

000100101000100101011101010101010101000101110101000101010001001010001001

POWERTEK

CyberThreats

WE DELIVER WHAT WE PROMISE.

Science, Technology and National Security Policy
4 April 2011

9420 Key West Avenue • Suite 210 • Rockville, MD 20850
Tel: 301.795.0400 • Fax: 301.795.0430
www.PowertekCorporation.com

 **powertek**
Your success. Our mission.





Dilbert.com DilbertCartoonist@gmail.com

© 2009 Scott Adams, Inc./Dist. by UFS, Inc.



Topics

- Introduction to the class (by me)
- Introduction by the class (to me)
- Cyber – What is It?
- Cyber Shock Wave
- First Principals
- Security Thoughts

My Questions for You

- Who are you
- What have you learned thus far
- Why is national leadership in Science & Technology important
- Why has the US had a lead in Science & Technology
- What is happening to impact on the US having such a lead

Cyber – What is It?

- So “What is it?”

Cyberterrorism

- Robert Knake, Council on Foreign Relations: perhaps comparable to the impact of the 2003 Northeast blackout. Cut service to 50 million people for up to four days; \$4.5B-\$10B – out of a \$14.2T economy
- Professor Irving Lachow of the National Defense University defines cyberterrorism as “a computer-based attack or threat made for political, religious or ideological reasons, and designed to generate fear comparable to that from a physical act of terrorism.”

Cyber Shockwave

- March Madness – my anecdote
- What was it
- What were the key issues that came up

Cyber Shockwave – Issues

- Doctrinal
 - War
 - Continuous war, continuous war footing?
- Public/private interaction
 - Public authority
- Source of attack
- **Boundaries**, the lack thereof

First Principals

- Nothing from nothing leaves nothing – transactional cost economics
 - Makes it advantageous necessary to utilize external resources as much or more than internal
- Here come the clowns – management and implementation by crowd sourcing
 - The death of hierarchy
- Everybody needs somebody sometime – the Internet of Things
 - Fast sensors
- Ptolemy vs Copernicus vs Warhol, changing approaches to architecture: Earth -> Sun -> Nothing

Security Thoughts

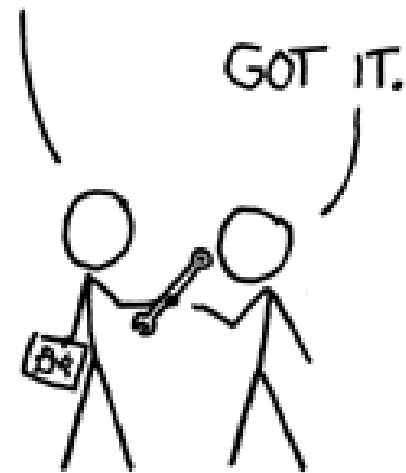
A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.



Factoids

- McAfee received > 34 million malicious code samples in 2009, will exceed that in 2010
- Operation Aurora, announced by Google, involved multiple high-tech companies probably attacked by Chinese operatives
 - Seems to have started when a Google employee clicked on a link in an instant message
- Cisco estimates that IP traffic will quintuple from 2008-2013, with 667 Exabytes of traffic in 2013
- According to Politico, by 2009, government agencies including Congress were attacked an average of 1.8 billion times/month

Homeland Security

*Since the number of targets is essentially unlimited,
since the probability that any given target will be attacked is near zero,
since the number and competence of terrorists is limited,
since target-selection is effectively a near-random process, and
since a terrorist is free to redirect attention from a protected target to an
unprotected one of more or less equal consequence,
protection seems to be sensible only in a limited number of instances.*

- Professor John Mueller, Ohio State University

SCADA Systems

- They have historically been stand-alone systems operated by the business, not IT; “air-gapped”
- Moving to common system designs and protocols as corporate IT functions
- Integrated into business systems for real-time information
- Typically distributed physically and logically; more opportunities for data interception, spoofing, and denial of service
- Stuxnet – hard coded passwords, USB device injection

© Cartoonbank.com



"Hannibal got elephants over the Alps. Bearing that in mind, somebody think of something."

Summary of Key Challenges

- Need for Public/Private cooperation
- Cloud Computing
 - Inability to quantify security status or define Service Level Agreements (SLA's)
- Social networking – especially by younger employees
 - Increasing power of commercial 'end-points'
 - Increasing interconnection to an internet of things
- False positives
- Whack-a-mole approaches to security
 - Inability to prioritize
 - Overemphasis on perimeter security, under emphasis on resiliency
- Difficulty for security professionals to understand or communicate with mission owners

Thoughts On What To Do

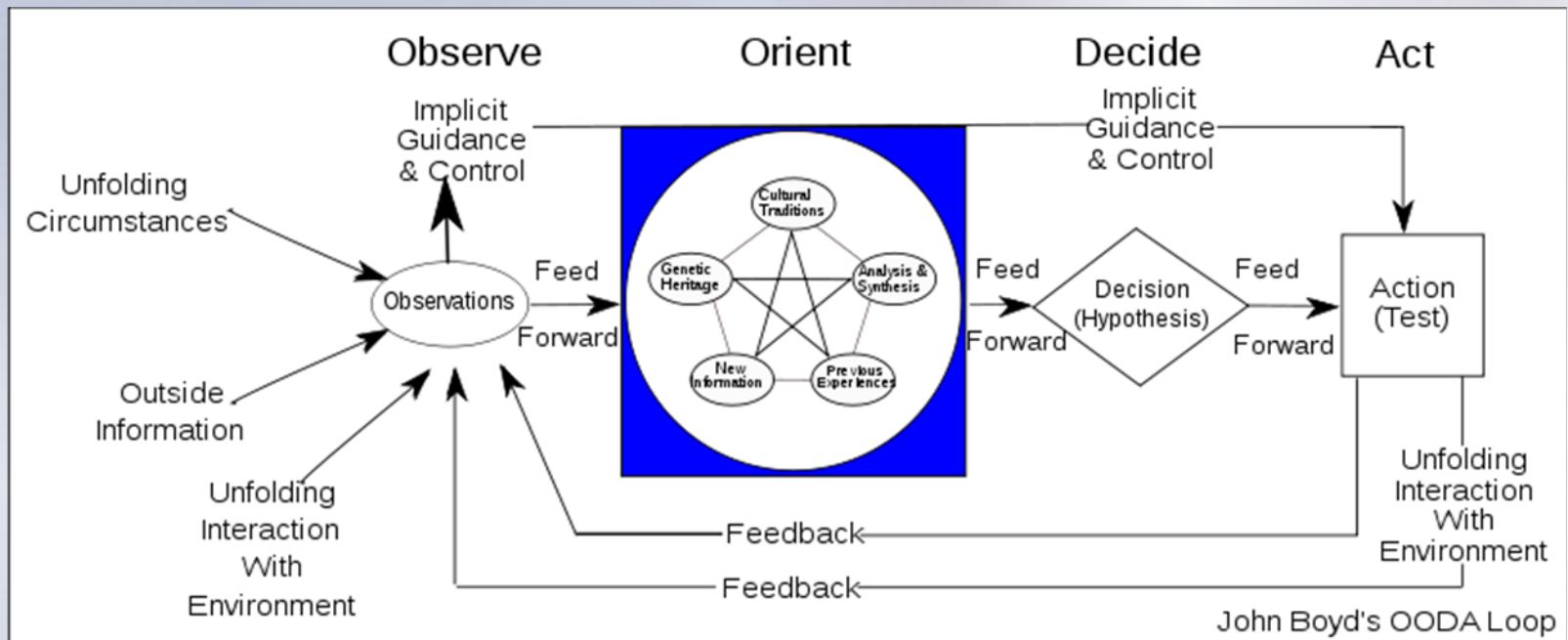
- The fundamental question is how to be secure when every component is insecure
- Security hygiene
- OODA Loop
- Biological Design

Security Hygiene

- Real-time situational awareness
- Build security into the budget process
- Transparent and relatively public status
 - Dashboards are your friend
- Be realistic

OODA Loop

- Developed by USAF Colonel John Boyd
 - “In order to win, we should operate at a faster tempo or rhythm than our adversaries”



Biological Design*

- Stigmergic systems: a mechanism of indirect coordination between agents or actions
- Characteristics
 - Multi-agent
 - Loosely coupled
 - Self-organizing
 - Systems-of-systems
- Behavior
 - Swarm intelligence
 - Tight learning loops
 - Fast evolution
 - Dedicated intent

* From INCOSE, International Council on Systems Engineering

Biological Design – 2*

- Self-organizing
- Adapting to unpredictable situations
- Reactively resilient
- Evolving in concert with a changing environment
- Proactively innovative
- Harmonious with system purpose

* From INCOSE, International Council on Systems Engineering

Powertek Corporation
9420 Key West Avenue, Suite 210
Rockville, MD 20850

www.powertekcorporation.com

Daniel Mintz, Chief Operating Officer

301-795-0418/o

301-332-0717/c

DMintz@PowertekCorporation.com

Twitter: www.twitter.com/technogeezer

Facebook: www.facebook.com/technogeezer