



*EPA  
Environmental  
Information Symposium*

*Emerging Cyber Threats  
to Critical Infrastructure*

*SSA Brian Herrick  
FBI Philadelphia*



# Federal Bureau of Investigation

---

## *Cyber Crime Program Philadelphia Division*

*Supervisory Special Agent Brian T. Herrick*

***EPA  
Environmental Information Symposium  
May, 2010***

# My Background

---



- FBI Agent since 2002
- Transferred to Philadelphia from Buffalo, NY field office
- Cyber Agent and Forensic Examiner
- Prior Life: IT Director
- Adjunct Professor: West Chester Univ.
- BA and MA: Villanova University
- MBA: West Chester University

# Agenda

---

**Overview of the FBI**

**Cyber Crime**

**Current Threat Climate**



# FBI Priorities

---

1. International/Domestic Terrorism
2. Foreign Counterintelligence
3. Cyber Crime
4. Public Corruption
5. Civil Rights
6. Transnational Criminal Enterprise
7. White Collar Crime
8. Violent Crime

## WORLD INTERNET USAGE AND POPULATION STATISTICS

World Regions	Population ( 2009 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2009	Users % of Table
<a href="#">Africa</a>	991,002,342	4,514,400	86,217,900	8.7 %	1,809.8 %	4.8 %
<a href="#">Asia</a>	3,808,070,503	114,304,000	764,435,900	20.1 %	568.8 %	42.4 %
<a href="#">Europe</a>	803,850,858	105,096,093	425,773,571	53.0 %	305.1 %	23.6 %
<a href="#">Middle East</a>	202,687,005	3,284,800	58,309,546	28.8 %	1,675.1 %	3.2 %
<a href="#">North America</a>	340,831,831	108,096,800	259,561,000	76.2 %	140.1 %	14.4 %
<a href="#">Latin America/Caribbean</a>	586,662,468	18,068,919	186,922,050	31.9 %	934.5 %	10.4 %
<a href="#">Oceania / Australia</a>	34,700,201	7,620,480	21,110,490	60.8 %	177.0 %	1.2 %
<b>WORLD TOTAL</b>	6,767,805,208	360,985,492	1,802,330,457	26.6 %	399.3 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics are for December 31, 2009. (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](#) . (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, disclaimer, 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](http://www.internetworldstats.com). Copyright © 2001 - 2010, Miniwatts Marketing Group. All rights reserved worldwide.

# LEGAL ATTACHE OFFICES

Abu Dhabi	Canberra	Paris
Almaty	Copenhagen	Prague
Amman	Honk Kong	Pretoria
Ankara	Islamabad	Rabat
Athens	Kabul	Riyadh
Baghdad	Kiev	Rome
Bangkok	Kuala Lumpur	Sanaa
Beijing	Lumpur	Santiago
Berlin	Lagos	Santo Domingo
Bern	London	Sarajevo
Bogotá	Madrid	Singapore
Brasilia	Manila	Sofia
Bridgetown	Mexico City	Tallinn
Brussels	Moscow	Tbilisi
Bucharest	Nairobi	Tel Aviv
Buenos Aires	New Delhi	Tokyo
Cairo	Ottawa	Vienna
	Panama City	Warsaw
		<b>Australia</b>



## The Cyber Division established the following priorities for Computer Crime Investigations:

---

- 1. Cyber/Computer Intrusion
  - A) Counterterrorism
  - B) Counterintelligence
  - C) Criminal
  
- 2. Online Sexual Exploitation of Children
- 3. Theft of Intellectual Property
- 4. Internet Fraud
- 5. Identity Theft

**These Cyber priorities are universal for the entire FBI**

# Terrorists Groups



**NEWS OF THE  
PEOPLE'S WAR**



# Terrorist Groups

---

- Terrorist groups are using information technology
- Terrorists possess the will and can easily obtain the means to attack IT targets
- Potential for major cyber attacks is very high



# Information Warfare

## 孫子兵法

"... attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence."

-Sun Tzu, The Art of War c. 350 B.C.



## People's Liberation Daily



**“An adversary wishing to destroy the United States only has to mess up the computer systems of its banks by hi-tech means. This would disrupt and destroy the US economy.”**

**February, 1996**

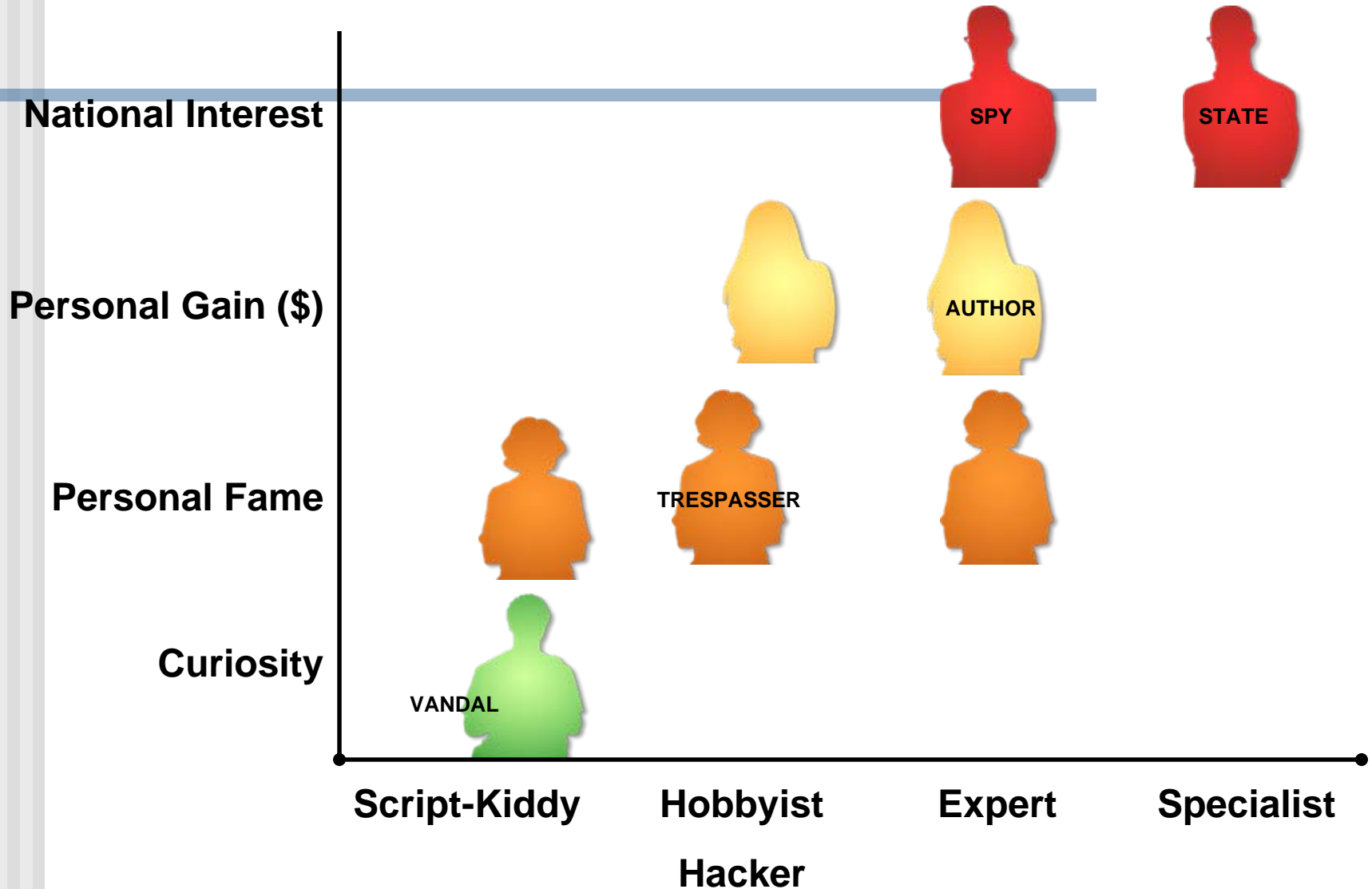
# Nation States: China

*"Chinese Cyber Invaders May be After Defense Logistics"*  
*The SANS Institute [NewsBites @sans.org](SANS, 2006)*

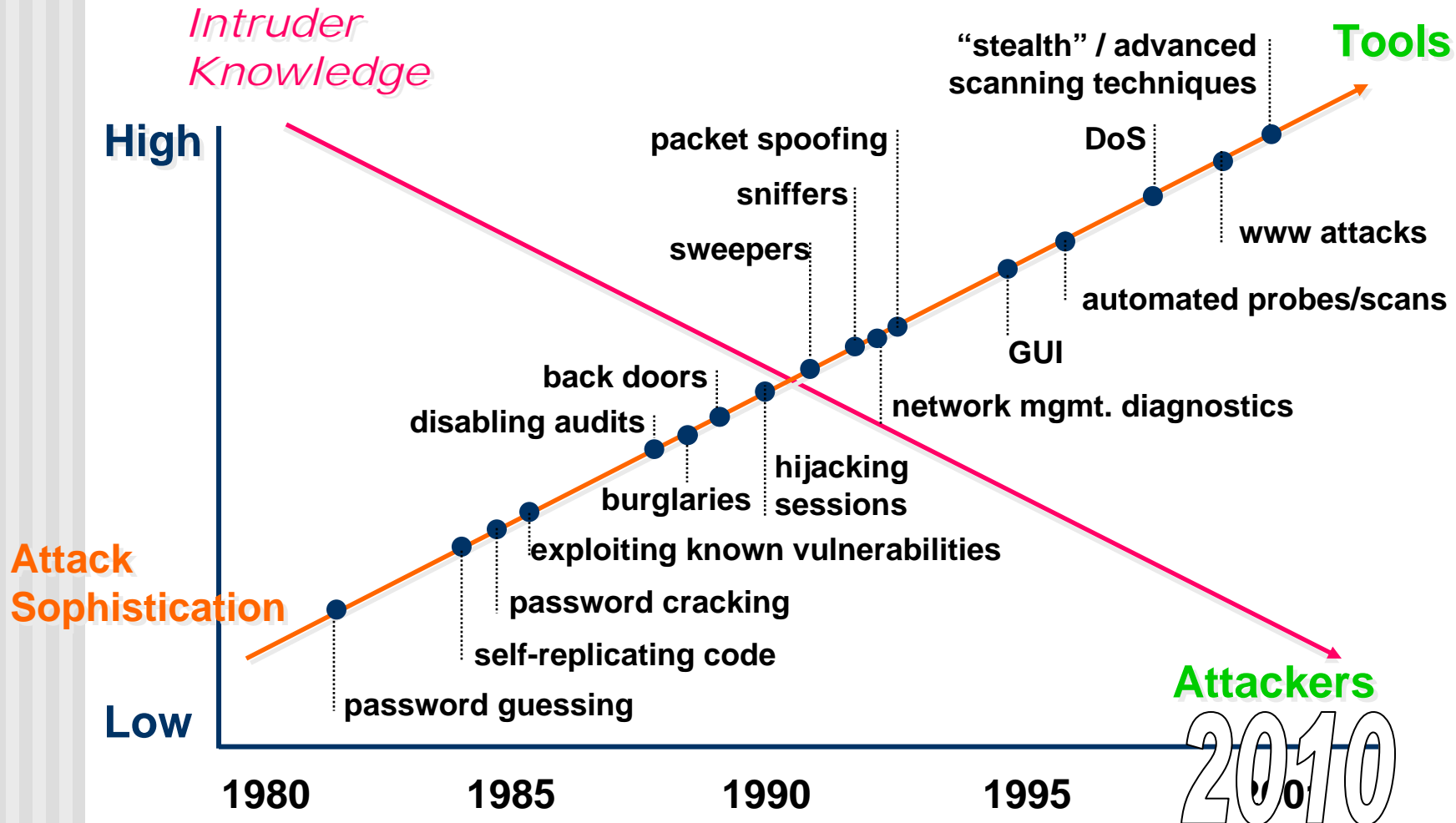
"Our country needs to go all-out to develop *high-quality internet warriors*. That should include development in exclusive universities as well as attracting private computer users to take part in *internet combat*". (*Liberation Army Daily, 2001*)



# The Landscape



# Attack Sophistication vs. Intruder Technical Knowledge



# BRINGING CIVILIZATION TO ITS KNEES...

## Goths



## Vandals



## Huns



KEVIN TIERS ©2000  
THE CHARLOTTE OBSERVER

## Geeks





To  .....

---

**Main Entry:** google

**Part of Speech:** *verb*

**Definition:** to search for information on the Internet, esp. using the Google search engine

**Example:** We googled to find the definition of the new word.

*I googled to find other websites with that same vulnerability.*

**Etymology:** trademark Google

**Usage:** googling *n*

[Source:](#) Webster's New Millennium™ Dictionary of English, Preview Edition (v 0.9.6)  
Copyright © 2003-2005 Lexico Publishing Group, LLC

# Wireless Crime

---

- Hacking
- Identity Theft
- Bandwidth Theft
- Drive-by Spamming
- Denial of Service

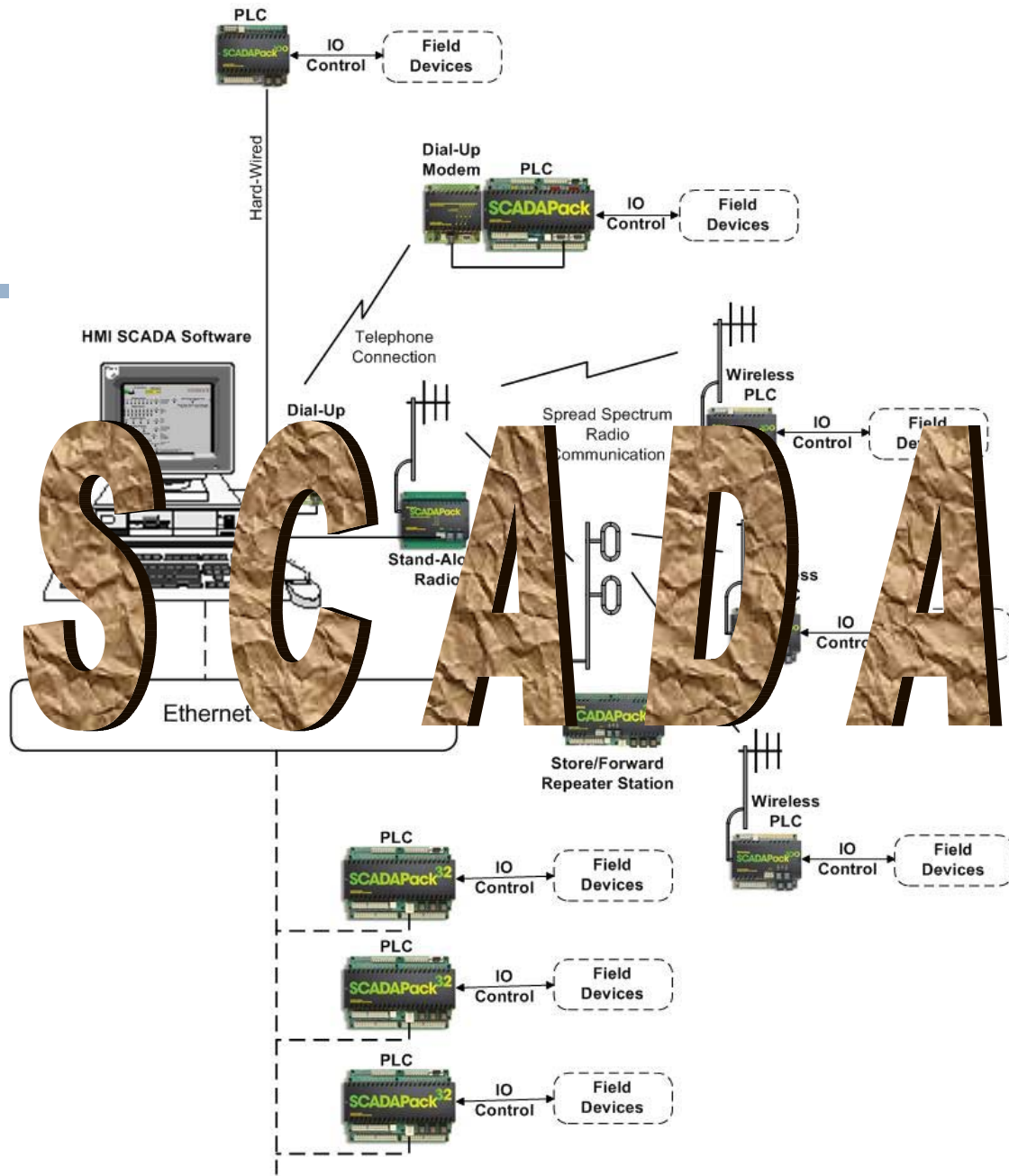




# Securing wireless

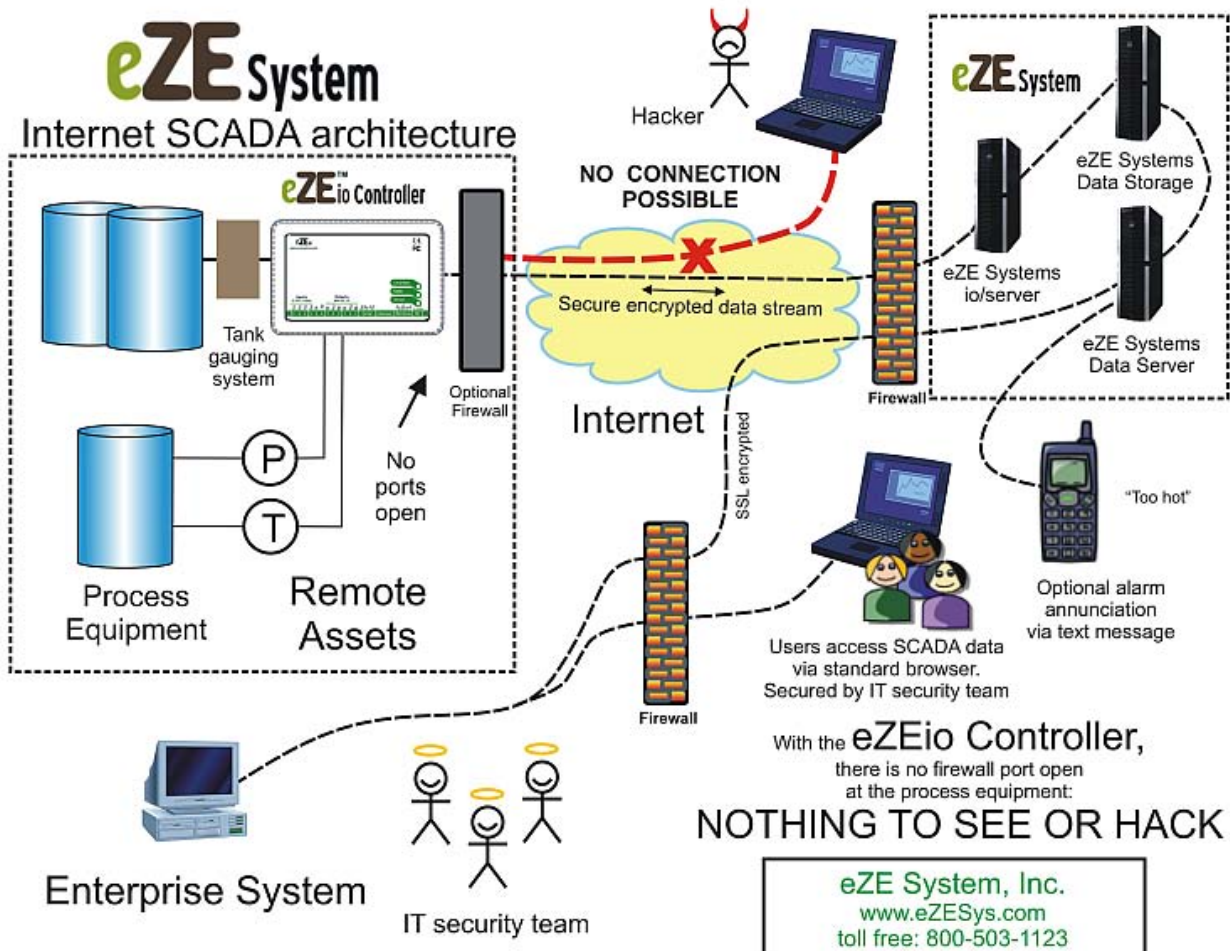
---

- Change the default password
- Change the SSID
- MAC address filtering
- DON'T increase antenna size or TX rate
- DO use encryption
  - WEP
  - WPA
- If all else fails, tin foil wallpaper will do fine



SCADA System Communication Types

# eZE System Internet SCADA architecture



With the eZEio Controller,  
there is no firewall port open  
at the process equipment:  
**NOTHING TO SEE OR HACK**

eZE System, Inc.  
www.eZESys.com  
toll free: 800-503-1123

## Taum Sauk Reservoir prior to 12/14/2005



## Taum Sauk Reservoir prior to 12/14/2005



12/14/05 – 1.3M gallons released due to dam wall breach



# In the news

The image is a screenshot of a news website, likely SFGate, featuring a prominent headline about a cyberwar emerging between Google and China. The page layout includes a top navigation bar with categories like Home, News, Sports, Business, Entertainment, Food, Living, Travel, and Columns. A search bar is visible, along with a 'Web Search by YAHOO!' option. The main article is titled 'After Google-China dust-up, cyberwar emerges as a threat' and is attributed to Jaikumar Vijayan from Computerworld, dated Wednesday, April 7, 2010. The article text discusses how a few events have crystallized U.S. fears over a cyber catastrophe, leading to calls for a strategic response. A sidebar on the left shows a '60 MINUTE' segment titled 'Popping Brain Power' and a section titled 'Where America Stands: Increasing No International Rule of Law' by Terry McCarthy. At the bottom, there are social media sharing options (PRINT, E-MAIL, SHARE, f, t) and a 'COMMENTS (0)' section. A small code snippet is visible in the bottom left corner of the page.

**SFGate**  
home of the  
**San Francisco Chronicle**  
Subscribe to the weekend Chronicle

**From \$54<sup>99</sup> Per Night**  
**Strike It Rich in Real Estate**  
Includes Breakfast, Upgrade and more!

SEARCH SFGate Web Search by YAHOO! | Advanced Search

Home News Sports Business Entertainment Food Living Travel Columns

Technology | Markets | Small Business | Chron 200 | Real Estate

## After Google-China dust-up, cyberwar emerges as a threat

Jaikumar Vijayan, Computerworld  
**COMPUTERWORLD**  
Wednesday, April 7, 2010

PRINT E-MAIL SHARE f t COMMENTS (0) FONT SIZE: [ ] [ + ]

### Cyber Attacks Jeopardize

Where America Stands: Increasing No International Rule of Law  
By Terry McCarthy

January may have compromised its recovered systems, imperiling millia

**(04-07) 06:39 PDT** -- Few events have crystallized U.S. fears over a cyber catastrophe, or brought on calls for a strategic response, more than the recent attacks against Google and more than 30 other tech firms.

The company's disclosure in January that it was attacked by China-based hackers -- and its subsequent decision to **scale back operations** there -- have stoked long-standing fears over the ability of cyber adversaries to penetrate commercial and government networks in the U.S.

```
playtrak.o  
playtrak.c  
playtrak.c.BAK  
projects/playtrak/forms:  
DESIGN DOC  
projects/playtrak/forms/DEMOS:  
demo01 demo02 demo03 demo04 demo05
```

# Cyberspace Policy Review

May 29, 2009



- Cyberspace underpins almost every facet of society
  - Leading from the top
  - Building a Capacity for a Digital Nation
  - Sharing Responsibility for Cybersecurity
  - Creating Effective Info Sharing & Incident Response
  - Encouraging Innovation

- Howard Schmidt's 2010 Cybersecurity protection predictions
  - Vulnerability of mobile devices
  - Cloud computing
  - Increased software testing required
  - 2-factor Authentication
  - Unsecured network connected devices
  - Increased Phishing/SPAM
  - Fake Anti-Virus
  - Social Networking
  - New Operating Systems

# Questions?

---

**SSA Brian Herrick**

[brian.herrick@ic.fbi.gov](mailto:brian.herrick@ic.fbi.gov)

