National Defense Industrial Association

RADM Edward H. Deets, III
Vice Commander, Naval Network Warfare Command

14 April 2010
Some Inconvenient Truths

• Non-kinetics may beat kinetics in the 21st century
• Business and admin systems have evolved into warfighting systems
• We can’t function today without the Internet
  – Our Millennials expect it
  – Our Millennials will use it to evolve cyber warfare
  – Our Millennials are a great source of innovation
  – DoD users make 1 billion+ Internet connections every day, passing 40TB of data
• Convenience and security must be in balance
The Challenging Battlespace

• Most rapidly changing battlespace

• More than Moore’s Law

• Battlespace is more than the networks
  – Increasing demand for computer network defense, attack and exploitation
  – Providing access to a bandwidth hungry generation
  – Fighting in an RF and network degraded environment
  – Building Navy’s EW/Spectrum Dominance

• Websense will categorize 11,000 websites as security risks in the next 60 minutes
And Increasingly More Exposed

Inbound Internet Traffic Growth

DoD Internet traffic growing 39% annually

Most Popular Sites Visited

- google.com
- streamtheworld.com: Music
- facebook.com: Social Networking
- imeem.com: Music
- yahoo.com
- rr.com: Portal
- zshare.net: File Sharing
- dailymotion.com: On-line Videos
- bitgravity.com: Streaming Television
- stagevu.com: Streaming Video
- amazon.com
- grooveshark.com: Streaming Music
- cnn.com: News
- megavideo.com: Streaming Video
- msn.com
- craigslist.org: Shopping
- eBay.com: Shopping, On-line Auctions

94% of DoD web traffic is commercial web browsing

Unconstrained Web Access Increases Exposure → Risk
How do breaches occur?

Most breaches resulted from a combination of events rather than a single action. Some form of error often directly or indirectly contributed to a compromise. In terms of deliberate action against information systems, hacking and malcode proved to be the attack method of choice among cybercriminals. Intrusion attempts targeted the application layer more than the operating system and less than a quarter of attacks exploited vulnerabilities. Ninety percent of known vulnerabilities exploited by these attacks had patches available for at least six months prior to the breach.

What commonalities exist?

66% involved data the victim did not know was on the system

75% of breaches were not discovered by the victim

83% of attacks were not highly difficult

85% of breaches were the result of opportunistic attacks

87% were considered avoidable through reasonable controls
Nature of Cyber Warfare

• We operate, defend, exploit and attack on the same platform as the adversaries
  – Threat characterization and attribution are challenging
  – Offense and defense have similar features

• Industry drives cyberspace technology

• Public, high profile adversary successes will breed additional actors
  – Inexpensive, anonymous and effective

• Cyber operations require a force that lives “on-the-network”
  – Global Cyber Common Operational Picture
  – Predictive cyber threat/response capability
  – Integrated NetOps, Defense, Exploit, Attack operations
Today’s Challenges & Solutions

• Culture
  – Accountability: full compliance with existing security directives would have reduced exploits through known vulnerabilities by over 90%
  – Culture of ‘network entitlement’ (i.e., “if I can do it, it must be okay”)
  – Commander’s ‘daily view’?
  – Damage Control, Force Protection
  – OPREP-3 Reporting

• What we don’t know about our networks
Today’s Complex Networking Environment

Multiple Classification Levels

U.S. Networks (NMCI / Legacy)

Overseas Networks (ONEnet)

Coalition Networks

Joint Forces Battlespace

Earth Station

Navy Users:
- Ashore ..................... 700k
- Afloat ...................... 100k
- Computers & Blackberry devices .. 465K

Earth Station
Afloat Networks

Average Networks Per
- Carrier 15
- Amphib 10
- Cruiser/Destroyer 7

Challenges
- Security
- Compatibility
- Platform centric acquisition
- Program alignment
- Install timelines
- Environment
- Training
- Finite manpower/Infinite demands
- Bandwidth-data choke point
- Life cycle costs
CYBERFOR Readiness is . . .

• Among other things
  – C5I afloat and ashore
  – IP’s and IT’s ready for tasking at the JNCC in Afghanistan and Iraq
  – CT’s and IT’s in Tactical Cryptologic Support and Terminal Guidance Units for tasking by Naval Special Warfare and Army Battalions
  – Space Operations Officers ready for tasking on ESGs, CSGs and in MOCs
  – CTNs ready to exploit, defend and attack
  – Transport, Connectivity, Security
Joint Crew Composite Squadron

• Navy EW Success Story
  – Competency across all warfare areas (E-4 to O-6)
    ▪ Technical Capability and Warfighter ethos
  – Assisting USA and USMC by filling EW gaps and building operational EW culture
Joint NETOPS Control Center
C10F Missions, Initial Functions & LOOs

• **Mission**
  – Central operational authority for networks, cryptology/SIGINT, IO, cyber, EW and space in support of forces afloat and ashore
  – Navy Component Commander to USCYBERCOM
  – Service Cryptologic Component Commander

• **Initial Functions**
  – Emphasis on defense
  – Operational culture

• **Lines of Operation**
  – Assuring Navy’s ability to Command and Control its operational forces in any environment
  – Achieve and sustain the ability to navigate and maneuver freely in cyberspace and the RF spectrum
  – On command, and in coordination with Joint and Navy commanders, conduct operations to achieve effects in and through cyberspace
Operational Capabilities

• Cyber Effects Delivery
  – Move to delivering information vice bodies and boxes …

• Warfighting Support
  – C10F TF Commanders integrated into targeting process
  – Build Cyber Intelligence Preparation of Environment

• Full Spectrum Cyberspace Operations
  – SIGINT-driven IO (CNA and Comms EA)
  – Grow non-kinetic capabilities and integrate into CONPLAN/OPLAN

• Operationalize Cyber
  – Integrate weapons into planning and training cycles
  – Develop non-kinetic COAs for each phase
Realigned to Achieve Information Dominance

Before

After

Echelon I

N2

N6

N3/5

N8

Multiple Resource Sponsors

Echelon II

USFFC

Multiple Operational Responsibilities

Echelon III

NNWC

Type CDR and OPS CDR

Echelon IV


Single Resource Sponsor

FLTCYBERCOM

Single Operational Commander

Navy Cyber Forces

COM 10th FLT

Type CDR

Ops CDR

NNWC

Network and Space Ops for C10F