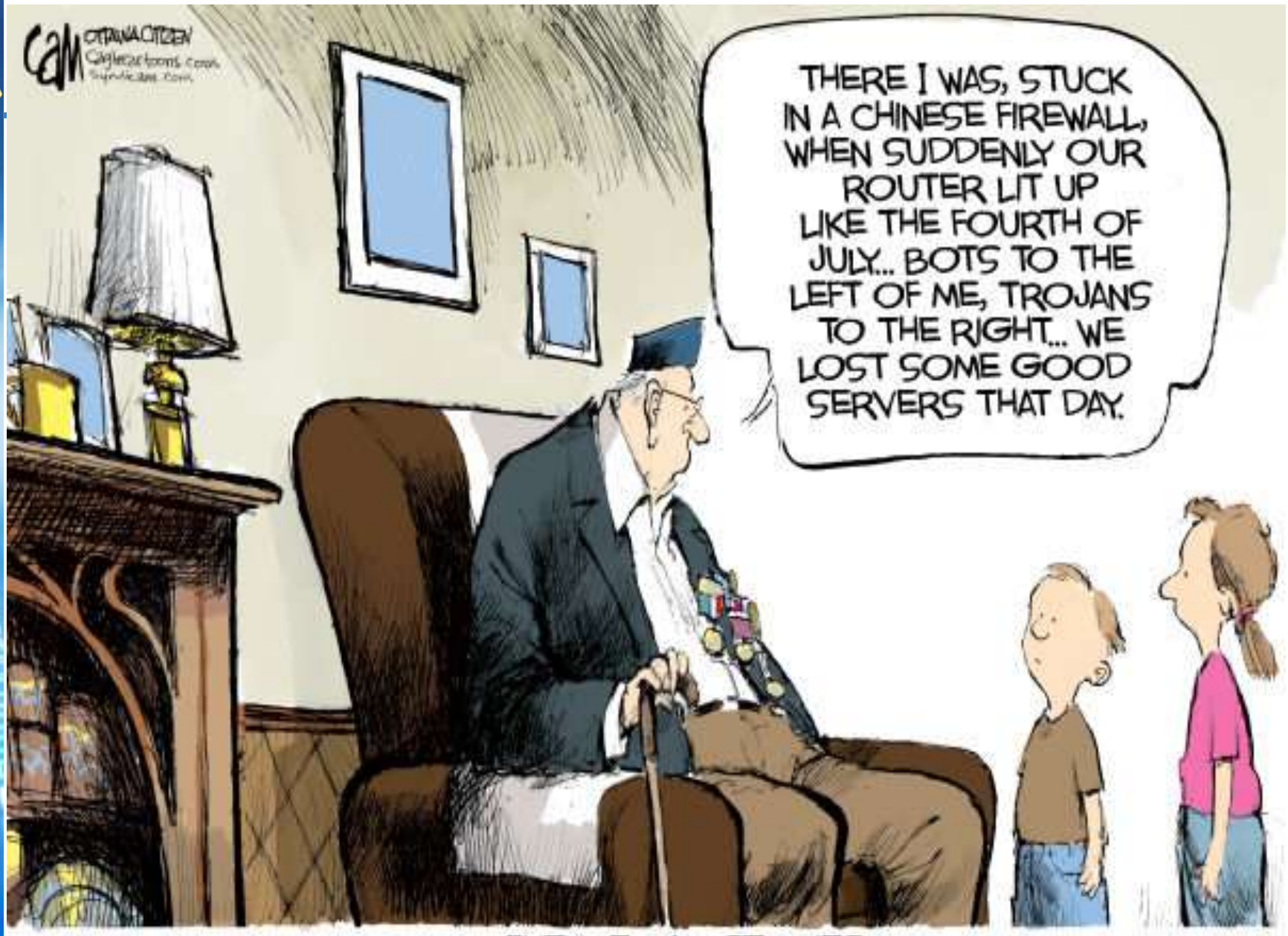
24 AF Welcomes Industry Leaders

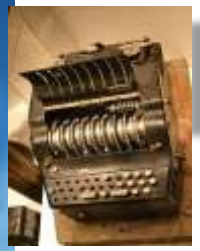
Overall Classification

UNCLASSIFIED

Maj Gen Suzanne Vautrinot
24 AF/CC


CAM OTTAWA CITIZEN
THERE I WAS, STUCK IN A CHINESE FIREWALL, WHEN SUDDENLY OUR ROUTER LIT UP LIKE THE FOURTH OF JULY... BOTS TO THE LEFT OF ME, TROJANS TO THE RIGHT... WE LOST SOME GOOD SERVERS THAT DAY.
FUTURE WAR STORIES

Where We Came From


Enigma


IBM Selectric


Mainframe


Zenith Z100

World Wide Web

Web Defacement

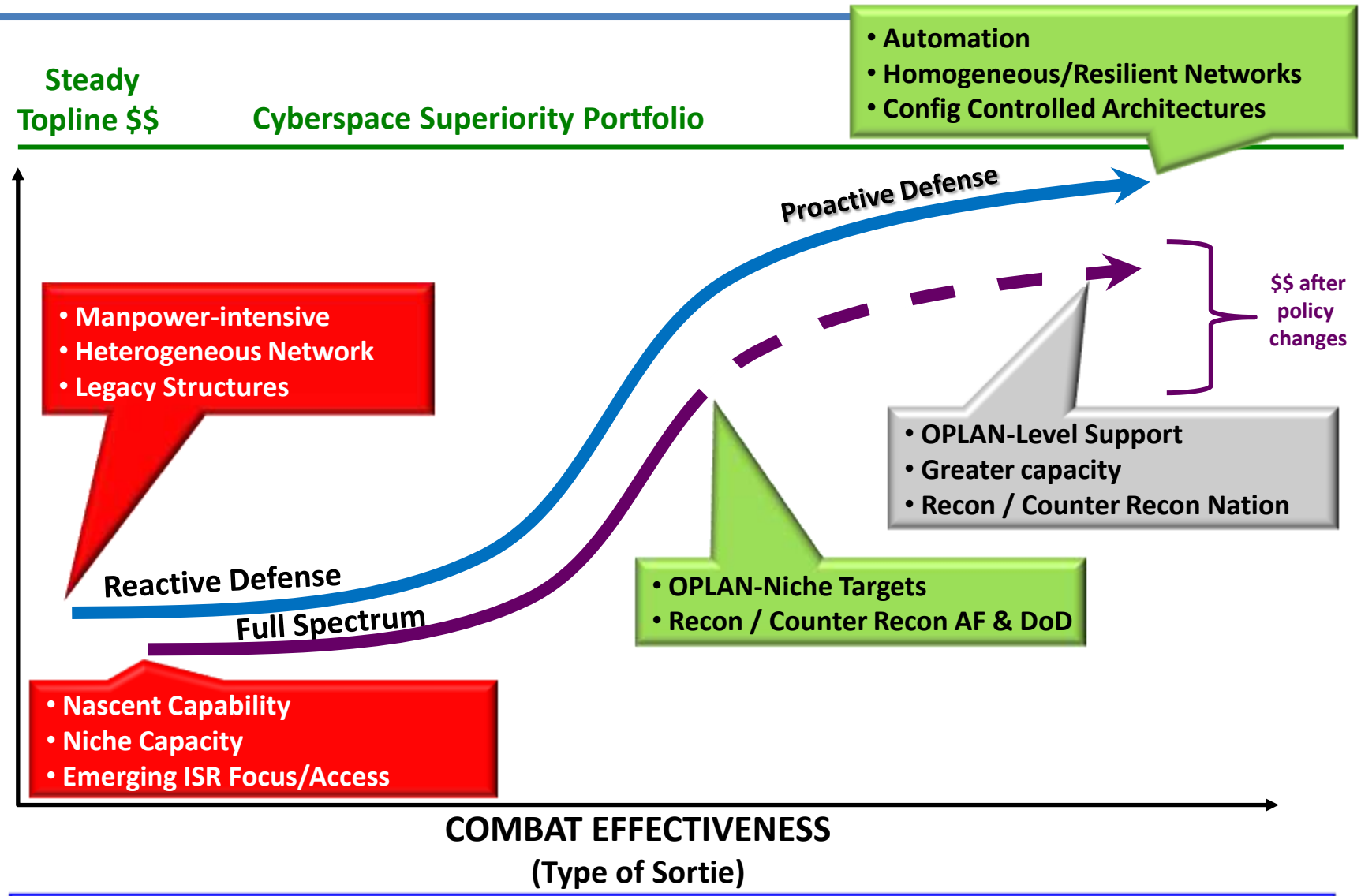

Stuxnet – Nuclear Centrifuge

We don't have 100 years… the future is here now.

Where We Are

- **AFCYBER**
  - **Defense**
  - **Offense**
  - **Exploitation**
- **24 AF**
  - **Advanced Cyber Training**
  - **Engineering & Installation**
  - **Rapid Tool Development**
  - **Network Extension/Tactical Comm**
- **AFNetOps**
  - **Forensics**
  - **Boundary & Gateway Monitoring**
  - **Metrics**
  - **Blue/Red Team Assessments**

Where We're Going…The Challenge



Maximizing Return on Investment

Where We're Going…The Intent

Mission Statement

Extend, operate and defend the Air Force portion of the DoD network and provide full spectrum capabilities for the Joint warfighter in through and from cyberspace

AFSPC Priorities

- Supporting the current fight
- Getting control of the cost of space programs
- Normalizing and operationalizing cyberspace

24 AF Priorities

- Normalize mission operations & staff responsibilities/processes
- Improving the Big C's: Capacity, Capability, Collaboration
- Stabilize and baseline 24 AF and cyber units/resources/structure

Support the Joint Fight

Moving Up the Curve

Assuring Mission via:

- Network Architectures
  - "Build to Baseline"
- Network Awareness
- Pro-Active Defense
- Recon
- Counter-Recon

Internal

Expanding Mission via:

- Exploiting Adversary Network
- Leveraging Planning

External

Defining a Paradigm Shift In Defense

Expanding Mission: Exploiting Adversary Networks


THE WALL STREET JOURNAL. TECHNOLOGY

Computer Spies Breach Fighter-Jet Project

By SIOBHAN GORMAN, AUGUST COLE and YOCHI DREAZEN

WASHINGTON -- Computer spies have broken into the Pentagon's $300 billion Joint Strike Fighter project -- the Defense Department's costliest weapons program ever -- according to current and former government officials familiar with the attacks.

Similar incidents have also breached the Air Force's air-traffic-control system in recent months, these people say. In the case of the fighter-jet program, the intruders were able to copy and siphon off several terabytes of data relating to the design of the plane's electronic systems, officials say, potentially making it easier to develop ways to defeat the aircraft.

The latest intrusions provide new evidence that a battle is raging between U.S. defense officials and potential adversaries over the data networks that connect military computers. The revelations follow a recent Wall Street Journal report that Chinese hackers have penetrated the U.S. electrical-distribution system, as well as other infrastructure networks, and have infiltrated by spies abroad.

HACKING VICTIM: Spies are said to have stolen data on the F-35 Lightning II fighter. Here, the plane undergoes flight testing over Texas.

Attacks ... them ... past six ... briefed ... been an... adding ... agencies ... are affe... this cou...

Many de... including ... attacker...

to the U.S. defense program, either in financial or secu...


FAST COMPANY

Pentagon Says F-35 Classified Designs Have Not Been Stolen

Defense Department spokesman Bryan Whitman said: "I'm not aware of any specific concerns." That's a key phrase. Lockheed Martin--the F-35 supersit's primary contractor--also commented: "We actually believe The Wall Street Journal was incorrect in its representation of successful

- Pro-active defense informs the offense
- Turn defensive gaps against adversary
- Find what the adversary is working on

… then build protection from it

"Don't wait for the Zero-day to hit…
I want to know about it
while it's being developed"

Expanding Mission: Leveraging Planning

- Oil/Gas Refineries


- Electric Power Plants


- Rail Yards


Vulnerability Assessments Advise…
At Home, With Friends, Against Adversaries

Collaboration is Key

- Why you are so important
  - DoD will never have capacity to keep up with threat
  - Technology in this domain is consumer driven – demands of the market
    - Near-term: automation, cloud computing, supply chain purity
    - Long-term: quantum computing/communications, multi-function devices (next-gen firewalls, deep packet interiors, etc.)
- Rethinking our approach
  - Technology push vs requirements pull
  - Sustainment – let's date, not marry
- Leveraging partnerships with industry to dominate strategic/global opportunities!

Cyber Dominance = Combat Power

Global Reach, Power, Presence

Questions?

Moving Up the Curve

FROM:

- Tracking network outages (uptime)
- "Firewall" defense
- Base level equipment maintenance
- Clean up response (wipe & reload)

We still think in these terms…

- Reporting still geared towards outages
- Questions are administrative… not mission focused
- Need to grow "operators" vs "administrators"

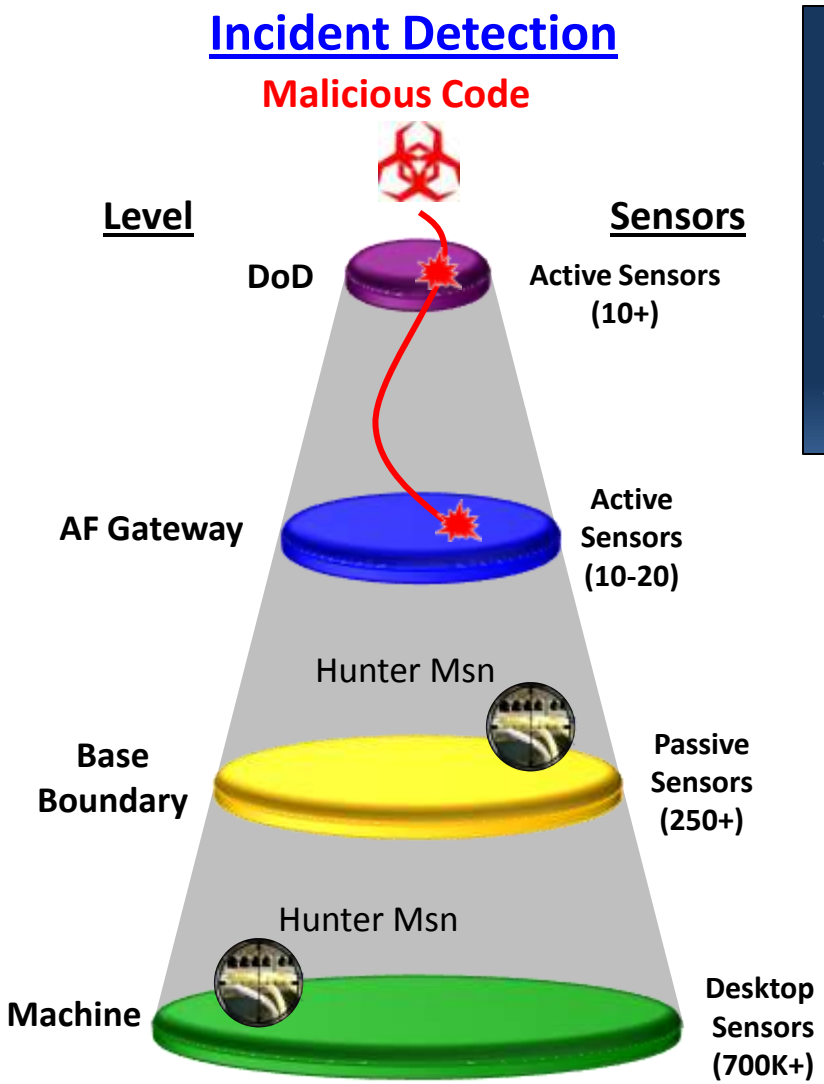
Defining a Paradigm Shift In Defense

Assuring Mission: Network Architectures

- Securing data vs. Securing systems
- Encryption, Sensoring, Analytics, Refresh, Configuration Control, Standards
- Defensible weapons system vs. comm system
- AFNET + Functional systems (PMO, medical, finance, etc)

Mission Assurance vs Network Assurance

Pro-Active Defense
Layered "Defense in Depth"



GOALS

- Prevent known bad from getting into network ✓
- Indications and Warnings ✓
- Remote forensic analysis ✓
- Preserve bandwidth & 'cleaning time' ✓
- Reduce threat response time **In Progress**

Forensics

↓

Signatures

↓

Heuristics

Recon (Hunter) Operations: Point Defense "Dominance"

Not your Father's 'Blue Team'

- Find the threat and neutralize it… "blocking"
- Persistent/active engagement in AF networks with broad authority to act
- Focus operations where threat is highest
- Map the network, prioritize "defended asset list"

Partnerships: -TRANSCOM / TACC

-PACAF / AOC

"In trying to defend everything, he defended nothing."
- Frederick the Great, King of Prussia, 1740-1786

Assuring Mission: Counter Recon

Responding to malicious events… “tackling”

- Civilian sector is already doing this
  - Microsoft took down three botnets in 2010 w/court order
  - FBI & Justice Dept got restraining order to shut down the Coreflood botnet in April 2011
  - Justice shut down Megaupload filesharing domain for copyright violations in Jan 2012
- Military constraints, working SROE
- Collaboration ongoing across Government