



Protecting our digital shores
Dec 7, 2011

Cyber gaps / needs

Mike Davis, ISSA / TSN

Bruce Roberts, Cubic Consultant, TSN



B.L.U.F.

(Bottom Line Up Front)

Key issues....

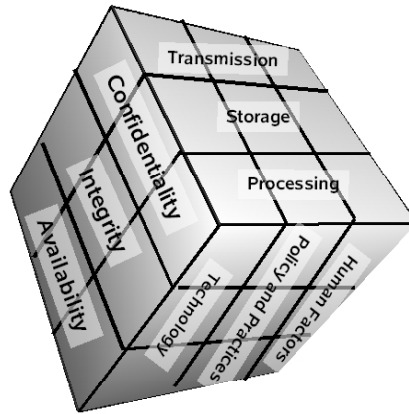
- Threats are illusive – so also plan around *consequences* (fault tree)
- *KISS, as complexity is our enemy – do the basics well (hygiene, anonymity, etc)*
- In a connected world, it's the *shared vulnerabilities* that will get you / us
- “They” have an *asymmetrical advantage*, so plan on it, leverage that
- *We must have a homogenous security protection in a heterogeneous world*

Key gaps / needs...

- Follow the OSD / NSA R&D / S&T perspectives, they're solid (we'll cover those)
- Apply trade-offs / assessments from a common end-state (open world / ubiquity)
- Using an enterprise risk management schema, develop YOUR cyber action plan
- If you can't integrate “it” into your IT/network environment, “it” is useless
- Most of the gaps and needs are “SoS” and “I&I” elements (the “glue”), not “stuff”

**If you don't know where you're headed, any path will do
Where the bad actors continue to count on us not being in sync**

Notional Representation of IA Vulnerabilities and Architectural Approach to Layered Defense in a NetCentric World



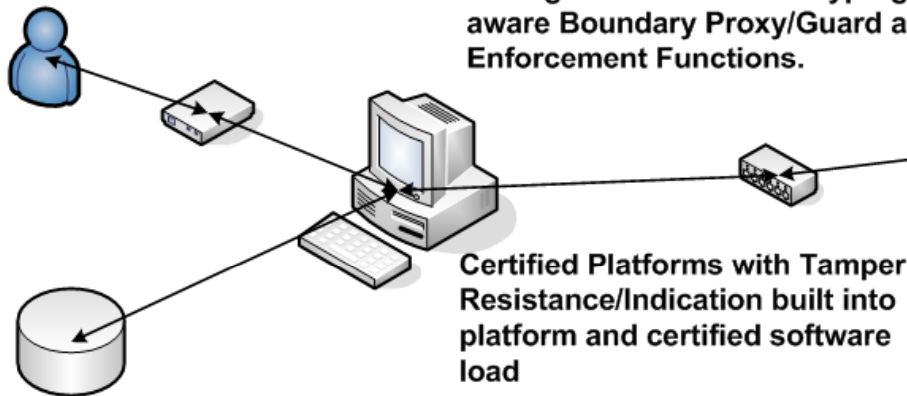
SO, What's a "simple" IA/Cyber vision / end-state look like?

Identity, access control and authorization are critical in this environment, significant work on distributed access control systems needs to be completed for High Assurance Solution for ID certification using distributed solutions

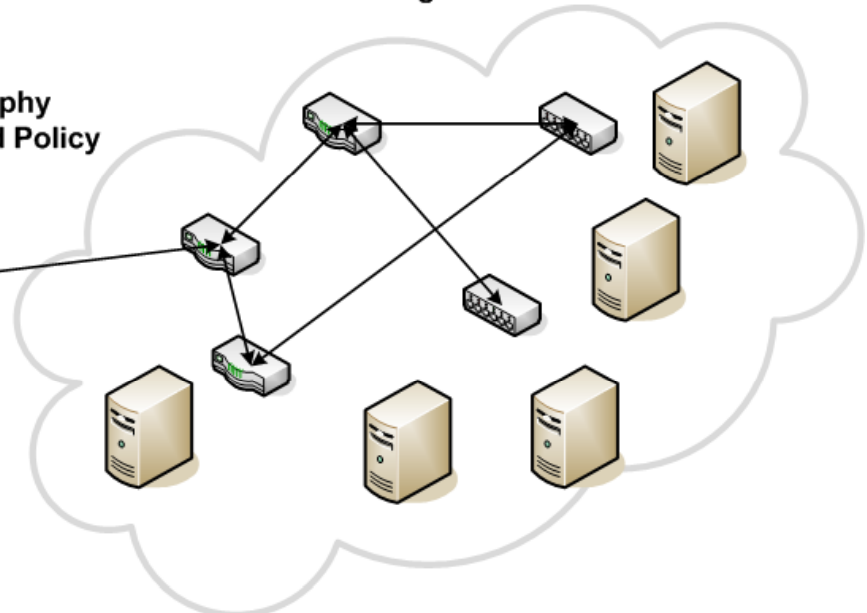
AND what are the "requirements"?

Protected Infrastructure, QOS, COS and Routing Grid

Intelligent Content and Cryptography aware Boundary Proxy/Guard and Policy Enforcement Functions.



Certified Platforms with Tamper Resistance/Indication built into platform and certified software load



In the Net Centric world data in motion and data at rest become indistinguishable there is a need to protect storage, queues, and memory locations across the grid from information exfiltration.

Common Services from Geo Targeting to DNS must be protected at the level required by the highest risk applications using them you cannot consume anything that you do not trust if affects your decision cycle in a way you cannot adapt to. Aggregate risk compounds the protection level required for the components and is seldom accounted for properly.

A cyber end-state stresses encapsulation through a secure virtualized fabric

What Threats?

Depends on your perspective... yet, *which should we all “really” worry about?*
And who says so?

- **Summary of the top threats**

- Malicious Code – viruses, botnets, etc
- Stolen/Lost Laptop or Mobile Device
- Spear Phishing – targeted SPAM
- Unsecured Wireless Internet Networks
- Insider/Disgruntled Employee

Where's your data?

- **Key Business Security problems** - Computer Security Institute Survey (2008)

- 42% reported **laptop theft**; 44% reported **insider abuse**; 50% detected **computer viruses**; 21% reported denial of service attacks; 20% reported systems being made bots

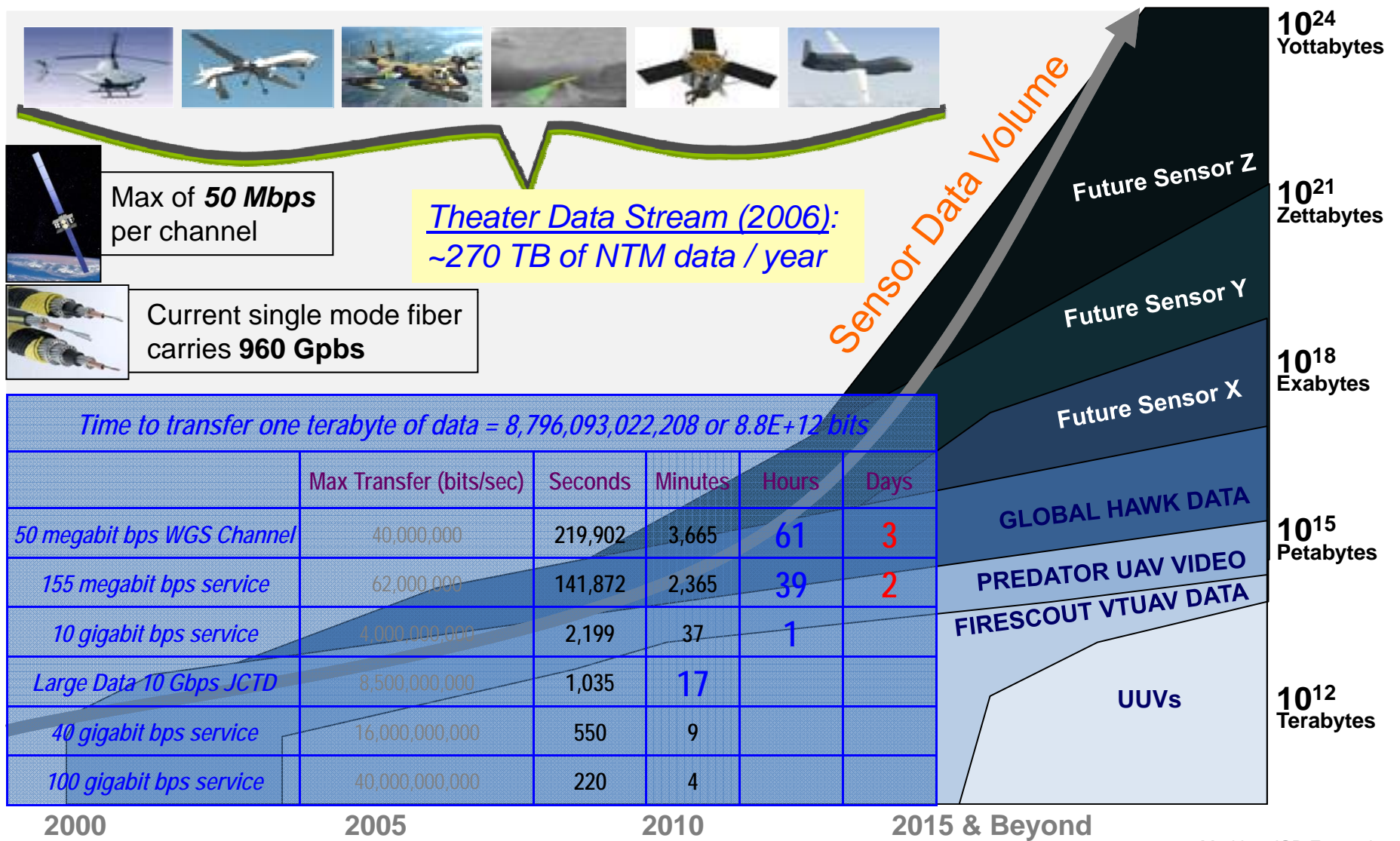
- **Survey of 10,413 information security professionals top threat concerns**

- **application vulnerabilities** (cited by 73%),
- **mobile devices** (66%) **viruses and worms** (65%) **internal employees** (63%)
- hackers (55%) and contractors (45%) Other concerns include cyber terrorism (44%),
- cloud-based services (43%), and organized crime (38%).

***Basically Everything... So follow the consequences
by practicing defense in depth – affordably....***

WHAT DATA to protect, when and how?

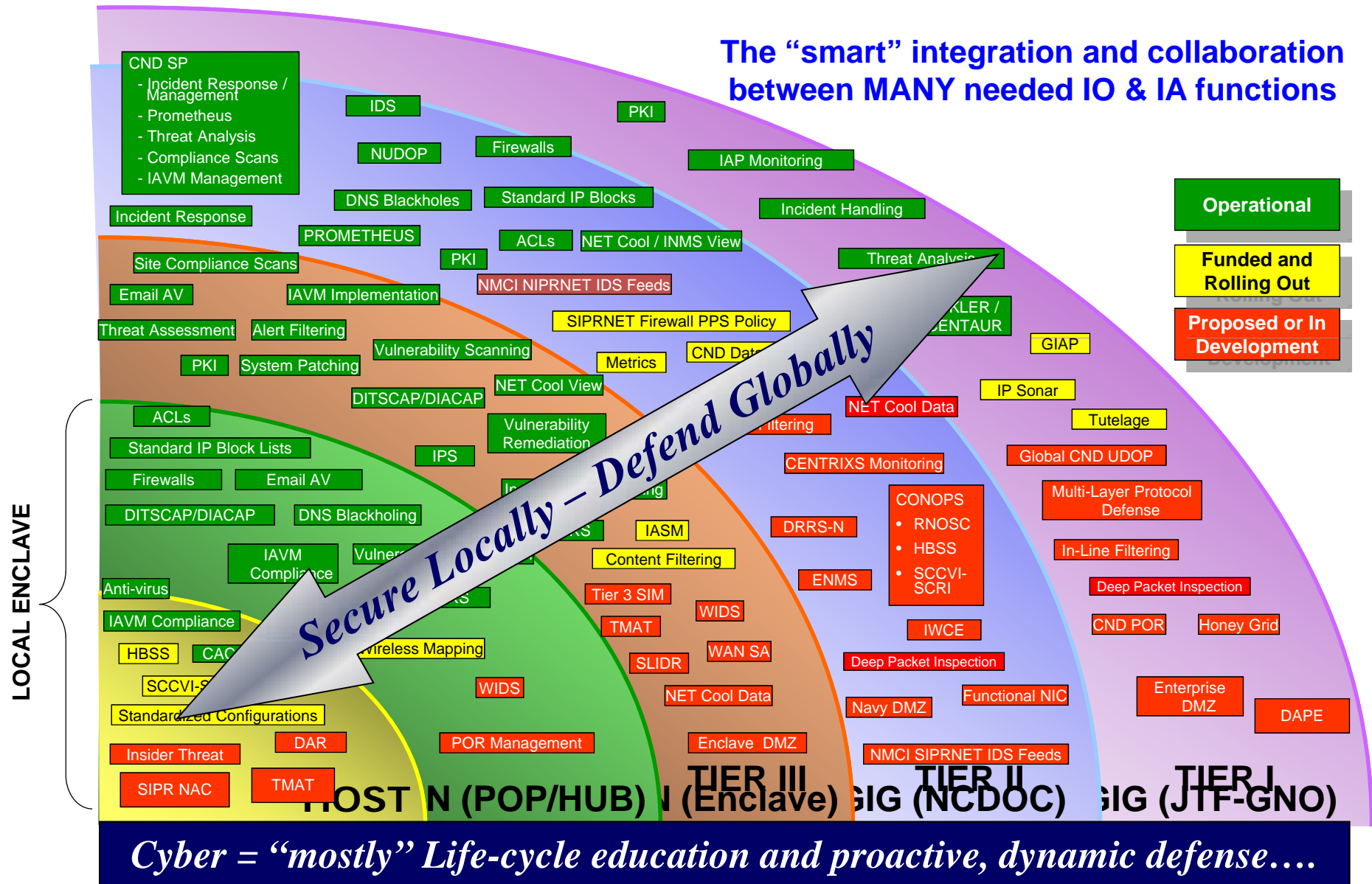
Exponential Data Growth & Security - Enabler & Challenge!



IF your DATA is everything, are you treating it so???

DoD CND (and “Cyber”) Defense in Depth

The “smart” integration and collaboration between MANY needed IO & IA functions



(From NCDOC briefs)

Future Threat Predictions

(top ten cyber security areas to be aware of *and* accomodate)

- **Nation-sponsored hacking: When APT meets industrialization**
 - More targeted custom malware (Stuxnet is but one example)
- **The insider threat is much more than you had imagined**
 - Coming from employees, partners, clients and compromised services and computing devices of all kinds. With Improved social engineering attack, social media exploitation & malware
- **Web security vulnerabilities will proliferate**
 - Browsers remain a major threat vector (and bypasses IA suite)
- **Misanthropes and anti-socials**
 - Privacy vs. security (and trust) in social networks. Radical group's DDOS attack can be effective on small businesses!
- **File / data security takes center stage....**
 - Data security goes to the cloud - the long IPv6 transition will provide threat opportunities... Data loss Prevention key...

SO... How can WE ALL realistically address ALL these challenges? ₇

Future Threat Predictions (Cont.)

- **Mobile devices compromise data security...**
 - Wireless security issues expand (besides 802.11 & WiMAX, to Zigbee, WirelessHART, Z-Wave, etc.) ARM hacking increases
- **Hackers feeling the heat...** (the easy vulnerabilities are diminishing)
 - they need to invest in better attack techniques and detection evasion, means bigger organizations are better
- **Cyber security becomes a business process...**
 - focused on data security, no longer a niche Industry
- **Convergence of data security and privacy regulation worldwide..**
 - compliance will be even more so (PCI DSS, HIPAA/HITECH, etc) ..
What is “good enough” security?
- **Full time incident responders needed, versus virtual**
 - Monitoring and analysis capability increase, but not enough (re: near real-time forensics & “chain of custody” evidence)

MORE??? Yes, there is much to consider,
evaluate, then effectively, collectively, protect against.

Five major tenets of Cyber / IA

- Complex and Dynamic “Digital” Policy
- E2E trust model and execution – to the edge
- Content mediation.. IA metadata, crypto-binding, etc
- Access control.. That works cross domain
- Governance and management – at all levels

These must be fully accounted for in our vision / EA

Building “good enough” trust worthy environments out of varying degrees of less trusted components

What “cyber variables” can we affect?

Elements that are effective as-is, or have a lower added ROI

- Prosecution/enforcement – need near real-time forensics, global reciprocity
- Offensive tools – good current capabilities, controlled use, escalation
- Try to fix all issues/problems – as many are intractable, givens (SCRM), etc.
- Continue to only emphasize perimeter defense – as *they* are already in!

Elements with the BEST potential impact and long term effectiveness

- Improve education and training – *cyber workforce capital management*
- Enterprise risk management – using both threats *AND* consequences
- Effective IA/Cyber Management – enforceable CM/hygiene & a trust model
- **Proactive, Dynamic CND/IA Defense** – DCD, as the best offense
 - Define & enforce network policy / SOPs – cut off those not in compliance

*Continue to finesse the first set / **Go full force on the last!***

Defense Science Board on IA

Defense Science Board; *Creating an Assured Joint DOD and Interagency Interoperable Net-Centric Enterprise*, March 2009

Warfare Commanders: “We are no longer network enabled. ***We are now network dependent.***”

“The task force reached an overall conclusion that without an integrated net-centric/cyberspace plan, threats from cyber-intelligent adversaries represent ***a clear and present danger*** to U.S. national security.”

“The primary finding in this study is that the major impediment to attaining an assured joint DOD and interagency interoperable net-centric enterprise is ***governance***—the “who is in charge?” issue.”

Naval Studies Board on IA

Naval Studies Board: *Information Assurance for Network-Centric Naval Forces*; March 2009

“Because of the forward positioning of both the Navy’s afloat and the Marine Corps expeditionary forces, IA issues for naval forces are exacerbated, and *are tightly linked to operational success.*”

“...manage system developments using sets of IA principles that are explicitly specified and required to be incorporated into the naval forces enterprise architecture, including specifically addressing the IA requirements of *service-oriented architectures....*”

“...The Office of the CNO and the Office of the CMC should consider approaches for reducing the separation and *enhancing the integration* across emerging offense, defense, and intelligence organizations related to IA.”

Notional “Navy” Top ten list (Dec 2008)

- IA Master Plan; Architecture vision; clear IA goals and objectives
- IA Governance Structure / Consistent Policies
- Workforce Quals / Certs / Training
- "Improve Speed to Capability
- Implementing newer technologies.. – HBSS, - DAR"
- IA Approach, Strategy consistent with all SYSCOMs and DoD
- IA Policy/Architecture Guidance
- Certification & Accreditation - Aggregation of systems
- Enterprise Access Control "Trust Model"
- Supply Chain Security / Defense in Breadth
- Sustain current IA and CND posture to ensure C4I current readiness

As well as these contenders:

- Integrated Computer Network Operations
- Data-centric security approach / integration with SOA
- One IA EA and directed standards / ISSE processes
- Enterprise-wide CM / Asset management
- Network awareness including afloat
- "Meaningful" IA metrics

MIEA IA / Security Recommendations

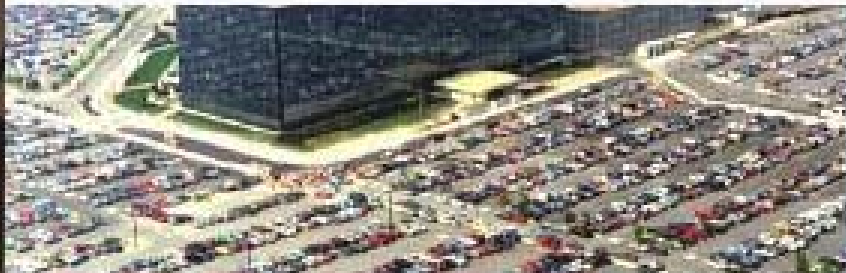
Maritime ISR Enterprise Acquisitions Recommendations			
#	Area Reviewed	Area #	Recommendation
34	Information Assurance 1	IA1	Ensure proper encryption of control signals and data transmissions between all maritime ISR sensors and ground stations
35	Information Assurance 2	IA2	Implement Virtual Secure Enclaves (within SIPRnet) on ashore and afloat ISR installations to include DCGS-N and DCGS-N Enterprise Node
36	Information Assurance 3	IA3	Investigate real-time security tagging of all maritime ISR data (both data streams and data products) using the IC-ISM standards
37	Information Assurance 4	IA4	Investigate real-time crypto-binding of all maritime ISR metadata to ensure integrity of maritime ISR data
38	Information Assurance 5	IA5	Investigate opportunities to move HAP IA technologies into PEO C4I Programs of Record
39	Information Assurance 6	IA6	Implement Attribute/Role/Authorization-Based access control capabilities for controlling user access to all maritime ISR data and analytical services
40	Information Assurance 7	IA7	Investigate and Implement cross-domain data exchange capabilities at the Maritime Centers of data to facilitate rapid distribution, replication and storage of maritime ISR data to all appropriate security enclave
41	Information Assurance 8	IA8	Pursue developing IA technologies that support "wave 3" separation of processing infrastructure and maritime ISR data services (decouples accreditation of infrastructure from accreditation of apps)
42	Information Assurance 9	IA9	Stand-Up an N2N6 funded "Mission Assurance" program that develops, fields, and operates cross cutting IA capabilities in support of virtualized, services based C2ISR capabilities



National Security Agency
Central Security Service

Corporate Technology Challenges

October 3, 2011





Technology Challenge Areas (IAD)



- Mobility, wireless networking, and secure mobile services
 - Software assurance
 - Virtualization, Separation, and Trusted Platforms
 - Cloud computing
 - Intrusion analysis and adversary tradecraft
 - Platform Integrity - Compliance assurance - Continuous Monitoring
 - Real-time situational awareness and CNO sync
 - End client security
 - Metrics and measurement for IA posture
 - Commercial architectures for assurance (e.g., CSFC)
-



Technology Challenge Areas (NTOC)



- Mobile Adversary
 - Cyber Indications and Warning
 - Mitigation Engineering
 - Countermeasure Provisioning
 - Network Intelligence
 - Predictive Analytics
 - Statistical Models for Cyber
 - High Performance Analytics
 - Mission Knowledge Management
-



Technology Challenge Areas (RD & TD)



- Wireless – especially new mobile broadband technologies –
LTE/WiMax
 - Video – collection, processing, analysis
 - Massive Data (Mining, Analytics), Statistical Analytics
 - Virtualization
 - Systems Understanding (Reverse Engineering at the system level)
 - Cyber Situational Awareness
 - Cyber Attribution
 - Advanced Technologies for HPC
 - Visualizations and tools to enhance analyst productivity
 - Secure Mobile technologies (ideally using COTS devices)
 - NISIRT
-

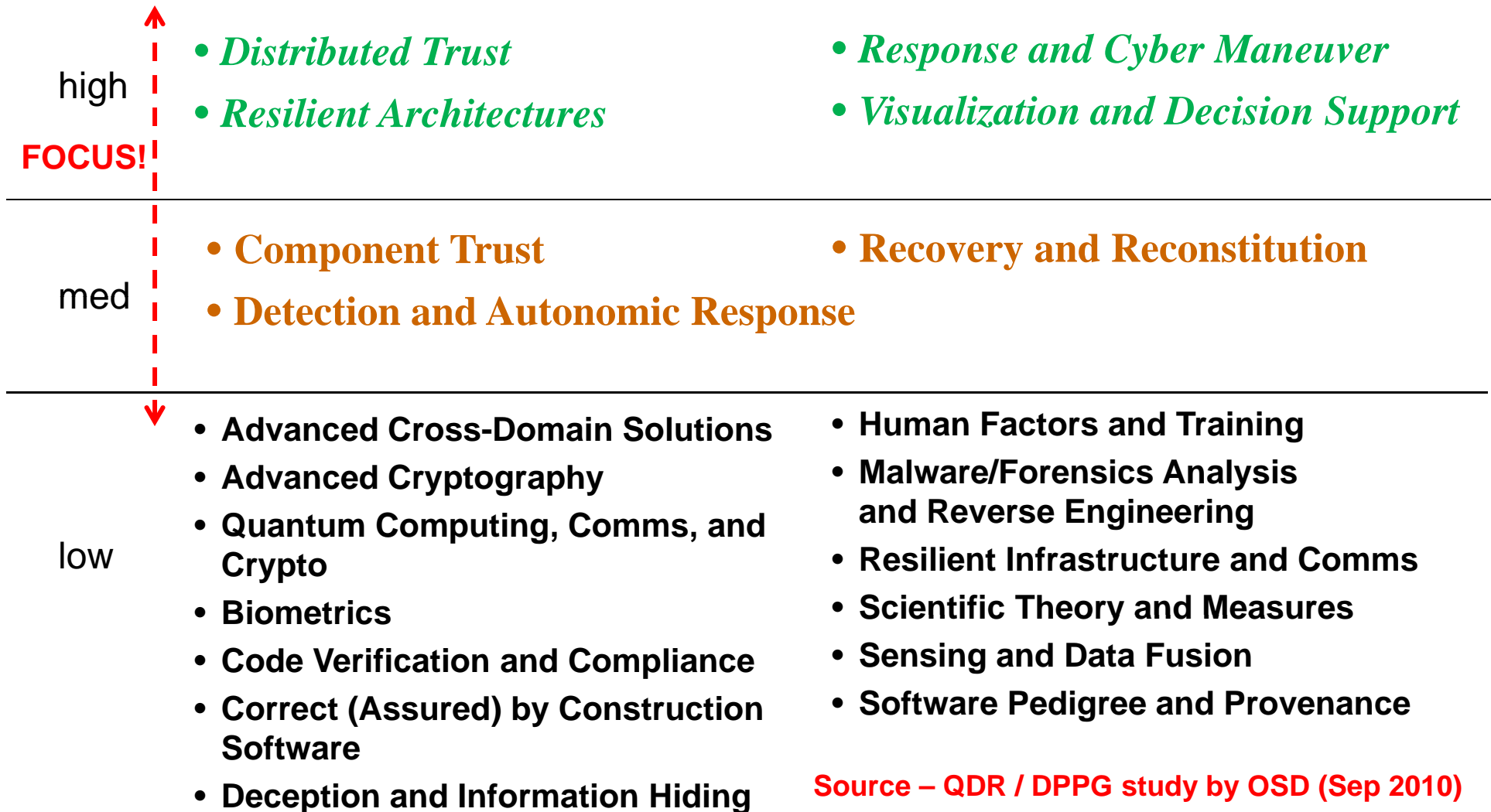


Technology Challenge Areas (SID)



- Massive Data – analytics from extremely large data sets; statistical approaches to data analysis
 - Virtualization – security vulnerabilities inherent in extant and emerging virtualization technologies
 - Advanced technologies for HPC – architectural or physical advances in cutting edge computing technologies for specialized applications
 - Visualization technology for large systems or data sets
 - Behavioral characterization of user communications
 - Methodologies for detection and visualization of malicious cyber activity
 - Video – feature extraction
-

Prioritization of the Consolidated Enabling Technology Areas (ETA)



CYBER is fundamentally about distributed trust, secure messaging!

Key cyber capabilities to develop

(think “[secure comms / messaging](#)” - here proposed wrt [top level ETAs](#))

- **Distributed Trust** --- Enable secure distributed interactions by establishing appropriate levels of trust among remote devices, systems, or users **supports:** Models and Protocols for Trust Establishment; Infrastructure; Dynamic Evaluation; Out-of-Band and Physical Trust Maintenance
- **Resilient Architectures** --- Enable functional capabilities to continue despite successful disruption or compromise by the adversary **supports:** Morphing Engines Generating Unpredictability; Secured Network Storage; System Decomposition for Mission-Tailored Tools; Response and Cyber Maneuver
- **Visualization and Decision Support** --- Enable human decision-makers to quickly understand the security and operational implications of the current situation and to rapidly ascertain the best course of action to pursue **supports:** Real-Time Analysis Engines ; Common Operational Framework; Holistic Cognitive Environment
- **Response and Cyber Maneuver** --- Enable defenders to perform shaping operations that minimize the attack space and frustrate adversary planning and to take action during attacks to block, disrupt, remove, or counter adversary actions. **supports:** Polymorphic Technologies; Cyber Obfuscation; Network Agility

Net-centric Security = “glue” = SoS and I&I aspects

Strategic Cyber Factors

- (1) Collaborate on **common enterprise IA / cyber strategy and vision**
policy mapped to prioritized capabilities with assigned resources
- (2) Develop common **overall enterprise risk assessment (ERA)**
accounts for both significant threat vectors & vulnerability consequences
- (3) **Prioritize enterprise level mitigations** from the ERA
Organizational specific items complement and weighted within the existing CNCI 12 focus areas
- (4) Align and **synchronize resources and cyber capabilities**
across federal organizations and tier 1 – tier 3 architecture perspectives
- (5) **Address pervasive lack of basic cyber hygiene** enterprise wide
within the total organization's folks, processes and products (technology)
- (6) **Reduce complexity - Build a trusted cyber infrastructure**
on top of the existing IA/CND infrastructure, *as an integrated "SoS"* - with enforced CM
- (7) **Better integrate / leverage education and offensive cyber (IO / CNO)**
thus optimize our overall cyber package and ensure synchronization and *RESILIENCY!*

**Top down approach to a balanced,
prioritized cyber execution plan**

So what can WE collectively DO?

- **Common way forward**
 - Sync with Federal cyber strategy / USCYBERCOM / other agencies
 - Support various cyber roadmap & C10F requirements / CNCI
 - Streamline acquisition process – tie to business priorities = value / affordability
- **Facilitate Collective / Collaborative Governance**
 - Integrated efforts: Plans / Policy, Operations, Acquisition, R&D, etc
 - Overall execution – coordination / cooperation between government, industry, academia, others – key cyber stakeholders
- **Cooperatively ACT on key tactical & strategic thrusts –affordably!**
 - Focus on: highest ERA ROI items, reduce complexity, enforce resiliency
- **Do the basics well & first - otherwise new toys matter little**
 - Enforce critical areas (like CM, hygiene...) and fix what ails us now
- **Leverage the bleeding edge - let NSA R7D / CNCI lead / sponsor**

Common: end-state, methods, processes & objectives

So what matters / are the key needs?

- **OSD / federal**

- Distributed Trust
- Resilient Architectures
- Response and Cyber Maneuver
- Visualization and Decision Support
- Component Trust
- Detection and Autonomic Response
- Recovery and Reconstitution

**It's NOT a lot of expensive new "cyber stuff"
– but more I&I "glue"**

- **NSA / agency**

- Mobility, wireless and secure mobile services
- Platform integrity / compliance assurance
- End client security
- Cyber indications and warning (I&W)
- Mitigation engineering (affordability)
- Massive data – (data centric security)
- Advanced technology.... (targeted)
- Virtualization – secure capabilities

Take Aways

- The best cyber way forward is to
 - do the basics well – that gets you 90+% of the way there
 - Know the next 10% is much harder and we need a common map
 - Follow the collective future state, challenge everything
- It's all about effective hygiene, managing anonymity, reducing complexity and commonality in purpose / methods
- Shared vulnerabilities will always exist, so trust but verify
- None of us is as smart OR safe as all of us as a collaborative cyber team in this heterogeneous ecosphere!

**We're either building a collaborative common way forward
Or we continue to let our shared vulnerabilities be our demise**

Summary

Q&A

Knowing what the needs / gaps are should feed your *risk management plan*, thus showing the high impact, value added mitigations and their ROI and risk reduction capabilities

For more information - contact

Mike@sciap.org

<http://www.sciap.org/blog1/>

BRUCE.ROBERTS@cubic.com

<http://xd-solutions.com/>

IA / Security “Best Practices” Overview

(Best practices are not a panacea, complete or only what you need to do – but a decent guide)

- Quantify your [business protection needs](#) – do you have an asset inventory?
- Determine [what is “good enough”](#) or minimally acceptable
- Quantify your environment’s threats and vulnerabilities
 - your list should have 10 – 50 or so threats assessed
- Have a [security policy](#) that’s useful, complete, CEO/leadership endorsed
 - yes, that’s *actually HAVE A POLICY*, choose a model, then enforce it too!
- Run [self-assessment](#) on security measures (use accepted tests, STIGs, etc) and compliance (HIPAA, PCI, CFR, SOX, etc)
- Training and awareness programs – much needed, but not a guarantee
- TEST your continuity, recovery plans, [backup – have you ever you restored?](#)
- [Encrypt where you can](#) - asses where / how you need it : IM, e-mail, file transfer, storage, backup, etc)
- Be familiar with the “NIST” IA/Security series – they are very useful!
- Always use capabilities from [approved / preferred products lists](#) (A/PPLs)
- A [risk management plan \(RMP\)](#) should roll all these into one effort

As, you can somewhat control what you plan,
but you usually ONLY get what you enforce!

Cyber Security – the Journey

STRATEGIC GOALS: DoN enterprise IA/cyber vision/strategy; Overall enterprise risk assessment (ERA); Align cyber resources and capabilities; Resolve lack of basic cyber hygiene/CM; Trusted enterprise cyber infrastructure; Integrate / leverage education and IO / CNO

KEY ACTIVITIES: ERA / prioritized mitigations; Reduce IA complexity / enforce the rules; Cyber workforce capital management; Governance / collaboration; Leverage / integrate IO/CNO - > genser / unclass protection

FOUNDATION: Overarching vision / strategy; Common architecture / standards / profiles; Common trust model / enterprise access control; Integrated IA/CND as an SoS; Lifecycle education / training; Dynamic Cyber Enterprise Management (DCEM - hygiene / CM / SOPs)

BEST POTENTIAL IMPACT / THRUSTS: Education and training; Cyber Hygiene/DCEM; Enterprise risk management; IA / Cyber Governance; & Cyber architecture = dynamic cyber defense... ->

Integrated CND & IA as a “SoS”

(all defensive “protections” must themselves act as one system)

- **It’s all about TRUST** – need a common enterprise trust model
 - Some HAP/TSM is needed, but where to put which EAL devices?
 - Need a common top-down, enforced IA/Cyber architecture/model
 - Need an alternative to commercial ISP – leverage existing dark fiber?
- **Effective / secure enterprise access control is everything:**
 - IA&A implementation focus = authorization based access control ... complemented by ABAC, RBAC, even RAdAC as an end-state...
- **Proactive/Dynamic Defensive I&W**
 - Detect abnormal patterns, characteristics, attributes, unusual requests.
 - Provide auto alerts; divert questionable actions; "wraps" issues/problems
(*This is the “catch all” capability, as we can’t protect everything near 99%*)
- **Life cycle education and training** must parallel acquisition
- Integrated **Computer Security Operations Centers** (eg: GNOSC, etc)
 - Centralized V&V / assessment collection and reporting (NCDOC / NIOC)
 - Fully integrated with DNDO – *dynamic network defensive operations*
- Institutionalize **Dynamic Cyber Enterprise Management** (DCEM)

Protect the Cyber C³ Crown Jewels!

Key Tactical Thrusts

- Organize Federal cyber security approach / governance - RACI
- Update ERA, prioritize mitigations and resources
- *Begin Dynamic Cyber Enterprise Management asap*
- Top-down enforcement of IA / Cyber architecture
 - *Secure enterprise access control / Cyber IFF*
 - Overall Dynamic Cyber Defense (DCD) approach
 - Proactive / dynamic defensive I&W – monitor abnormal behavior
 - Virtual storefront – reacts quickly to predictive IO/IA I&W
 - IA/CND treated as an integrated “SoS” with lead/lag feedback
 - Common enterprise trust model
 - *Reduce complexity - IA Building blocks / APLs with pedigrees*
 - Integrate into an enterprise cyber security model / framework
- Execute lifecycle *awareness*, education, and training

95%
security
incident
reduction

A diagram consisting of three red arrows pointing towards a central text block. One arrow originates from the 'Secure enterprise access control / Cyber IFF' bullet point and points to the central text. A second arrow originates from the 'Overall Dynamic Cyber Defense (DCD) approach' bullet point and points to the central text. A third, longer arrow originates from the 'Reduce complexity - IA Building blocks / APLs with pedigrees' bullet point and points to the central text.

High ROI Activities that get us all moving quickly

CNE / CNA

(the “offense” side of cyber)

- Provide **near-real time OPSEC to IA**
 - Effectively leverage the black side Intel into secret (& below) protections
- Establish “**Cyber” War Reserve Modes**”
 - Isolated networks, C² “order wire”, mil using dark fiber, etc
- **Fusion of diverse data**, into KM we can use in all of cyber
 - All sensors, CNE/A effects, OpSec, Intel, etc = improved CND/IA
- **Can’t easily / rapidly tell WHO the bad actors are...**
 - Need cyber detection / forensic capabilities (Service's responsibility)
 - Offensive uses best done by STRATCOM / USCYBERCOM / C10F...
- “**Cyber War**” / ROE undefined, unclear if win-lose / lose-lose

**Offensive cyber methods/tools/activities
require authorized and skilled subject matter experts**

SO... What/Who are “Key” technical Issues?

Top Cybersecurity Threat Is Users..... say Security Experts

- **SANS Major security risks** (*2 risks outweigh most others*):
 - Priority One: **Client-side software that remains unpatched.**
 - Yet we can't get into a “patch tail chase” – as threats morph quickly
 - Priority Two: **Internet-facing web sites that are vulnerable**
 - We have much SANS / OWASP / NIST guidance – not yet well followed / implemented
- **SANS Overall security risk trends:**
 - Rising numbers of zero-day vulnerabilities
 - Application Vulnerabilities Exceed OS Vulnerabilities
 - Web Application Attacks
 - Windows: Conficker/Downadup, others
 - *Apple: QuickTime and Six More, MUCH more Mac malware now*

We have met the enemy, and they are us!

Push MUCH BETTER than Pull

99.999% less data for the operator to consider

**In a world of infoglut,
for bits to have value,
they must find their consumers**



5 orders of magnitude more efficient