Cyber Perspectives

Science and Technology Roadmap

NDIA S&T Conference
14 April 2010

Pat Sullivan
SSC Pacific

Approved for Public Release. Distribution Statement A

Cyber Warfare Capabilities, Opportunities and Challenges

Capabilities:

- Global, 24x7 Network Operations
- Largest corporate internet – NMCI
- Blue and Red Team
- Attack Sensing and Warning
  - Cyberspace awareness
  - Fusion of sensor data

Opportunities / Challenges:

- Every platform a sensor
- Every sensor a network
- Network more important than ever – C2
- Information is an element of power
- Non-kinetic options as a force multiplier
- Information free-flow without borders
- Physical effects from virtual action
- Recruit, train and maintain cyber workforce

Building the right capability and capacity to achieve prominence and dominance in the information age

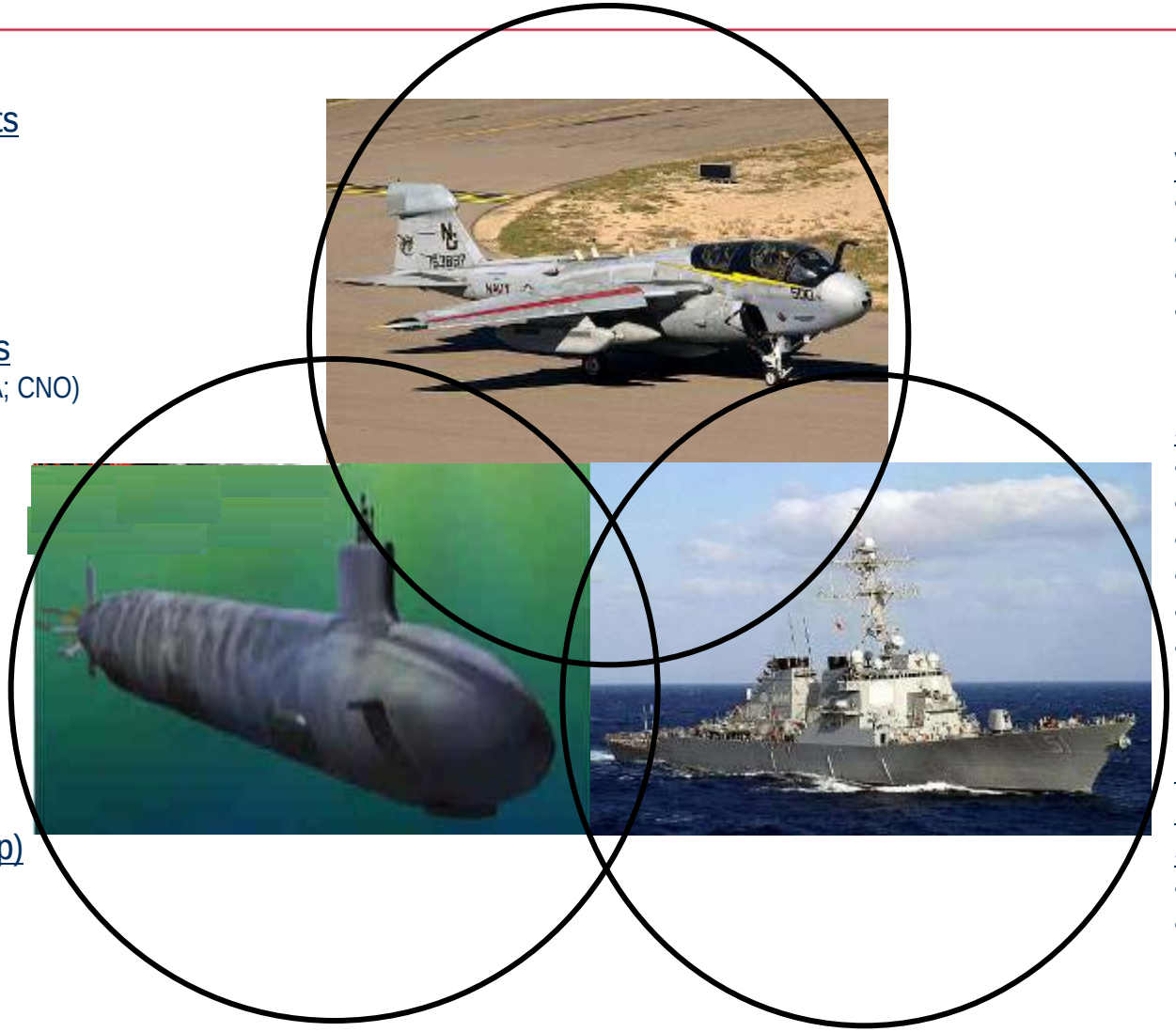
Navy Comms/ Electronic Warfare/ Sensor Networks

Intel/ Operational Nets
- SIPRNET
- JWICS
- Special Access

Non-Kinetic Weapons
- SSEE Inc F (Comms EA; CNO)
- SLQ-32 (EA), follow-on
- ISCRS/ TROLL (Subs)
- Banshee (Air)

Unclassified Nets
- MWR
- Supply

Data Flow (Physical Layer around the ship)
- Fiber Optic
- Copper



Voice Nets
- V/UHF
- HF
- SATCOM
- Cellphone

Sensor Nets
- Tomahawk Targeting
- Link 16
- Link 11
- Other fire control nets
- RADAR
- SONAR

Data Flow (Physical Layer On/ Off the Ship)
- SATCOM
- HF/ VHF/ UHF/ SHF

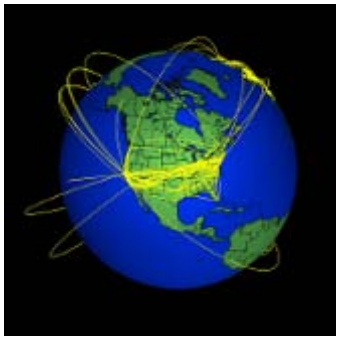
Multi-Dimensional Networks

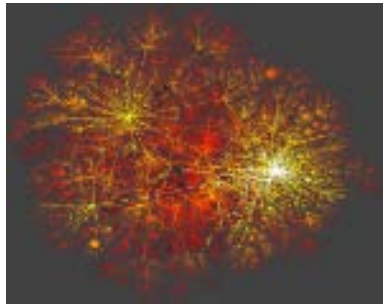
Approved for Public Release. Distribution Statement A

Cyber evolution looking forward

- All the buzz is about cyber …
  - Cyberwarfare, Cyberspace, US Cyber Command, C10F, CNCI
- … but it's misplaced, cyber is but just one means that networks use, they also use others…
  - "Networks are pervasive in all aspects of life: biological, physical, and social. They are indispensable to the workings of a global economy and to the defense of the United States against both conventional military threats and the threat of terrorism." - National Research Council, 2005, "Network Science"
- The real buzz should be about what cyber will become:
  - It will be ubiquitous: u-computing·u-networking·u-sensors·u-linking·u-information
  - Networks converge: Social + Physical + Biological Networks
  - The human aspect: how will we interact with a converged & ubiquitous network?
  - Technology drivers: miniaturization, nanotechnology, machine learning, GPS, data farms, virtualization, cloud computing
  - … and the exponential pace at which it is developing

Cyber's Future Operating Environment





u-linking

u-sensors

u-networks

u-information

Physical Networks

Social Networks

Network Convergence

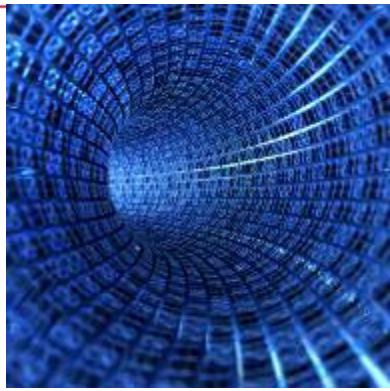
Ubiquity

Biological Networks

u-computing

u-collaboration

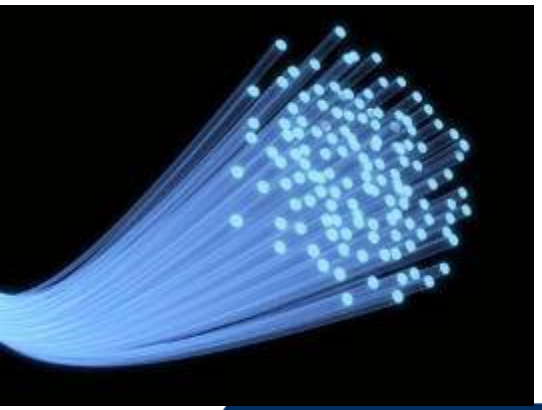
Cyber Roadmap Technical Elements



- Ubiquitous Dynamic Network Defense Operations
  - Network Operations
  - Computer Network Defense (traditional)
  - Computer Network Exploitation
  - Computer Network Attack
- Ubiquitous Assured Wireless and Wired Communications
- Ubiquitous Assured Space Capabilities
- Electronic Warfare
- Signals Intelligence
- Integrated Adaptive Planning Systems to incorporate above into conventional planning capabilities
- Policy Items
  - Expanded Public Private Partnerships

Roadmapping Process

- Start with the *"End in Mind…"*
- Revolutionary vs Evolutionary Technology Development
- Transdisciplinary Sciences as the keystone
- Execute process to build a *revolutionary* S&T Roadmap for 2025



Cyber's "S&T Grand Challenge"

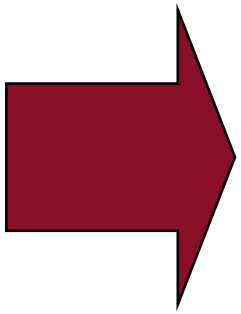
- Transparently protect Warfighters and their information
  - Decreased staffing levels, Increased autonomy
- Ubiquitous robust, secure information generation and flow
  - Ability to operate under known level of risk when parts of the system are compromised
  - Cyber elements/options tightly integrated into planning
- Isolate and mitigate Cyber threats in real time
  - Attribution and reactive Action
- Real time situational awareness of the Cyber battlespace throughout all phases of operations
  - Live and breathe in the cyber domain

Actionable and secure information sharing…

Trusted information always available

Functional Characteristics for Cyber

Challenge Area
Transparently protect Warfighters and their information
Ubiquitous robust, secure information generation and flow
Isolate and mitigate Cyber threats in real time
Near-real-time situational awareness of the Cyber battlespace



Functional Characteristics
Overall
Self-directed and self-aware
Transparent
User confidence
Prepared
Integrated system
Information
Ubiquitous, robust info integration and flow
Real-time info and action
Tell me what I need to know
Trusted
Predictive
Action
Adaptable threat detection and identification
Automated response actions
Logistics
Sustainable at reasonable cost
Trusted supply chain

Required Capabilities and Strategy

Challenge: Actionable and secure information sharing…

Trusted information always available

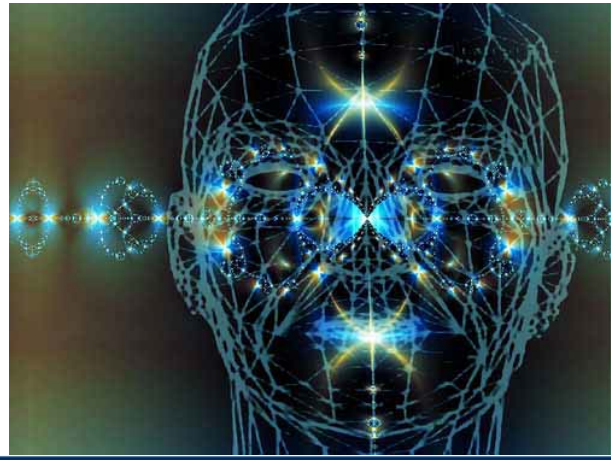
Capability Strategy:
Dynamically, proactively and predictably defend critical information and information systems

Capabilities required to support strategy 2010-2030. These capabilities spell out the Capability Strategy.

Technical Capabilities
Trusted computing from untrusted platforms
Operate with known level of risk
Reconstitution of trust
Risk-adaptive information sharing and access
Dynamic reconfigurable levels of tolerance
Ubiquitous cross domain solutions
Automatic metadata from different content/context
Context and content validation in CDS
Steganography detection and protection
Self-decontaminating systems
RT threat classification/anticipation/estimate
Decentralized, autonomous analysis
Actively sense and develop countermeasures
Dynamic use of intel
Tiered data fusion
Predictive models for attack patterns
Present cognitively appropriate info
Self protecting resilient platforms
Trusted supply chain for hardware and software
Platforms to support computationally intensive IA

Going forward……

- Cross disciplinary science will be key to developing new and innovative capabilities
- Utility of Cyber Roadmap:
  - Information for Program Planning/ POM Guidance
  - Framework for S&T planning and investments
  - Basis for planning of human capital development
    - Internal
    - S&T community
  - Focus for small business development
    - SBIR topics
  - Identify leveraging and partnering opportunities
    - E.g. DOE, DHS, NSF, NIST, DOD



Questions and Discussion