokens
    - ~50M hardware tokens and ~250M smartphone apps

- Sony PlayStation Network (PSN) hack (April 2011)
  - PSN and Qriocity network down
  - Over a two-week period, Sony incrementally reports network failures, that the network was hacked, it is being rebuilt, personal information might have been compromised, and credit card information was lost
  - 19 year old arrested in U.K. (June 2011)
- Sony Pictures databases attacked (June 2011)
  - Two *LulzSec* members arrested (Sept. 2011)

Operation Shady RAT

- Reported August 2011
  - "Five year targeted operation by one specific actor" reported by McAfee
    - More than 70 organizations in 14 countries were targeted, including U.N., IOC, defense contractors, and businesses
    - The "actor" is reported to be China
  - Is this an APT?
    - Some said that McAfee is being "alarmist" because Shady RAT is neither new nor sophisticated
    - McAfee observes that it was effective!

Anonymous

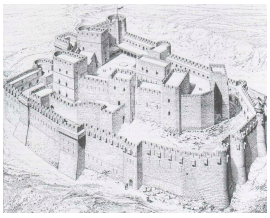
- Staging Internet hacktivism since 2003
- Came into recent popular awareness due to mainstream negative responses to WikiLeaks and Occupy Wall Street
- Attacks, threats, and Web defacement targets in 2012 include CIA, FBI, police departments*, Greek and U.S. DOJ, the Vatican, Interpol, and InfraGard...
  - ...and neo-Nazi and Syrian government sites
- The amorphous, constant nature of Anonymous... is this an APT?

*** including Burlington (VT) P.D.**

Mitigation and Preparation

Getting Back to Basics

- New technological solutions will be needed but we are already underutilizing current technologies
  - Ingress filtering by ISPs
  - Least privilege
  - Separation of duties
  - MAC, DAC, RBAC
  - Network-based *and* host-based protection
  - Multi-factor authentication
  - *Virtual VPNs?*



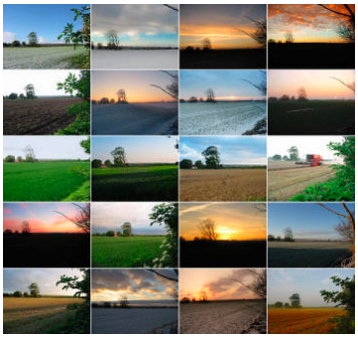
- Best defense will continue to be defense-in-depth, biodiversity, and redundancy... and education
- Prioritize issues for a remediation strategy

Basic Defense 101

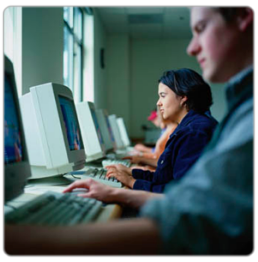
- What are your information resources?
- Where is the greatest threat likelihood?
  - I.e., what are the best targets and who are the potential attackers?
- Think like an adversary
  - If you were attacking your own network, with all you knew about your network, what would you do?
  - Get outside of your cultural, moral, ethical, social, and legal box
- "There are no secure sites on the Internet, only vigilant ones." (S.O. Bradner)

The Landscape is Changing

- Traditional networks are morphing into
  - Thin clients
  - Mobile computing
  - Cloud computing
  - Web-based storage
- Information leakage will continue to grow, largely driven by Web 2.0
- Data will continue to become more portable
- Networks will continue to be increasingly porous



The Role of the Users



- Technology cannot defend against new social engineering attacks -- both online and offline -- that target humans
- Problems can be mitigated with *education*
  - Less so by *training*
  - We need to make users part of the solution!
- On where should burden lie for protection -- networks or users?
  - E.g., highways. People know how to drive but they are neither mechanics nor road designers
  - E.g., boating. There are no lanes, just rules of the road!

The IA Culture Needs to Change

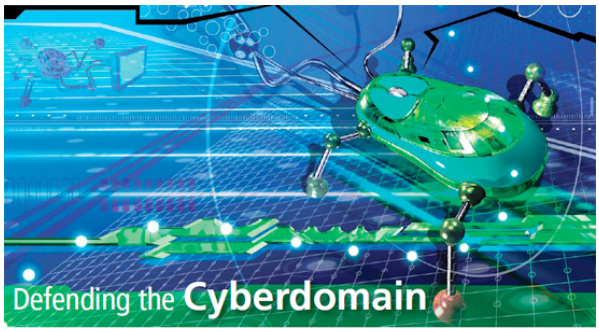
- Information security has been a problem since the inception of information!
- The face of the infosec adversary is changing
  - Our approach to securing information has to be fluid and dynamic
  - Defenders will always lag behind the attackers
- Information is an organizational asset; thus...
  - Recognize information security as a business need
  - Do **not** outsource infosec if at all possible
- **Protect data; not networks, not computers**

Where To From Here?

- The "APT" term ***is*** probably being overused
- That said, the ***threat*** is real and our adversaries are escalating the types of attacks, the tools, and their persistence
- If someone can attack Sony, HBGary, RSA, et al. at will, can they successfully attack *you*??

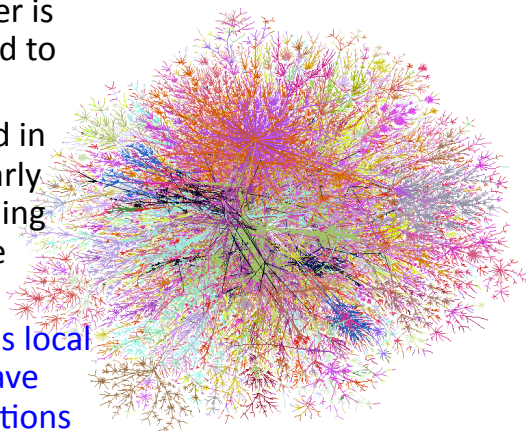
- Our response must be two-pronged
  - Implementation and policy (technology)
  - Strategy and tactics (analysis and intel)

Formalizing the Response

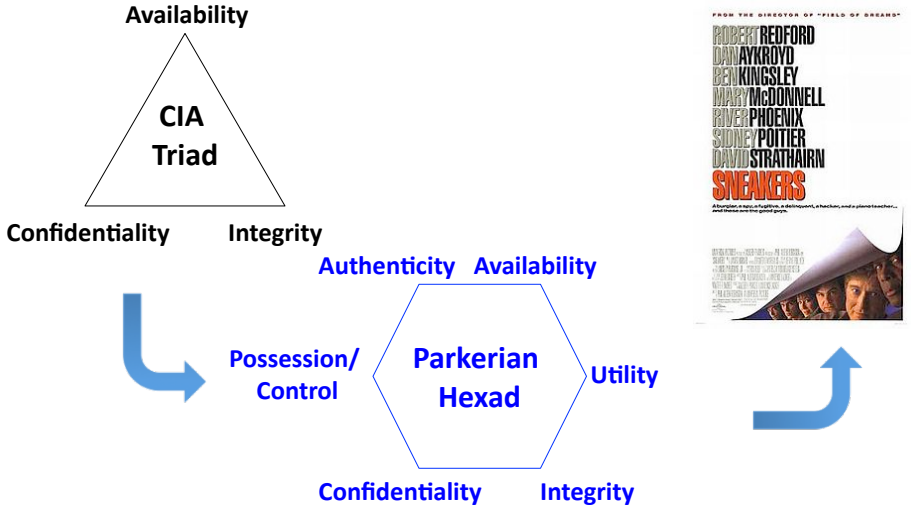


The Nature of Networks

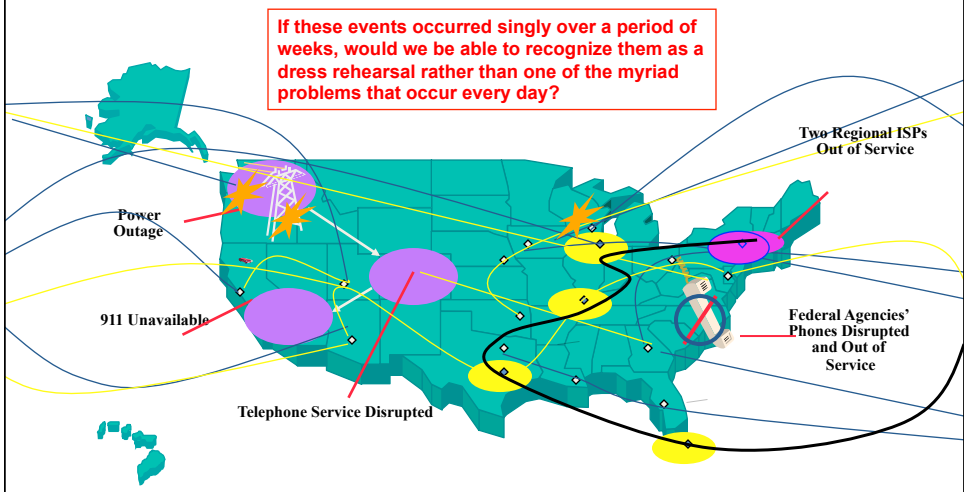
- The only secure computer is one that is not connected to another computer
- The Internet has resulted in the intertwingling of nearly every computer -- including smartphones -- onto one global network
- All information security is local but the attack vectors have national defense implications



Basic Tenets of Infosec



Synthesize This...



The Federal Response

The Clinton Administration's Policy on Critical Infrastructure Protection:

Presidential Decision Directive 63

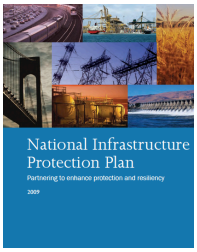
May 22, 1998

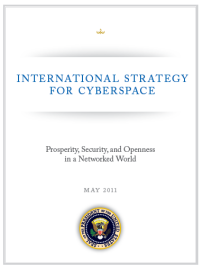
Homeland Security Presidential Directive-7

December 17, 2003

SUBJECT: Critical Infrastructure Identification, Prioritization, and Protection

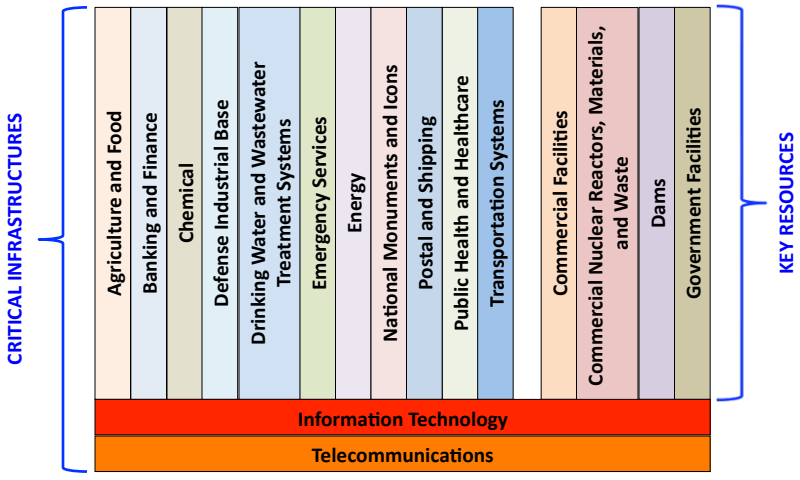
- **InfraGard* formed by FBI, 1997**
- **NIPC formed under the FBI, 1998**
- **NIAC formed under DHS, 2001**





* http://www.infragard-jax.org/

Critical Infrastructures*



National Infrastructure Protection Plan

* >85% owned by the private sector

The Role Of Education

ERAU Homeland Security Program Mission Statement

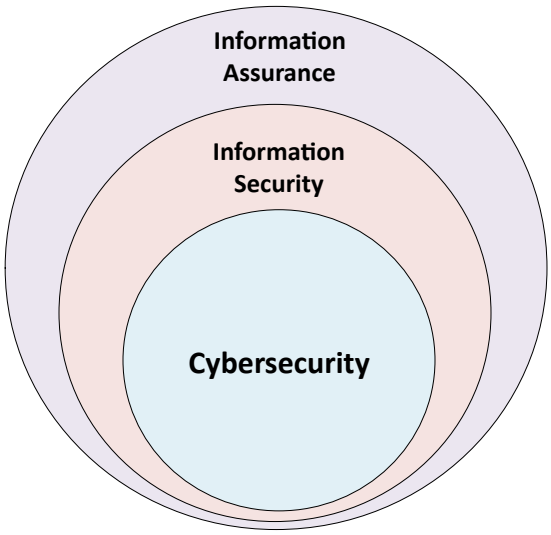
It is the *purpose* of the Homeland Security Program at Embry-Riddle Aeronautical University to **enhance and expand the discipline of homeland security** by **developing and delivering the highest quality academic and professional program in the field**. Academic courses, projects and field experiences are designed to **provide exposure to concepts, procedures, and operations consistent with those found within agencies and organizations charged with providing homeland security for this nation**.

DHS Cybersecurity Mission

The growing number of attacks on our cyber networks has become, in President Obama's words, "one of the most serious economic and national security threats our nation faces." The Department of Homeland Security plays an important role … to keep our federal civilian networks secure, and secure the cyberspace and critical infrastructure on which we all depend. That means working across the federal government, partnering with the private sector, and empowering the general public to create a safe, secure, and resilient cyber environment, and promote cybersecurity knowledge and innovation.

http://www.dhs.gov/cyber

What's In A Name?



Perspectives on *Information Security*

- Several different ways in which to approach the practice of infosec
  - Proactive (infosec) vs. reactive (incident response, digital forensics)
  - Offensive (info ops) vs. defensive (defense-in-depth)
  - Public policy vs. organizational implementation
  - Public sector vs. private sector

Approaches to Education

- Undergraduate level
  - B.S., Information Security
    - *Focus is on technology and implementation*
    - Subject matter includes system administration, software engineering, network technology and protocols, infosec technology
  - B.S., Homeland Security w/ cybersecurity concentration
    - *Focus is on threat analysis and protection*
    - Subject matter includes Infosec technology and policy, public policy and the law, critical infrastructure planning, anti-terrorism and intelligence gathering, business continuity

- Graduate level
  - M.S., Information Security
    - *Focus is on computer science and engineering*
    - Subject matter includes next generation tools, algorithms, methodologies
  - M.S., Information Security Management
    - *Focus is on managing the process and organization*
    - Subject matter includes analysis, policies, procedures, interaction with an organization, strategy and tactics, personnel, business practices, technology, leadership

Centers of Academic Excellence

- CAE in Information Assurance Education
  - NSA, DHS
- Centers of Digital Forensics Academic Excellence
  - DoD, DHS
- Intelligence Community CAEs
  - Office of the Director of National Intelligence
- Homeland Security Centers of Excellence
  - DHS
  - *Note: Projects and research, not education*

It's Like Herding Fish...

Anyone who thinks that technology can solve all of their problems does not understand technology or their problems.

A paraphrase by GCK

Further Reading

Alperovitch, D. (2011). *Revealed: Operation Shady RAT*. Santa Clara, CA: McAfee, Inc. Retrieved from http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

Dharmakumar, R., & Prasad, S. (2011, September 19). Hackers' Haven. *Business.in.com* Web site. Retrieved from http://business.in.com/article/boardroom/hackers-haven/28462/0

Gross, M.J. (2011, September). Enter the Cyber-dragon. *Vanity Fair online*. Retrieved from http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109

Krekel, B. (2009, October 9). *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. McLean, VA: Northrup Grumman Corp., Information Systems Sector. Retrieved from http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

Mandiant. (2010). *M-Trends: The Advanced Persistent Threat*. Washington, D.C.: Mandiant Corp. Retrieved from http://www.princeton.edu/~yctwo/files/readings/M-Trends.pdf

Robertson, M., & Zhu, H. (2011, August 28). Slip-Up in Chinese Military TV Show Reveals More Than Intended. *The Epoch Times*. Retrieved from http://www.theepochtimes.com/n2/china-news/slip-up-in-chinese-military-tv-show-reveals-more-than-intended-60619.html

Author Contact Information

Gary C. Kessler, Ph.D., CCE, CISSP
GARY KESSLER ASSOCIATES
2 Southwind Drive
Burlington, VT 05401

mobile: **+1 802-238-8913**
e-mail: **gck@gary*kessler.net***
Skype: ***gary.c.kessler***

http://www.garykessler.net
http://www.vtinfragard.org

http://www.garykessler.net/presentations

Acronyms and Abbreviations

APT	Advanced persistent threat
CAE	Center of Academic Excellence
CIA	Central Intelligence Agency *or* Confidentiality, integrity, availability
DAC	Discretionary access control
DHS	Department of Homeland Security
DoD	Department of Defense
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
IA	Information assurance
IOC	International Olympic Committee
IP	Internet Protocol
ISP	Internet service provider
K	Thousand (10^3) *or* kilo (2^{10})
M	Million (10^6) *or* mega (2^{20})
MAC	Mandatory access control
NIAC	National Infrastructure Advisory Council
NIPC	National Infrastructure Protection Center
NSA	National Security Agency
PRC	People's Republic of China
RAT	Remote access trojan
RBAC	Role-based access control
SQL	Structured Query Language
UN	United Nations
VPN	Virtual private network