SLIDES ONLY

NO SCRIPT PROVIDED

NDIA S&ET Conference
Cyber COI Strategic Overview
20-22 MAR 2018

Dr. Bharat Doshi
Cyber COI WG Lead
Bharat.t.doshi.civ@mail.mil

Senior Research Scientist (Cyber Security)
US Army CERDEC

Cyber COI Leadership and Membership

Steering Group:

Mr. Gary Blohm, Army, Chair
Dr. Wen Master, Navy, Deputy
Mr. Timothy Sakulich, Air Force
Mr. Chester Maciag, Air Force
Ms. Cheryl Mawhinney, NSA
Dr. Steven King, USD (R&E)

Working Group:

Dr. Bharat Doshi, Army, Chair
Mr. Giorgio Bertoli, Army
Dr. Ryan Craven, Navy, Deputy
Ms. Anna Weeks, Air Force
Dr. Todd Finkler, NSA
Ms. Sharothi Pikar, USD (R&E)

Cyber COI Sub Working Groups

Protection

- **Ryan Craven (Navy) (Lead)**
- Alex Wancowiz (Army)
- Donald Coulter (Army)
- Juanita Riley (AF)
- Kim Ferguson (NSA)

TEM June 2018

Access & Effects

- **Philip D'Ambrosio (NSA) (Lead)**
- Mark Farwell (Army)
- Bill O'Mara (AF)
- Dan Koller (Navy)

TEM Sep 2016

Cyber SA

- **Giorgio Bertoli (Army) (Lead)**
- Humza Shahid (Army)
- Mark Williams (AF)
- Danko Nebesh (NSA)
- Waleed Barnawi (Navy)

TEM June 2018

Cyber C2

- **Anna Weeks (AF) (Lead)**
- Paul Robb (Army)
- John Gancasz (AF)
- Greg Harriot (NSA)
- Joe Mathew (Navy)

TEM 8 Aug 2017

Cross Cutting TEMs on Topics of broader Interest:
Machine Learning and Artificial Intelligence 15 NOV 2017

Sub Working Groups Purpose & Responsibilities

- ***Increase grass roots engagements of SMEs in the four major S&T areas***
- ***Deep dive TEMs***
- ***Develop bottom-up collaboration opportunities***
- ***Proactively identify S&T gaps, help develop roadmaps, and proposals.***

Cyberspace

- **Cyberspace: Domain characterized by the use of electronics, electromagnetic spectrum, and software to store, modify, and exchange data via networked systems and associated physical infrastructure.**
- **Cyberspace is relatively new, fast growing, and dynamic**
  - Rapid growth of user base
  - Rapid insertion of new technologies
  - Rapid growth of new applications
- **Pervasive underpinning of nearly all personal life, business, public services, national security, and defense functions, across all phases of shaping and conflict.**
- **Reliance on the Cyberspace is growing rapidly.**

Cyberspace Growth, Ubiquity, & Dynamics

Personal, Commercial, and Some Public Service

- Global Internet
- Wi-Fi, Cellular telephony and data
- Critical Infrastructures (e.g. Energy, Transportation, Finance, and Communication)
- IoT, wearable electronics, machine-machine and man-machine systems, Autonomous Systems
- Brain-machine, Brain-brain

DoD/IC

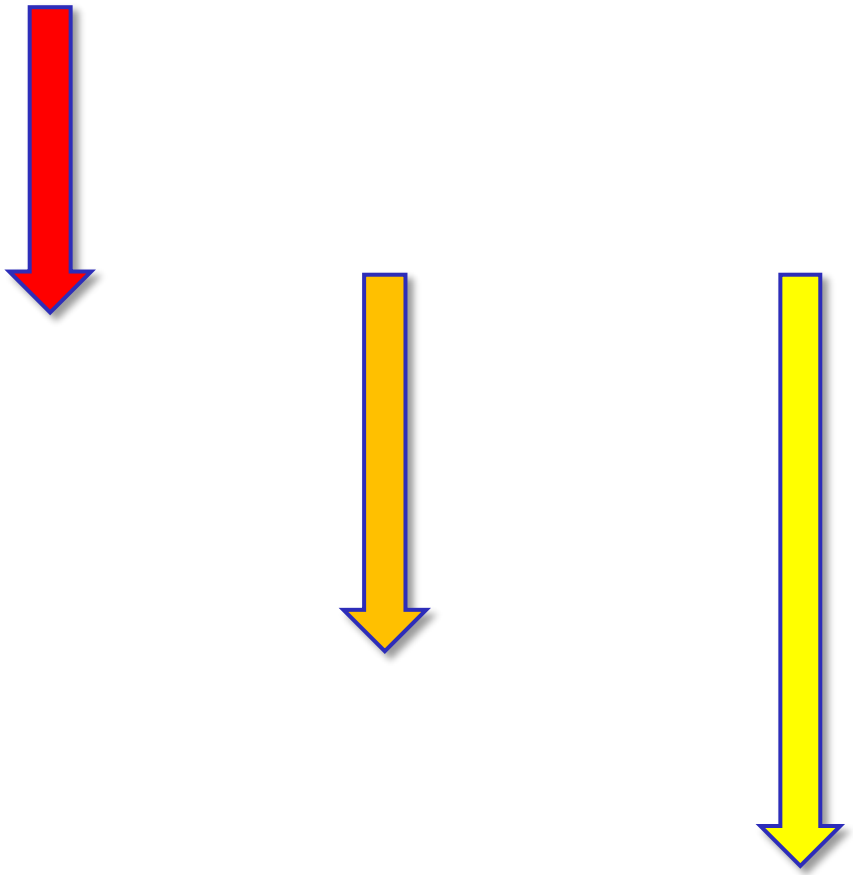
- C4I Networks
  - Ground, air, space, underwater/surface
  - Wired, wireless, mobile
  - PNT, C2, Logistics, Fire, Medical, Situation Awareness
- Energy and power systems
- Platforms : G, S, A, Space
- Weapons systems
- Wearable electronics and sensors
- Distributed sensor networks
- Machine-Machine, Man-machine and Autonomous Systems (MUM-T, Robots, UAVs, UUVs, Swarms)
- Brain-machine and brain-brain communication

Cyberspace, Cyber S&T, Cyber COI and Relationships with Other COIs

- **Other COIs deal with technologies that create new cyberspace capabilities and applications**
- **However, cyberspace is vulnerable to errors and cyber attacks that lead to adverse impact on the mission via**
  - Loss of service (Availability)
  - Exfiltration of vital information (Confidentiality and Privacy)
  - Corruption of information (Integrity)
  - Loss of control; Destruction or malfunction
- **New vulnerabilities surface as new cyberspace technologies and applications are introduced. Threats and Opportunities.**
- **Cyber COI S&T is aimed at novel approaches/technologies to secure current, emerging, and future cyberspace and its applications, and to create desired effects on adversary cyberspace.**

Steps in a Cyber Attack

- Reconnaissance
- Scanning
- Access
- Escalation
- Exfiltration
- Sustainment
- Assault
- Obfuscation



Attack vs Defense Timelines

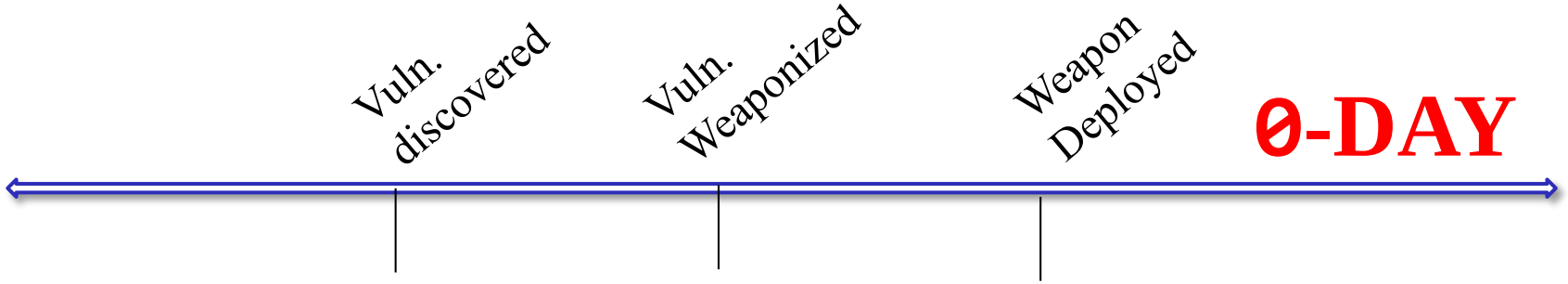


Figure: Attacker's Timeline

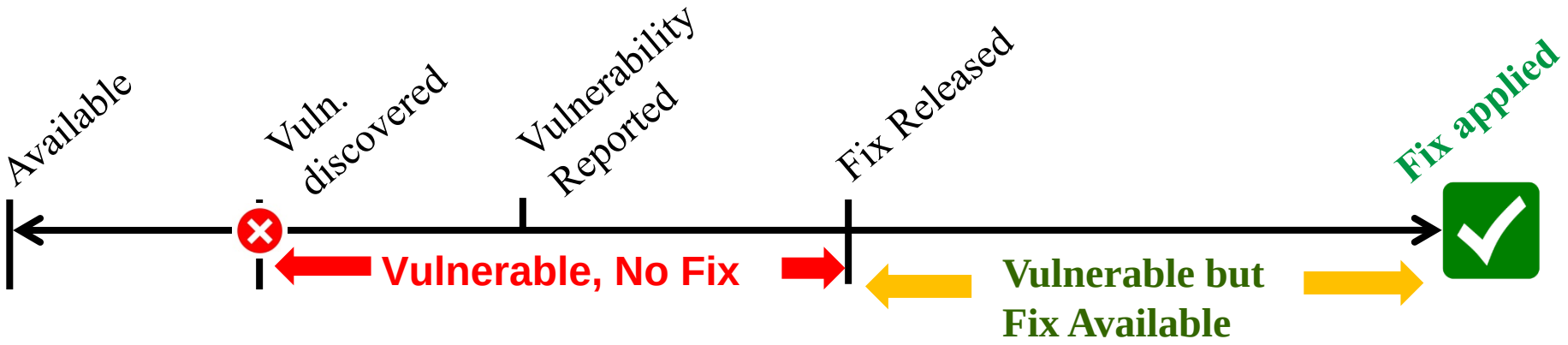


Figure: Defender's Timeline

Goals of Cyber S&T

- **Technologies that autonomously prevent the adversaries from accessing blue and gray cyberspace and minimize the adverse impact if the adversary succeeds in gaining access.**
- **Technologies that enable desired effects on the adversary cyberspace**
- **Technologies and tools to help Cyber Mission Force teams, Cyber Protection Teams, and other Cyber Operators conduct winning Defensive and Offensive Cyber Operations (DCO, OCO)**
- **Technologies and guidelines for proactively developing architectural and design principles, sensors, and analytics to ensure that emerging and future cyberspace are secure.**

Tier 1 S&T Areas of the New Two-Tier Cyber COI Taxonomy

Protection

Prevention of adversarial access to blue cyberspace. **Autonomic Cyber Resilience to** minimize the mission impact after adversarial access. **Local Sensors, Analytics, and Actions**

Effects

Successful effects in presence of adversary defenses

Cyber Situation Awareness (Cyber SA)

Technologies for collection and fusion of data from multiple sources. Analytics, machine learning, and deep learning for intrusion detection, attribution, and BDA. Echelon and role specific visualization.

Cyber Command and Control (Cyber C2)

Mission mapping. Tools for COA. Technologies, platforms, and tools for collaborative planning and evaluation of strategic and tactical plans in cyberspace.

New Two-Tier Taxonomy: Tier 1 S&T Areas and Application Areas

Tier 1 Taxonomy, Four S&T Areas

Protection
- *Prevention*
- *Resilience*

Effects
- *Delivery Mechanism*
- *Weapons*

Cyber Situation Awareness ***(Cyber SA)***

Cyber Command and Controls ***(Cyber C2)***

Applications

Broadly Applicable Technologies

Enterprise Level DoDIN

Tactical C4ISR Networks

Platforms (Ground, Sea, Air, Space)

Weapons Systems

Sensors and other IoBT Devices

Key Investment Trends

Responding to Emerging Threat and Technology Opportunities

Demand Signals from Cyber Mission Force Teams and other operational communities ➔ **Increasing S&T for Cyber SA and Cyber C2**

Increasing role of cyberspace in platforms and weapons systems ➔ New vulnerabilities, consequences, and OODA loop ➔ **increasing S&T for cyber operations on DoD Cyber Physical systems**

Projected exponential growth in low cost, small SWaP, connected devices in commercial and DoD applications (Internet of Things) ➔ **Increasing S&T for cyber operations on DoD IoT**

Rapidly decreasing cost of providing controlled dynamics in low level functions ➔ **Increasing S&T for the use of the dynamics to provide obfuscation, deception, and evasion for increasing adversary work factor**

Increasing system complexity, shrinking OODA loop, cognitive overload, and multi-source data/intelligence ➔ **Increasing S&T for machine learning and autonomy in cyber defense/offense**

- **Simplicity and minimalism for security**
- **Predictability, reusability, and controllability of effects**
- **Modeling human dimensions**

Major New Initiatives

Attack Surface Reduction for the Entire Computing and Networking Systems

- SW and protocol de-bloating, removal of unneeded features
- Virtualization

Resiliency in Platforms, Weapons systems, and Critical Infrastructure

- Fast and autonomic recovery

Low SWaP and Low Resource Devices (IoT)

- Wearable, easy-to-use, multi-factor authentication
- Defense of low resource devices

Integrated Cyber-EW-SIGINT

- Integrated SA and Integrated C2
- Multi-function hardware and software

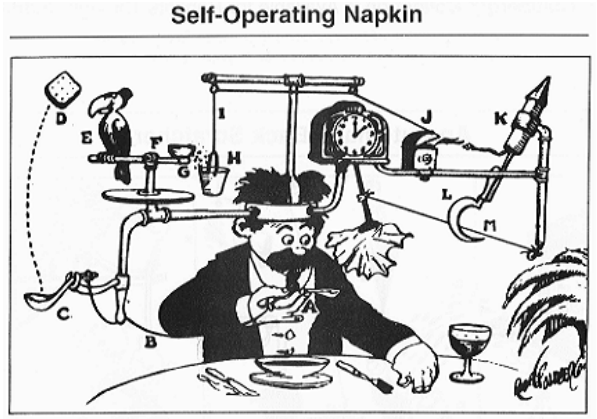
USD (R&E) Priorities

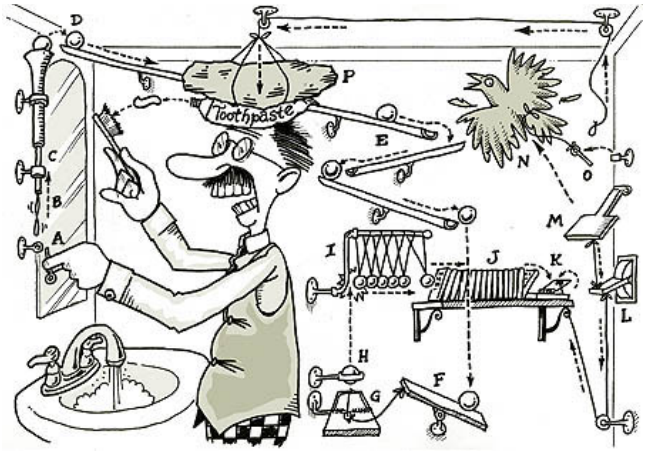
- Behavioral Cyber Science, Self-Securing Systems, Mathematical Foundations for Cyber, and Precision Effects

SW Complexity and Bloat

BACKGROUND: Modern software is exceedingly complex and bloated

- Current practices encourage it (OOP, layers of abstraction, etc.)
- Priority is to maximize code reuse and increase programmer productivity
- One-size-fits-all feature set



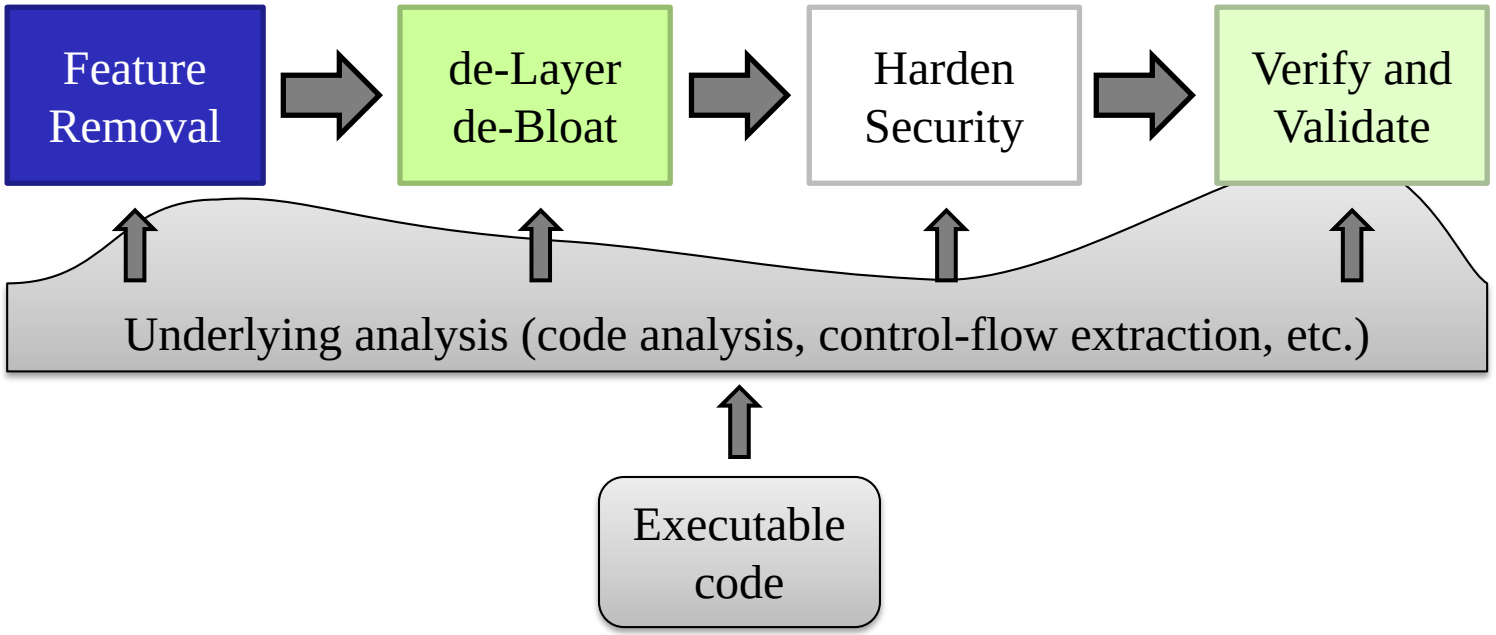


- "In every application we looked at, an enormous amount of activity was executed to accomplish simple tasks."
- "For example, a stock brokerage benchmark executes **268 method calls** and creates **70 new objects** just to move a *single date field* from SOAP to Java."

Excerpted from:
Sevitsky et. al. (IBM TJ Watson Research Center) on framework based applications
http://lcsd05.cs.tamu.edu/papers/sevitsky_et_al.pdf

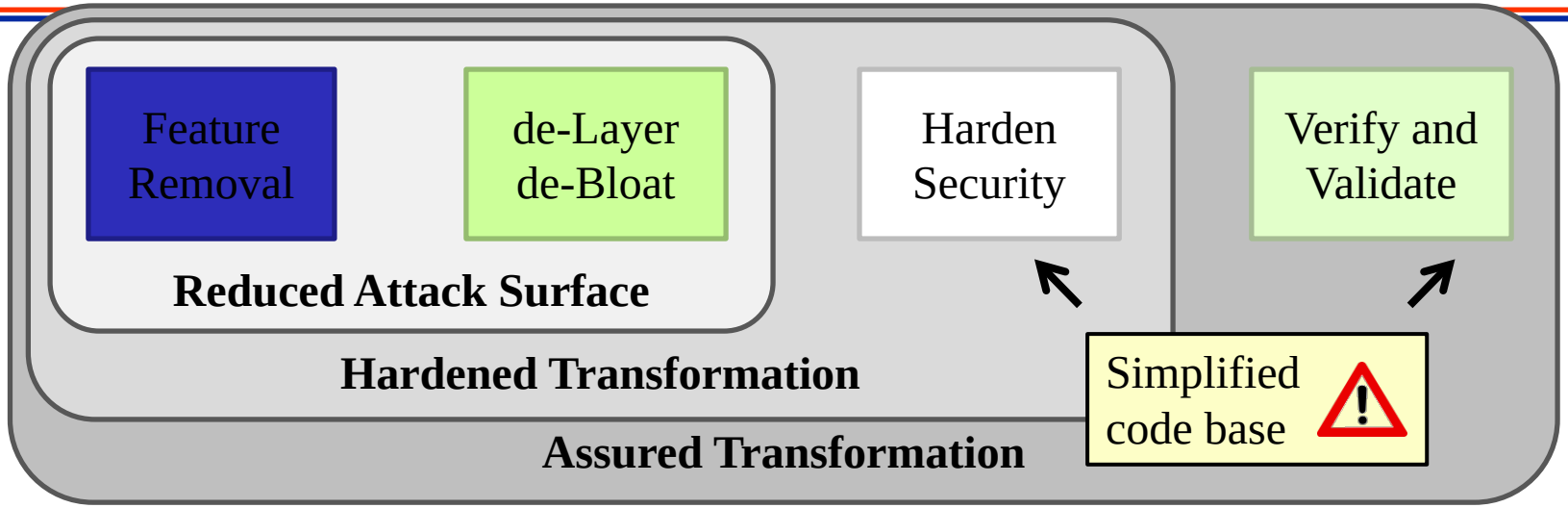
RESEARCH VISION: Late-stage / install-time transformations

- Hard to change the way people write code, so work around it
- Series of automated transformations for legacy code
- Four independent, separate steps



Improving Software Robustness and Efficiency

Architecture & Strategy for Development & Deployment



- **Feature Removal**
  - Cut unneeded functionality (admin-assist)
  - Is a functionality-preserving transformation but only for **desired** features
- **Complexity Reduction (dLB)**
  - Functionality-preserving transformation for the aggressive reduction of code size/complexity, indirection, and layers of abstraction
- **Retrofitting Security**
  - Security-focused code analysis and functionality-preserving transformations for enhancing robustness and security
- **Asserting correctness and security**
  - Automated and *in situ* verification of validation to ensure the transformation results are robust and secure

Success Stories

Protection

- SW Assurance
- SW/FW/Protocol De-bloating
- Hybrid binary/Ternary Computing
- Formal Methods for Cyber Physical Systems
- PKI for Tactical, Including Non-Person Entities
- Cross-Domain Solutions (CDS) for Enterprise, Tactical, and Tactical Edge
- System-on-the-Chip Reprogrammable Encryptor
- Cyber Defense of Microprocessors and Controllers
- Byzantine Fault Tolerance for Control Systems
- Extremely Lightweight Intrusion Detection Systems (IDS): Tactical and Tactical Edge

Effects

- Integrated Cyber Electro-Magnetic Effects
- Resilient OCO

Cyber SA

- SCADA Sensors and Remote Monitoring
- Code Attribution via Analysis of Coding Style
- CEMA SA Framework and Analytics
- Universal Composable Visualizer for SA

Cyber C2

- Cyber C2 Through Graph Visualization
- Integrated CEMA Operations Specifications
- Scalable Cyber Technology Integration
- Cyber Operations Architecture

A Sample of Recent Accomplishments

Transitions

- Low level Monitoring for popular Programmable Logic Controllers. Major impact on the security of platforms and weapons systems. Transitioned to NAVSEA and used on several ships
- Defense of embedded firmware via injection of software Symbiotes for reverse engineering, repairing, and simplifying: Transitioned to several commercial vendors.
- Several Effects Technologies transitioned to Operations and PEOs
- Visualization and post-compromise SA tools for PEOs and Operational Communities

Promising New Results

- Software De-bloating is fruitful
  - JAVA Apps: 50% Reduction
  - Java Run Time Environment (JRE): 83% Reduction
  - Firmware Bios Images: 70-85% Reduction
  - Compelling Impact on security and efficiency
    - Known bugs in JRE 50% Reduction
    - 8x Speedup on R language code
- 100-1000x reduction in memory and processing requirements for Intrusion Detection. Allows use in low resource devices and mobile networks
- Very promising accuracy in attribution using: coding style; and the attacker behavior observed in and out of the blue cyberspace
- Dynamic binary/ternary architecture for major gain in obfuscation and resilience: Demos of Cryptology; PUF; and Random Number Generator

Impact

Significant Reductions in Capability Gaps

- Secure Cross Domain Data Transfer
- Hardened Attack Surface via Static and Dynamic SW Assurance
- Cyber Resilience via Reconfiguration, Obfuscation, Deception, and Fault Tolerance
- Situation Awareness Framework and Analytics
- Low Level SA, Actions, and Recovery

Increased Mutual Reliance and Investment Leverage

- Complementary Cyber S&T Priorities for SA & C2
- Complementary Cyber S&T Priorities for Platforms and Weapons Systems
- Complementary Cyber S&T Priorities for IoT in DoD
- Complementary Cyber S&T Priorities for SW/FW/Protocol De-Bloating

Shifted Investment Focus

- Increased S&T for Cyber SA and C2
- Increased S&T for Cyber Defense/Offense for Platforms and Weapons Systems
- Stronger Interest in Machine Learning and Autonomy for Cyber Defense and Offense
- Growing Interest in Human Dimensions in Cyber Operations

S&T Focus Going Forward

Protection

- Novel Authentication Mechanisms for Tactical Environments
- SW/FW Simplicity and Minimalism
- Automated Obfuscation, Deception, and Maneuvers
- Automated Intrusion Detection and Actions, Self Securing Systems

Effects

- Predictability, Reusability, and Controllability
- Resilience and Morphability

Cyber SA

- Cyber Battle Damage Prediction and Post Attack Assessment.
- Integrated SA: Multi-Service; Organic and External Intelligence; Cyber and Electromagnetic; Cyber, EW, and Kinetic

Cyber C2

- Platform and Infrastructure Architecture
- Integrated Course of Action: Cyber and Non-Cyber

Enablers

- Machine Learning, Artificial Intelligence, and Autonomy ➔ OODA Loop, Cognitive Load
- Human Dimensions

Cyber Defense/Offense for IoT, Platforms, and Weapons Systems

Examples of Longer Term S&T

- **ML/AI and Automation with Minimal Human Assistance**
  - Vulnerability Discovery
  - Design of Defensive Techniques
  - Design and Characterization of Cyber Weapons
- **Diversity and Dynamics in Core Functions: Obfuscation and Deception**
  - Scenario Dependent Selection of Functions to be ‘Randomized’
  - Orchestration of the Selected Subset for Optimal Results
- **Mutually Learning Human-Computer Teams for Cyber Operations**
- **Ubiquitous Sensors Feeding Integrated Cyber-EW Operations**
- **Cyber Operations for Tightly Coupled Man-Machine and Autonomous Systems**
- **Quantum Computing for Cyber**

Performers for DoD Cyber S&T

- **S&T Labs in Services and Agencies: AFRL, NRL, NSA, RDECOM**
- **DOE Labs, FFRDCs, and UARCs**
- **Academia**
- **Industry Players**
  - Defense Industrial Base
  - Non-traditional
  - Small Companies with Key Expertise and Products
- **About 80% Extramural**
- **Emphasis on Leveraging Industry and Academic Expertise**

Engagement Opportunities for Industry: Engagement Mechanisms & Sources of Information

- Direct Engagement with Services S&T via feedback on IR&D plans and technology directions.
- www.FedBizOpps.Gov: Industry Days, RFIs, RFPs, BAAs.
- Defense Innovation Marketplace http://www.defenseinnovationmarketplace.mil/index.htm
- Cyber Security and Information Systems Information Analysis Center. https://www.csiac.org/
- Cooperative Agreements, SBIR/STTR
- T&E and Risk Reduction

Questions