

# Technologies And Gaps In The Context of the Cyber Initiative

Technology Contributions in Formulating A  
Common Response

Bob Gourley

<http://ctovision.com>

[bob@bobgourley.com](mailto:bob@bobgourley.com)

10 Dec 2008

# Some Technological Context

- So much activity is underway we should consider progress and re-examine remaining gaps.
- Can discuss context in terms of:
  - Types of technologies government using to defend
  - Shortfalls in current tech approaches
  - R&D addressing the gaps
  - Remaining gaps not addressed
  - Thoughts on advanced public-private partnerships

# Types of technologies government using to defend

Three choices: 1) hardware, 2) software, 3) integrations of both

**1) Hardware:** Enhancing tamper resistance and physical security. Enhanced devices for DPI & Websec (Cloudshield, Cisco Ironport, Narus to name a few). Hardware VPN.

**2) Software:** Agent based configuration and remediation (Triumphant good example). Software encryption built into OS (Vista bitlocker good example). Of course software firewalls, IDS, antivirus, antispam and other standard stuff. Enterprise management tools (HP OV, BMC, IBM Tivoli etc), some behavior detection. Some info correlation and discovery tools. Some DRM. Some collaboration.

**3) Integrations:** Identity management, authorization, advanced visualization, collaborative tools, information discovery, DVTC, VOIP, thin client architectures, Cloud Computing approaches.

# Shortfalls in current tech approaches

- Legacy components and legacy data must be protected
- Insider threat modeling and analysis
- Standards don't keep up
- End-to-End IT management thought of as impossible?
- Who's Who and What's What?
- Visualizations of the federal space
- Visualizations of the commercial space
- Wireless security and Wireless availability
- DRM for federal data
- Ability to collaborate and coordinate response virtually
- And, perhaps the hardest challenge of the last decade:  
Ability to use technology to determine attribution of attack,  
with precision required for either legal or military action

# R&D addressing the gaps

Tremendous amount of work in the federal R&D space, including:

- HSARPA (see [www.dhs.gov](http://www.dhs.gov) for list. It includes work in visual analytics, privacy, forensics, standards, DNSSEC, IdM)
- DARPA (Cyber Trust)
- NSF (Trustworthy Computing, Cylab)
- NCSC: Steering visualization and collaboration work
- IARPA: One of three key areas is safe and secure ops
- NSA IAD, NIST, Others: Standards, IA related research

Tremendous amount of work in academia. Centers of note:

- Carnegie Mellon SEI
- Purdue University CERIAS
- MIT CSAIL

# Remaining gaps not addressed

- Insider threat modeling and analysis is producing some results, but my sense is huge gaps remain before results can be comprehensively integrated into the federal enterprise
- How can we, in one swift action, replace all legacy with modern IT?
- How can we determine the status of the entire federal enterprise and visualize that in a way that can support decision-makers?
- How can we use threat modeling and analysis as a component of attribution?
- How can we cut through the pain and cost of face to face collaboration and meetings and travel? Telepresence? (Need this across every federal domain and across the fabric of the civilized world).

# Thoughts on advanced public-private partnerships

- AFCEA plays a wonderful role here.
- But how much of industry is really reached by events like this?
- Isn't it primarily the parts of industry that really want to do business with the federal government?
- Are the thought leaders of American R&D here with us today?
- How do we go to them? How do we establish trust-based relationships when our FAR bounds every discussion?
- Can we free up every government employee to blog? If the answer is no, why not? Don't we trust them?
- How can we bring all the good guys into our nets and never allow a bad guy in?

# A Concluding Challenge

- A metaphor from Sci-Fi:
  - The Kobayashi Maru
- Humans create technology. We conceive, design, produce, field and configure it.
- Now it is time to do it all better.
- The goal: through standards, regulations, training and R&D, increase both the security and functionality of enterprise IT by two orders of magnitude in the next 24 months
- An assumption and a question: If the things called for in this briefing are done it will make both attribution and privacy better. Right?

# About This Briefing

- This presentation was created online in a secure cloud.
- Your thoughts/guidance/suggestions are very much appreciated. Send me a note and I'll grant you online access to my grid. I'm at [bob@bobgourley.com](mailto:bob@bobgourley.com)
- For related thoughts see my blog at <http://ctovision.com>
- And for a stream of cool stuff subscribe to my Twitter feed at <http://www.twitter.com/bobgourley>