

# **Cybersecurity – Just Another ‘Y2K’?**

Association of Old Crows –  
The Chesapeake Roost

21 October 2010

J.O. McFalls

President, National Security Division


# Introduction

POINT ONE

- Purpose: To Gain a Sense of Urgency Regarding Cybersecurity for the Nation
- Presenter
  - J.O. McFalls, Senior-level Consultant
  - Former USAF Fighter Pilot
  - Private and Public Sector Experience
- Caveats for this Presentation
  - No Restricted Information
  - Personal Opinions
  - Open Source References

# December 31, 1999 – Headlines, Quotes, and Media Hype

POINT ONE

- 
- “The Y2K problem is the electronic equivalent of the El Niño and there will be nasty surprises around the globe.”
  - “There will be a 30-40% decrease in travel starting in December with people cancelling plans to travel over the holidays and rollover.”
  - “Stores report shortages (out of stock on items); attributed to Y2K stocking.”
  - **Outcome...**
    - No significant failures occurred in New Zealand and Australia. After Japan and China reported in with no infrastructure problems, by noon the North American TV networks reported that the Y2K computer crisis is over. A TV reporter in Hawaii says: “***It was over before it began.***”

# Cybersecurity

POINT ONE




Is This Year 2000,...  
All Over Again?

You Tell Me, After We Consider...

# Cyberspace – What is It?

POINT ONE

- 
- Three Key Attributes
    - Convergence
    - Large Amounts of Data
    - High Rate of Change of Technology
  - So What?
    - Touches Virtually Every Aspect of Modern Life
    - Threats to IT Infrastructure Endanger...
      - National Security
      - Economic Security
      - Our Citizens' Privacy
  - The Ubiquity of Cyberspace, combined with the design, manufacture, and service of IT moving more overseas – Our vulnerabilities continue to grow

# Cybersecurity: Potential Adversaries

POINT ONE



- Non-Ally Nation States
- Traditional Foreign Intelligence Services (and Surrogates)
- Developing Nations
- Terrorists
- Individual Hackers
- Criminal Elements (Organized Crime)
- Insiders

# Cybersecurity: Who are the Players?

POINT ONE



## Homeland Security Sectors

- IT Sector
- Telecommunications Sector
- Banking and Finance Sector
- Defense Industrial Base Sector
- Critical Infrastructure Sector(s)

## International

- All Levels

## Law Enforcement

- Federal
- State, Local, Tribal

John Q. Public

# Cybersecurity: Who Else?

POINT ONE

## Federal Government

- |   |  |
|---|--|
| <ul style="list-style-type: none"><li>• DHS</li><li>• DoD and Military Services</li><li>• Intelligence Community<ul style="list-style-type: none"><li>• DNI + Agencies</li></ul></li><li>• Commerce</li><li>• Treasury</li><li>• Justice</li><li>• State</li><li>• Energy</li></ul> | <ul style="list-style-type: none"><li>• U.S. Courts (FISA)</li><li>• U.S. Congress</li><li>• White House<br/>[ICI-IPC]</li></ul> |
|---|--|

# U.S. Intelligence Community (IC)

POINT ONE




## Office of the Director of National Intelligence (ODNI)

1. Central Intelligence Agency
2. National Security Agency
3. Defense Intelligence Agency
4. National Geospatial-Intelligence Agency
5. National Reconnaissance Office
6. U.S. Air Force
7. U.S. Army
8. U.S. Navy
9. Department of Homeland Security
10. Federal Bureau of Investigation
11. Department of Treasury
12. Department of State
13. Drug Enforcement Administration
14. Department of Energy
15. U.S. Marine Corps
16. U.S. Coast Guard



# Cybersecurity – What is Happening?

POINT ONE

- 
- National Strategy - CNCI
    - 12 Initiatives
    - 6 Enablers
  - Dept of Defense Strategy
    - National Military Strategy for Cyberspace Operations
    - Quadrennial Defense Review – Cyber ‘Tiger’ Team
    - U.S. Cyber Command
  - Enduring Security Framework
    - Public-Private Partnership at the Executive Level

# Cybersecurity – Use of Scenarios

POINT ONE

## An Emerging Trend - Scenarios Utilized at All Levels

- NMS-CO was First
- White House – Cybersecurity Policy Review
- DoD and DHS “Tabletop” Exercises
- QDR
- Financial Sector
- “CYBERSHOCK” CNN Special
- JCS, Combatant Commands, and Military Services
  - Terminal Fury
  - Schriever Wargame
- Enduring Security Framework


# Cybersecurity – Sample Scenarios

POINT ONE

- 
- Intellectual Property Loss
    - Recycled Laptop
  - Loss of Military Capability
    - Foreign Software Implants into US Transportation Command networks
  - Supply Chain Risk
    - Sensitive Proprietary Industrial Information ‘Exfiltrated’ Overseas
  - “Cyber Katrina”
    - Breach of North American Power Grids and Their Control Systems

# Cybersecurity – Ongoing Issues

POINT ONE

- 
- Lack a Standard Lexicon (terminology)
  - How Can You Have Certainty of Attribution?
  - What Constitutes a Hostile Act in Cyberspace?
  - What is Adversary Cyberspace?
  - Is Cyberspace Sovereign Territory, a ‘Global Commons,’ or Both?
  - What is Deterrence in Cyberspace?
  - U.S. Code (Title 10 vs. Title 50 vs. Title 18 vs. Title 32)
  - Civil Liberties and Privacy vs. National Interest
  - Etc.


# Cyberspace and Cybersecurity

POINT ONE

- Is This Year 2000, All Over Again?
- Yes,....but it's **Y2K<sup>100</sup> !!**

# How Can You Help? – Homework

POINT ONE

- 
- Read Three Unclassified Documents
    1. Securing Cyberspace for the 44<sup>th</sup> Presidency, CSIS Commission, December 2008
    2. White House Cyberspace Policy Review, “Assuring a Trusted and Resilient Information and Communications Infrastructure,” May 2009
    3. The Comprehensive National Cybersecurity Initiative, declassified March 2010  
[\[http://www.whitehouse.gov/cybersecurity\]](http://www.whitehouse.gov/cybersecurity)
  - Participate in Subject Matter Expert Groups such as NIST\*, NSTAC\*, PSTAC\*, etc. (Start with a Standard Lexicon, and a best case Industrial Model)
  - Design and Use Your Own, Tailored Cyber Scenarios

# Questions and Comments?

**J.O. McFalls**

**703-414-5440**

**[jomcfalls@pointoneinc.com](mailto:jomcfalls@pointoneinc.com)**

# Back-Up


**J.O. McFalls**

**703-414-5440**

**[jomcfalls@pointoneinc.com](mailto:jomcfalls@pointoneinc.com)**


# CNCI - Major Goals and Initiatives

POINT ONE

- 
- Establish a Front Line of Defense
    - Initiative 1: Trusted Internet Connections
    - Initiative 2: Passive Sensors
    - Initiative 3: Automated Defense
    - Initiative 5: Connectivity
    - Initiative 12: Engage Private Sector
  - Defend Against the Full Spectrum
    - Initiative 6: Cyber Counter-Intelligence
    - Initiative 7: Classified Network Security
    - Initiative 11: Supply Chain Management

# CNCI - Major Goals and Initiatives (2)

POINT ONE

- 
- Shape the Future Environment
    - Initiative 4: Research and Development
    - Initiative 9: Leap Ahead Technology
    - Initiative 8: Education
    - Initiative 10: Deterrence
  - CNCI Enablers
    - All-Source Analysis
    - Sensors and Backbones
    - Cryptanalysis
    - Human Intelligence
    - Law Enforcement
    - Monitor/Coordinate