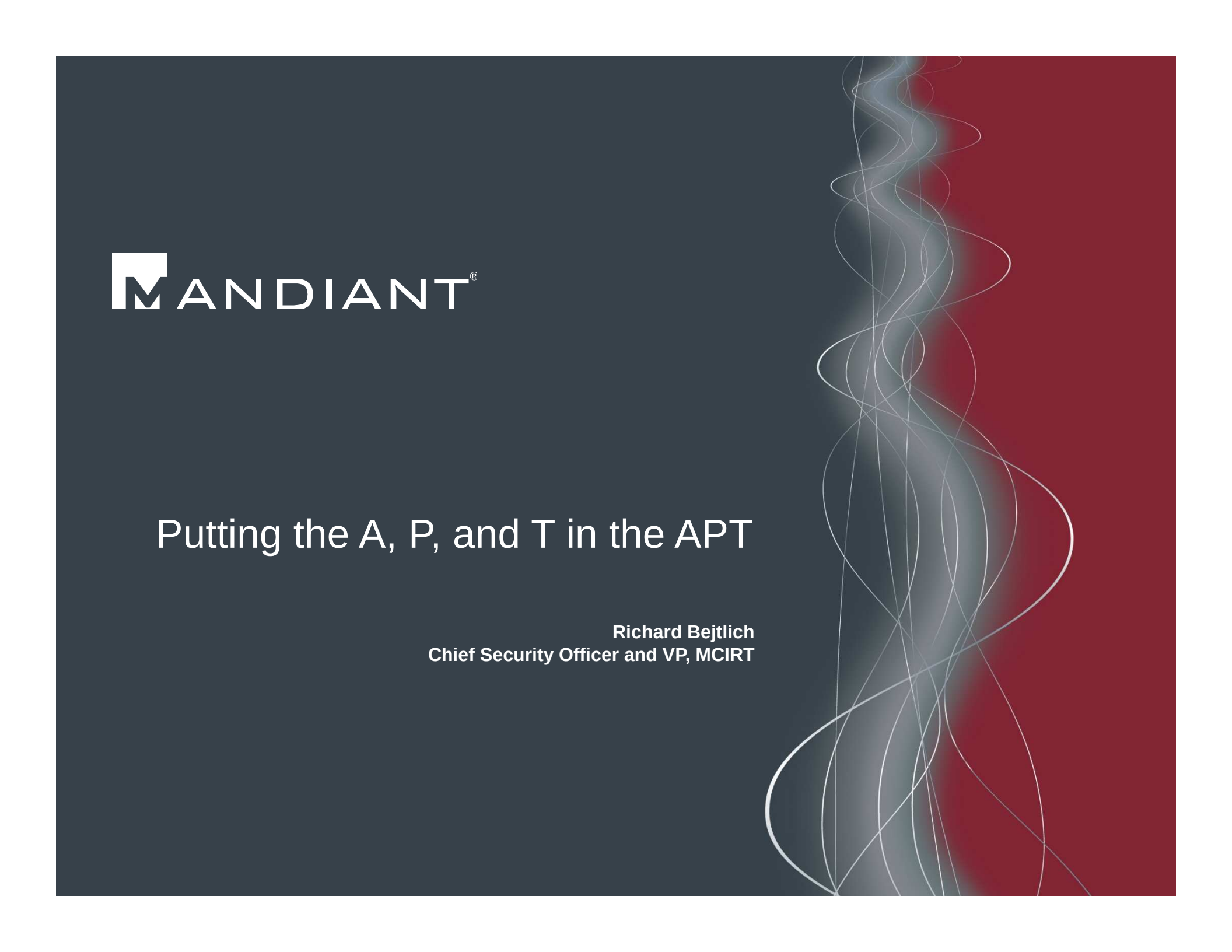
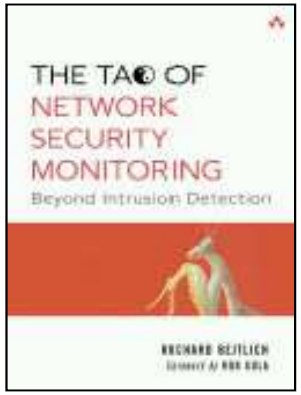


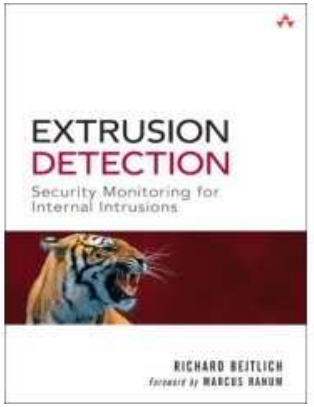
Putting the A, P, and T in the APT

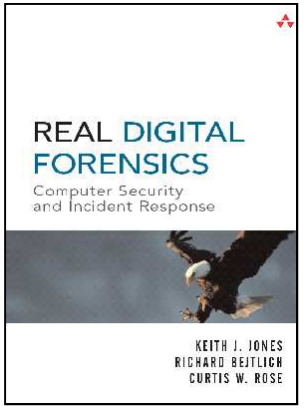
Richard Bejtlich
Chief Security Officer and VP, MCIRT

Bejtlich Biography

- Bejtlich ("bate-lik") biography
  - Mandiant (11-present)
  - General Electric, (07-11)
  - TaoSecurity (05-07)
  - ManTech (04-05)
  - Foundstone (02-04)
  - Ball Aerospace (01-02)
  - Captain at US Air Force CERT (98-01)
  - Lt at Air Intelligence Agency (97-98)
- Author
  - Tao of Network Security Monitoring: Beyond Intrusion Detection (solo, Addison-Wesley, Jul 04)
  - Extrusion Detection: Security Monitoring for Internal Intrusions (solo, Addison-Wesley, Nov 05)
  - Real Digital Forensics (co-author, Addison-Wesley, Sep 05)
  - Contributed to Incident Response, 2nd Ed and Hacking Exposed, 4th Ed
  - TaoSecurity Blog (http://taosecurity.blogspot.com) & @taosecurity

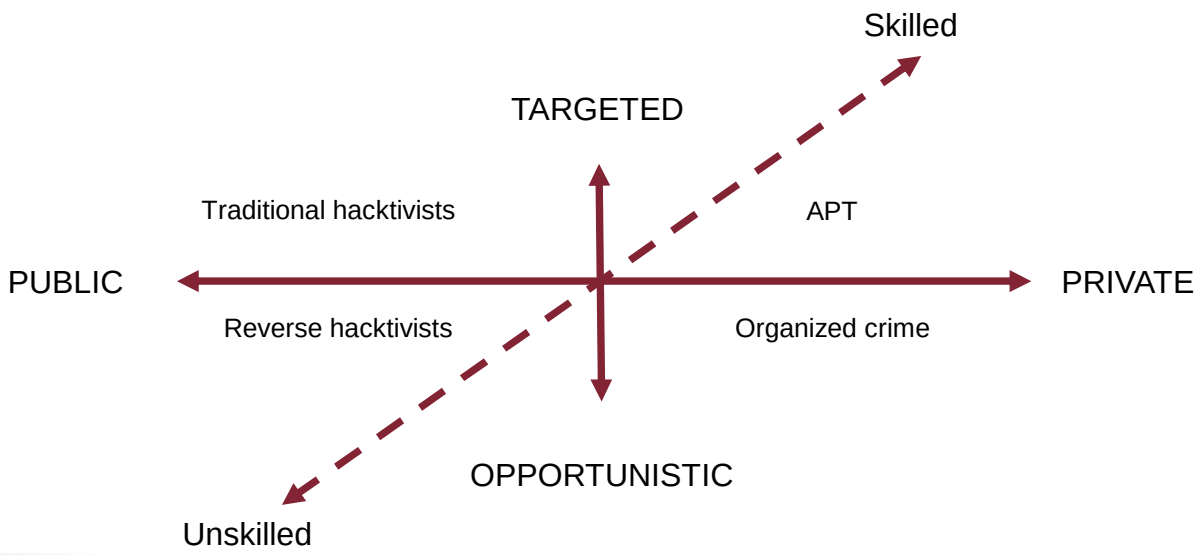






Risk and Threat Groups

- Risk = f(Threat, Vulnerability, Asset)
  - Threats occupy different dimensions
  - Vulnerability is pervasive
  - Any online resource is an asset



Advanced Persistent Threat

http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14_gci1516312,00.html

APT in the Private Arena

TIME
IN PARTNERSHIP WITH CNN

SEARCH TIME.COM

U.S.

Main • The Page • Politics • Swampland • Assignment Detroit • The Detroit Blog
White House Photo Blog • Videos

The Invasion of the Chinese Cyberspies

By NATHAN THORNBURGH/WASHINGTON Monday, Aug. 29, 2005

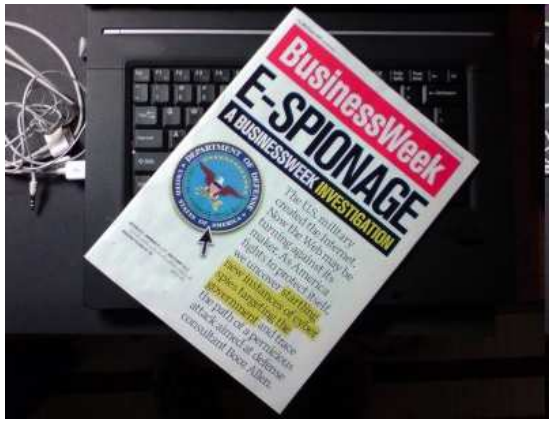
More on TIME.com

Fall Entertainment Preview 2010

PRINT EMAIL MORE

It was another routine night for Shawn Carpenter. After a long day analyzing computer-network security for Sandia National Laboratories, where much of the U.S. nuclear arsenal is designed, Carpenter, 36, retreated to his ranch house in the hills overlooking Albuquerque, N.M., for a quick dinner and an early bedtime. He set his alarm for 2 a.m. Waking in the dark, he took a thermos of coffee and a pack of Nicorette gum to the cluster of computer terminals in his home office. As he had almost every night for the previous four months, he worked at his secret volunteer job until dawn, not as Shawn Carpenter, mid-level

APT in the Public Arena



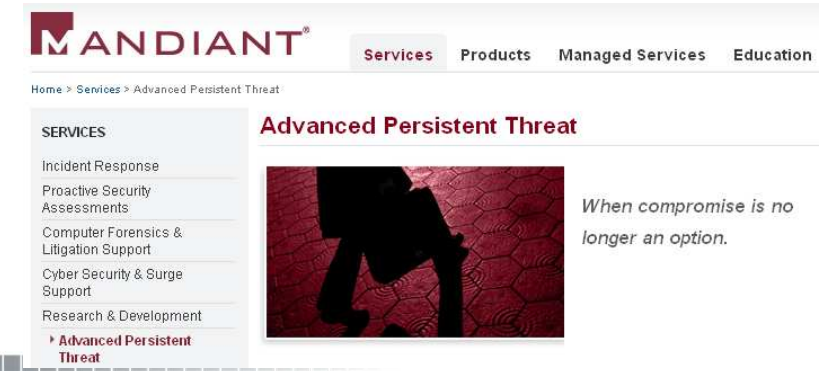
BusinessWeek April 2008

Friday, July 10, 2009

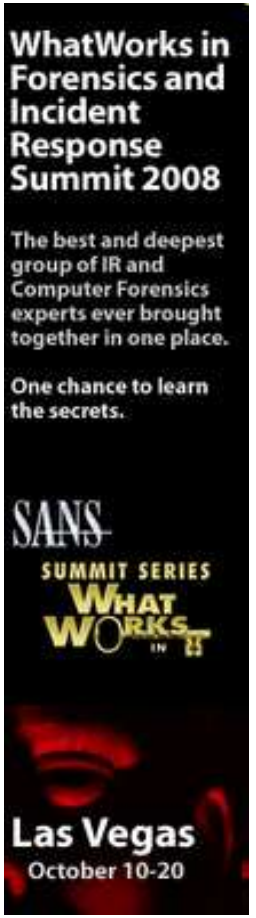
You Down with APT?

Today I had shared a phone call with a very knowledgable and respected security industry analyst. During the course of the conversation he made a few statements which puzzled me, so I asked him "do you know what APT means?" He might have thought I was referring to the Debian Advanced Package Tool or apt, but that's not what I meant. When I said Advanced Persistent Threat, it still didn't ring any bells with him. I decided to do some searching on the Web to see what was available regarding APT.

TaoSecurity Blog July 2009
(first APT post October 2007)



SANS Forensics
and IR Summit
October 2008



MANDIANT
Webcasts in
Summer 2008

Google Blog Post Jan 2010

The Official Google Blog

Insights from Googlers into our products, technology, and the Google culture.

A new approach to China

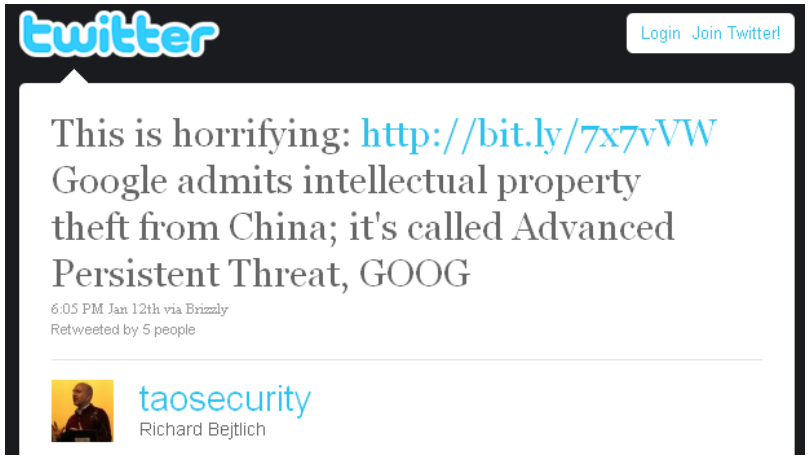
1/12/2010 03:00:00 PM

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident--albeit a significant one--was something quite different.

First, this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors--have been similarly targeted. We are currently in the process of notifying those companies, and we are also working with the relevant U.S. authorities.

First, this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors--have been similarly targeted...

In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google...



http://twitter.com/taosecurity/status/7692969460

Who is the APT and Is It Cyberwar?

"The Aggressive Threat"

"The Stealthy Threat"

Economist
July 2010

APT and Two-Dimensional Thinking

- Offender
- Defender
- Means
- Motive
- Opportunity

Attribution Is Not Just Malware

- **Timing**. What is the timing of the attack, i.e., fast, slow, in groups, isolated, etc.?
- **Victims or targets**. Who is being attacked?
- **Attack source**. What is the technical source of the attack, i.e., source IP addresses, etc.?
- **Delivery mechanism**. How is the attack delivered?
- **Vulnerability or exposure**. What service, application, or other aspect of business is attacked?
- **Exploit or payload**. What exploit is used to attack the vulnerability or exposure?
- **Weaponization technique**. How was the exploit created?
- **Post-exploitation activity**. What does the intruder do next?
- **Command and control method**. How does the intruder establish command and control?
- **Command and control servers**. To what systems does the intruder connect to conduct command and control?

Attribution Is Not Just Malware (cont)

- **Tools**. What tools does the intruder use post-exploitation?
- **Persistence mechanism**. How does the intruder maintain persistence?
- **Propagation method**. How does the intruder expand control?
- **Data target**. What data does the intruder target?
- **Data packaging**. How does the intruder package data for exfiltration?
- **Exfiltration method**. How does the intruder exfiltrate data?
- **External attribution**. Did an external agency share attribution data based on their own capabilities?
- **Professionalism**. How professional is the execution, e.g., does keystroke monitoring show frequent mistakes, is scripting used, etc.?
- **Variety of techniques**. Does the intruder have many ways to accomplish its goals, or are they limited?
- **Scope**. What is the scope of the attack? Does it affect only a few systems, many systems?

APT Timeline

- Late 1990s - military victims
- 2000-2004 - non-military government victims
- 2005-2009 - defense industrial base
- 2009-present - intellectual property-rich targets and software companies

APT Objectives

- **Political:** maintaining internal stability.
- **Economic:** steal intellectual property from victims. Such IP can be cloned and sold, studied and underbid in competitive dealings, or fused with local research to produce new products and services more cheaply than the victims.
- **Technical:** further their ability to accomplish their mission. These include gaining access to source code for further exploit development, or learning how defenses work in order to better evade or disrupt them.
- **Military:** identifying weaknesses that allow inferior military forces to defeat superior military forces.


2001

중국 젠-20과 F-22 랩터 비교

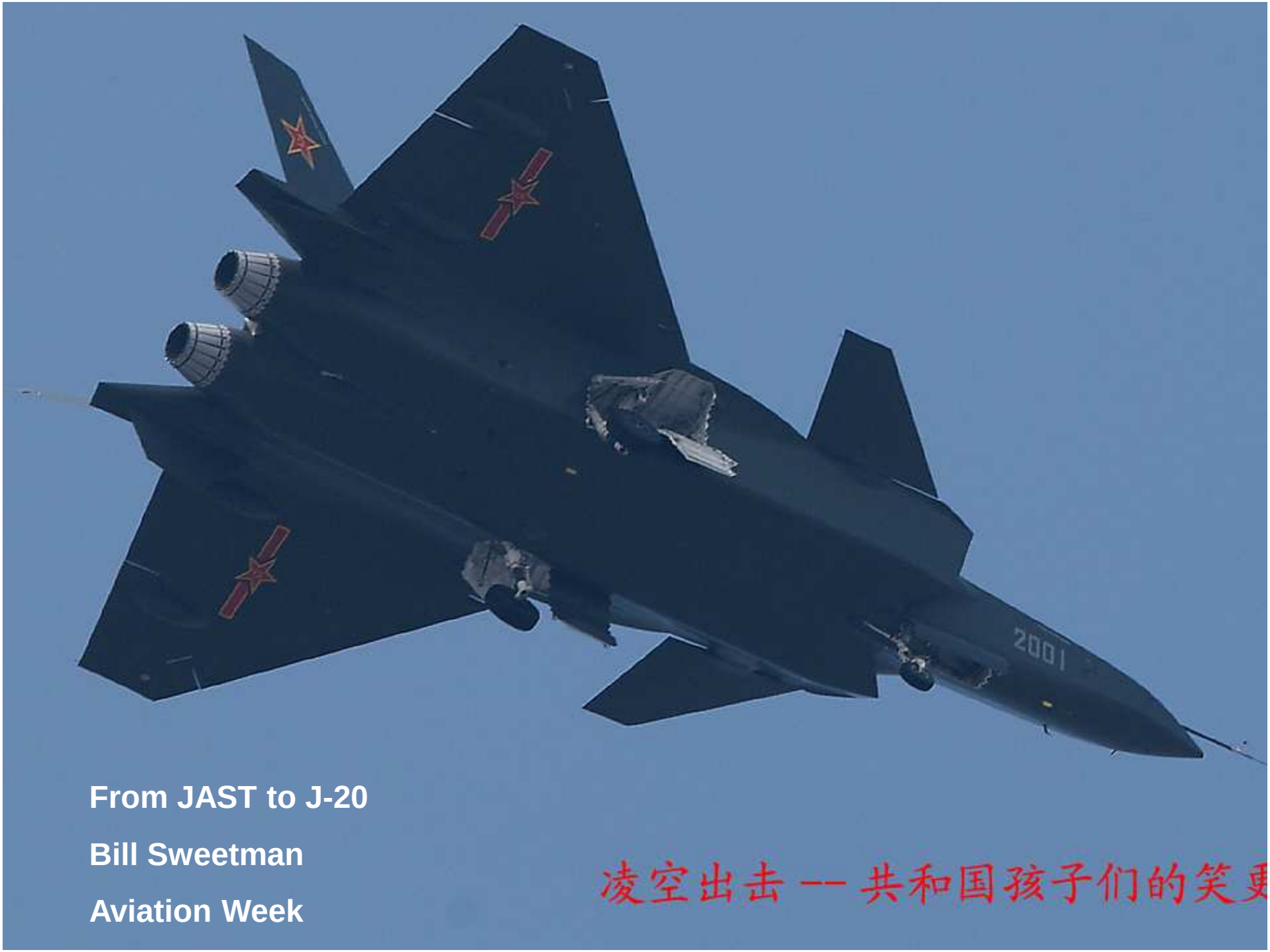
젠-20

F-22

중국	제작사	美 보잉, 록히드 마틴
약 21m(추정)	길이	18.9m
미상	높이	5.08m
미상	날개폭	13.56m
미상	최대속도	마하 1.8
미상	작전반경	759km
스텔스 기능	특징	스텔스 기능
2017년(예정)	실전배치	2006년
미상(공중급유 통해 장거리 비행 가능)	항속거리	3,218km
개량형 WS 엔진(추정)	엔진	2X프랫 앤 휘트니 F119-PW-100 피치(Pitch) 추력 편향 터보팬
장거리 순항미사일 등	주요무기	6xAIM-120 암람 및 2xAIM-9 사이드와인더 미사일, 2 X 1,000 lb (450 kg) JDAM 폭탄 등

자료/'간와아주방무월간', 미 국방부

MARINES



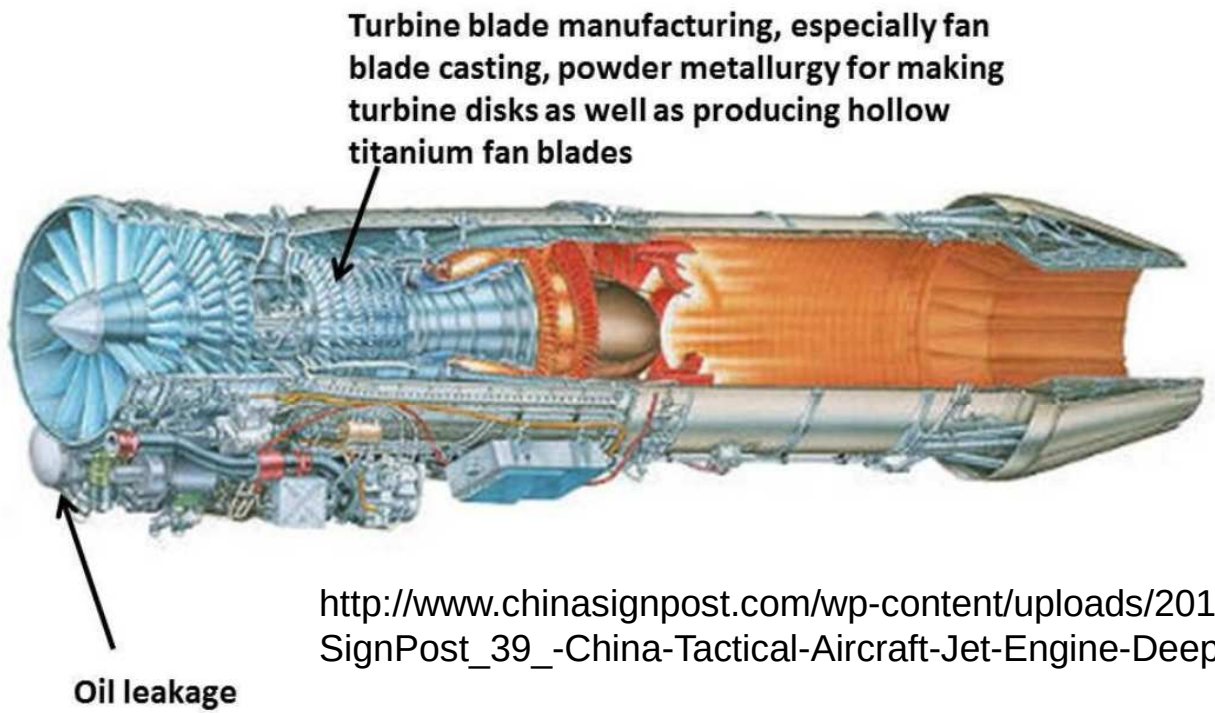
From JAST to J-20

Bill Sweetman

Aviation Week

Example: Business Methods

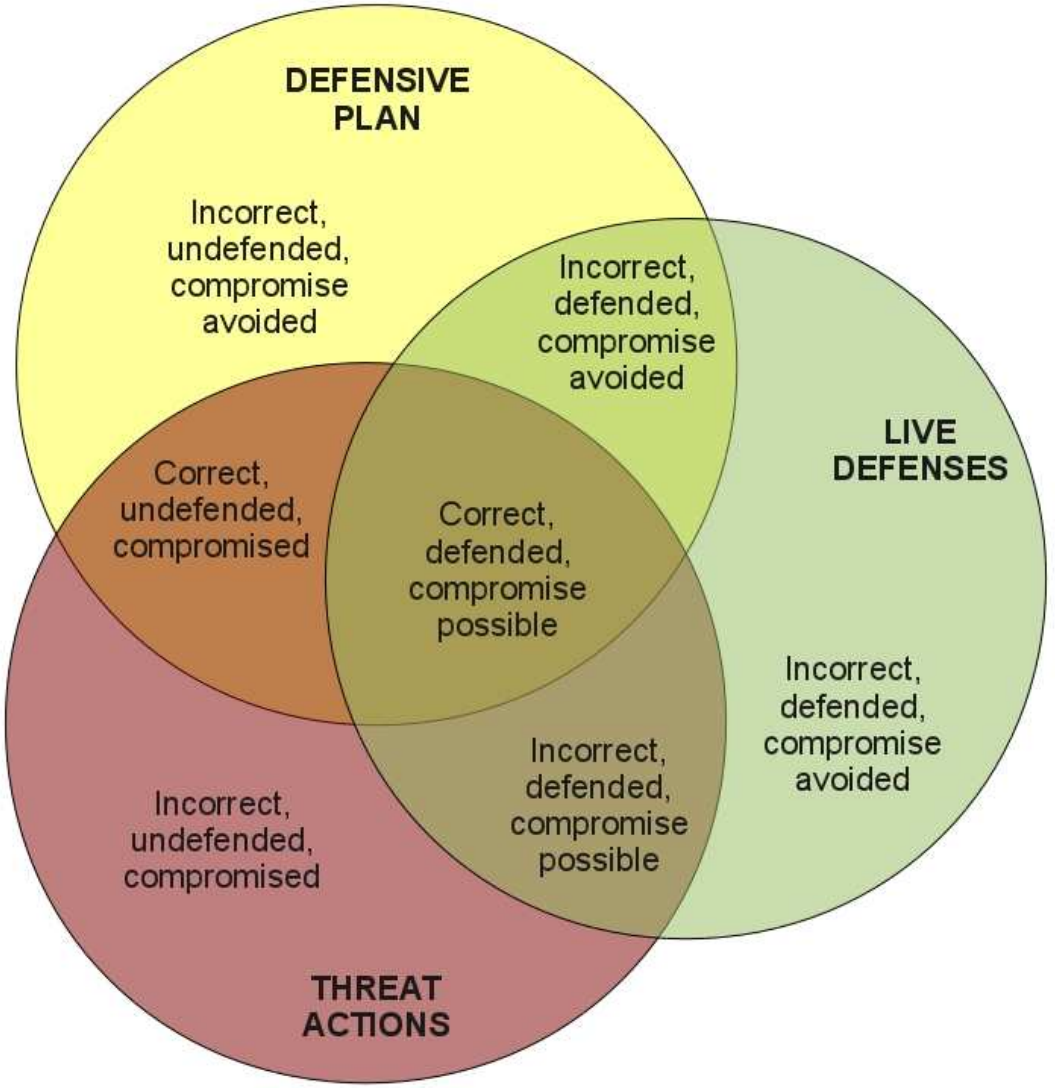
Exhibit 3: Where China's Military Jet Engine Makers Continue to Experience Problems



http://www.chinasignpost.com/wp-content/uploads/2011/06/China-SignPost_39_-China-Tactical-Aircraft-Jet-Engine-Deep-Dive_20110626.pdf

Overall: Weak process standardization and over-reliance on individual machine operators' skill & experience causes lack of consistent engine quality. Heavy emphasis on promoting better process standardization, more automated production processes, and improved training of workers.

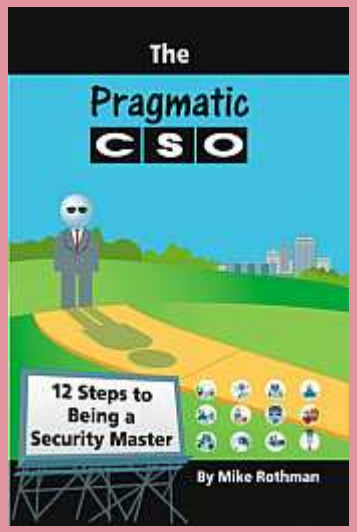
TaoSecurity Security Effectiveness Model



What to Do About APT

- Defensible Network Architecture (2.1)
  - Monitored
  - Inventoried
  - Controlled
  - Claimed
  - Minimized
  - Assessed
  - Current
  - Measured

Related, but separate:



www.pragmaticcso.com

Ref: taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html

Reliable Sources

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

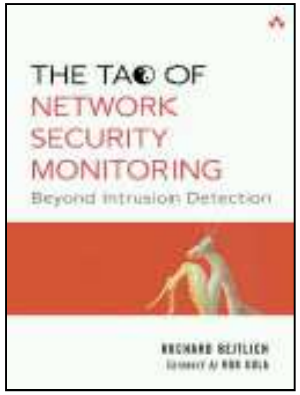
NORTHROP GRUMMAN

http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

http://www.mandiant.com/products/services/m-trends

What to Do About APT

- Talk to the FBI
- Talk to peers
- Educate the enterprise
- Build a CIRT, not just a SOC
- Instrument your enterprise at the network, host, and application levels
- Accelerate your security analysts



MCIRT
ADVANCED DETECTION AND RESPONSE SERVICES