Homeland Security Advanced Research Projects Agency

# The Federal Cybersecurity R&D Strategic Plan – What Gets Funded?

*Douglas Maughan, Ph.D.*
*Division Director*

*November 27, 2012*

http://www.cyber.st.dhs.gov

Homeland Security

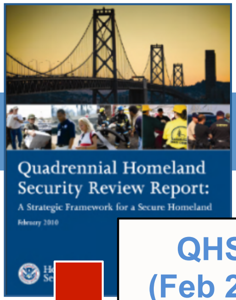
Science and Technology

Homeland Security
Science and Technology

# DHS S&T Mission Guidance

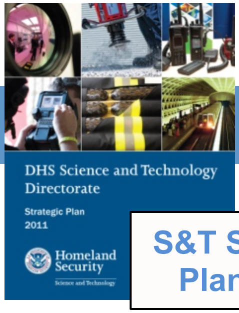
**Strategic Guidance**

Homeland Security Act 2002


Quadrennial Homeland Security Review Report:
A Strategic Framework for a Secure Homeland
February 2010

QHSR (Feb 2010)

BUR (July 2010)



S&T Strategic Plan (2011)

**QHSR**

**Threats**

Smaller Scale Terrorism | Trafficking, Crime | Pandemics, Accidents, Natural Hazards | Violent Extremism | High Consequence WMD

**Core Missions**

1. Preventing terrorism & enhancing security
2. Securing and managing our borders
3. Enforcing & administering immigration laws
4. Safeguarding and securing cyberspace
5. Ensuring resilience to disasters

**Operational Directives**

HSPD-5 National Incident Management System (2003)

HSPD-9 Defense of U.S. Agriculture & Food (2004)

HSPD-10 Biodefense for the 21st Century (2004)

HSPD-22 Domestic Chemical Defense (2007)

PPD-8 National Preparedness (2011)

***Prevention, Protection, Mitigation, Response, Recovery***

Homeland Security
Science and Technology

# Cybersecurity for the 18 Critical Infrastructure Sectors

**DHS provides advice and alerts to the 18 critical infrastructure areas …**

Agriculture & Food

Banking & Finance

Chemical Sector

Comms Sector

Commercial Facilities

Critical Manufacturing

Dams

Information Technology

Energy

Government Facilities

Healthcare and Public Health

Water

Nuclear Reactors, Materials and Waste

Postal and Shipping

Defense Industrial Base

Transportation Systems

National Monuments Icons

Emergency Services

**… DHS collaborates with sectors through Sector Coordinating Councils (SCC)**

**In the future, DHS will provide cybersecurity for …**

- ❑ The .gov and critical .com domains with a mix of:
  - ➢ Managed security services
  - ➢ Developmental activities
  - ➢ Information sharing
- ❑ Linkages to our U.S. – CERT (Computer Emergency Readiness Team)

National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 center for production of a common operating picture …

# DHS S&T Mission

***Strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise***

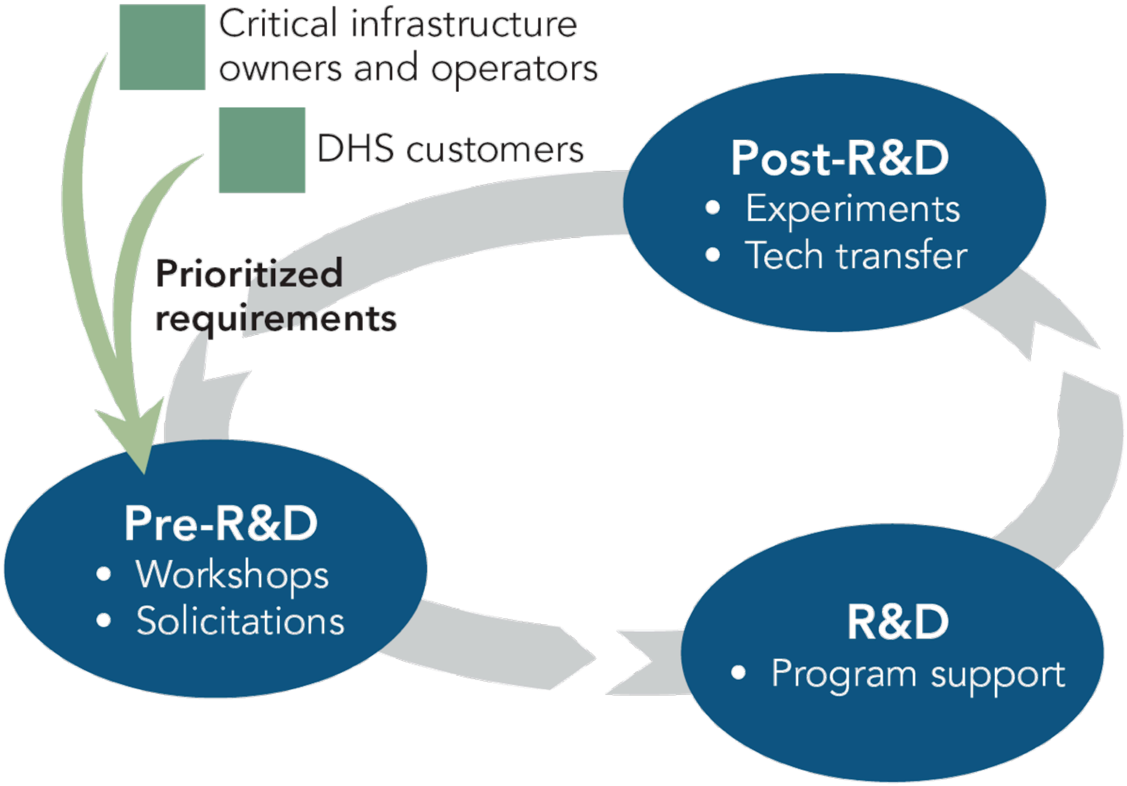
1) Create new technological capabilities and knowledge products
2) Provide Acquisition Support and Operational Analysis
3) Provide process enhancements and gain efficiencies
4) Evolve US understanding of current and future homeland security risks and opportunities

**<u>FOCUS AREAS</u>**

- Bio
- Explosives
- Cybersecurity
- First Responders

Homeland Security
Science and Technology

# CSD R&D Execution Model

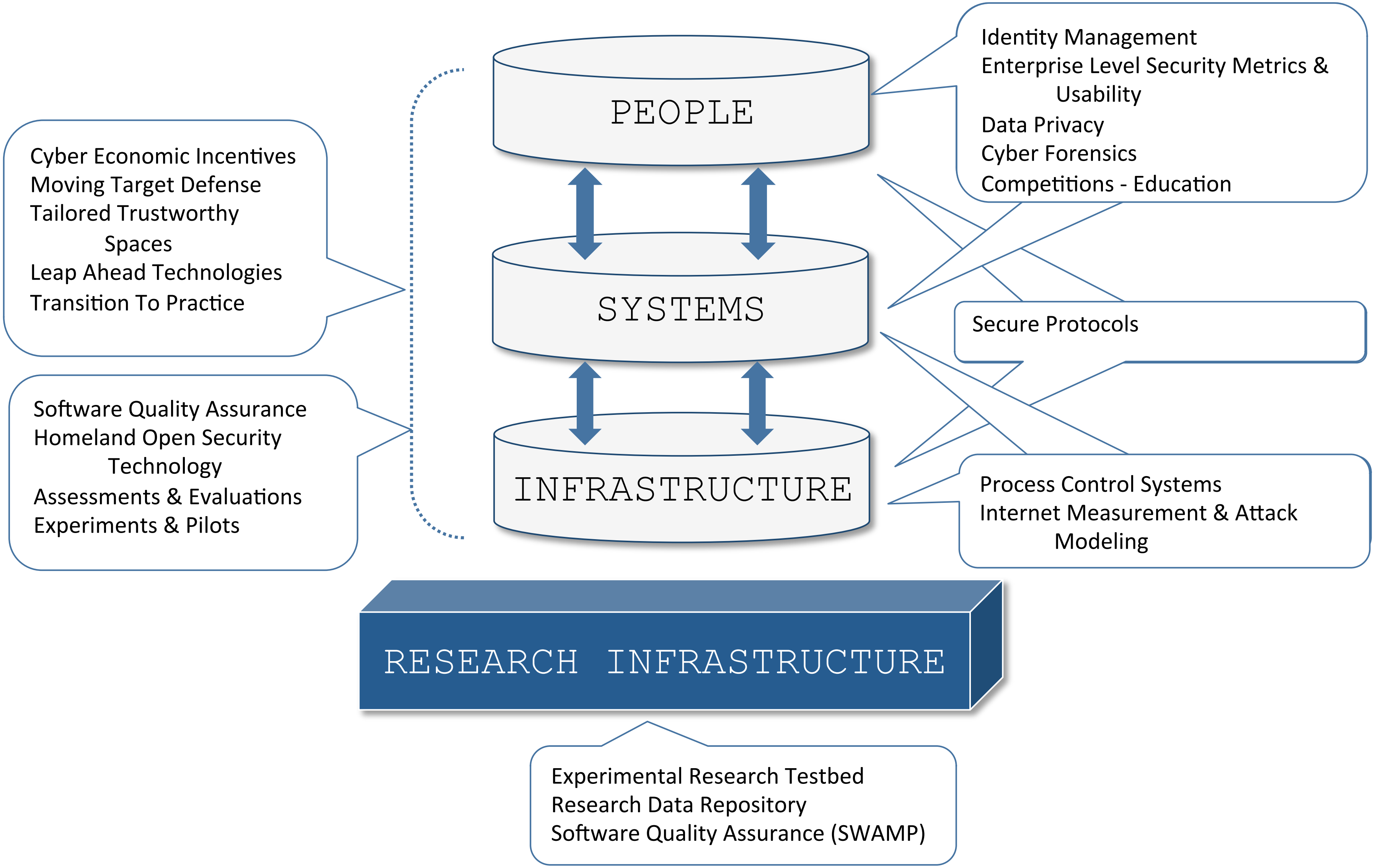


**Research
Development
Test and Evaluation &
Transition (RDTE&T)**

## Successes

- Ironkey – Secure USB
  - Standard Issue to S&T employees from S&T CIO
  - Acquired by Imation
- Komoku – Rootkit Detection Technology
  - Acquired by Microsoft
- HBGary – Memory and Malware Analysis
  - Over 100 pilot deployments as part of Cyber Forensics
- Endeavor Systems – Malware Analysis tools
  - Acquired by McAfee
- Stanford – Anti-Phishing Technologies
  - Open source; most browsers have included Stanford R&D
- Secure Decisions – Data Visualization
  - Pilot with DHS/NCSD/US-CERT; Acquisition

# CSD Programs and Relationships - Across Layers



Identity Management
Enterprise Level Security Metrics & Usability
Data Privacy
Cyber Forensics
Competitions - Education

Secure Protocols

Process Control Systems
Internet Measurement & Attack Modeling

Cyber Economic Incentives
Moving Target Defense
Tailored Trustworthy Spaces
Leap Ahead Technologies
Transition To Practice

Software Quality Assurance
Homeland Open Security Technology
Assessments & Evaluations
Experiments & Pilots

Experimental Research Testbed
Research Data Repository
Software Quality Assurance (SWAMP)

# Cyber Security R&D Broad Agency Announcement (BAA)

- Delivers both near-term and medium-term solutions
  - To **develop new and enhanced technologies** for the detection of, prevention of, and response to cyber attacks on the nation's critical information infrastructure, based on customer requirements
  - To perform research and development (R&D) aimed at **improving the security of existing deployed technologies** and to ensure the security of new emerging cybersecurity systems;
  - To **facilitate the transfer of these technologies** into operational environments.

- Proposals Received According to 3 Levels of Technology Maturity

**Type I (New Technologies)**

- ✓ Applied Research Phase
- ✓ Development Phase
- ✓ Demo in Op Environ.
- ✓ Funding ≤ $3M & 36 mos.

**Type II (Prototype Technologies)**

- ✓ More Mature Prototypes
- ✓ Development Phase
- ✓ Demo in Op Environ.
- ✓ Funding ≤ $2M & 24 mos.

**Type III (Mature Technologies)**

- ✓ Mature Technology
- ✓ Demo Only in Op Environ.
- ✓ Funding ≤ $750K & 12 mos.

**Note: Technology Demonstrations = Test, Evaluation, and Pilot deployment in DHS "customer" environments**

# BAA 11-02 Technical Topic Areas (TTAs)

| | | |
|---|---|---|
| TTA-1 | Software Assurance | DHS, FSSCC |
| TTA-2 | Enterprise-Level Security Metrics | DHS, FSSCC |
| TTA-3 | Usable Security | DHS, FSSCC |
| TTA-4 | Insider Threat | DHS, FSSCC |
| TTA-5 | Resilient Systems and Networks | DHS, FSSCC |
| TTA-6 | Modeling of Internet Attacks | DHS |
| TTA-7 | Network Mapping and Measurement | DHS |
| TTA-8 | Incident Response Communities | DHS |
| TTA-9 | Cyber Economics | CNCI |
| TTA-10 | Digital Provenance | CNCI |
| TTA-11 | Hardware-Enabled Trust | CNCI |
| TTA-12 | Moving Target Defense | CNCI |
| TTA-13 | Nature-Inspired Cyber Health | CNCI |
| TTA-14 | Software Assurance MarketPlace (SWAMP) | S&T |

- ➢ 1003 White Papers
- ➢ 224 Full Proposals encouraged
- ➢ 34 Awards – Sep/Oct 2012

- ➢ Int'l participation from AUS, UK, CA, NL, SWE
- ➢ Over $4M of joint funding

# BAA 11-02 Winning Awards

| | |
|---|---|
| Applied Visions, Inc | Oak Ridge National Laboratory |
| Carnegie-Mellon University | Pacific NW National Laboratory |
| Columbia University | Purdue University |
| Def-Logix | Raytheon BBN Technologies |
| George Mason University | Rutgers University |
| Georgia Tech Research Corp. | Princeton University |
| HRL Laboratories, LLC | University of Alabama at Birmingham |
| IBM Research | University of North Carolina |
| International Computer Science Institute | Dartmouth College |
| ITT Exelis | Indiana University |
| Kestrel Technology, LLC | University of California, San Diego |
| Merit Network Inc | University of Houston |
| Morgridge Institute for Research | University of Illinois at Urbana-Champaign |
| Naval Postgraduate School | University of Maryland |
| Northrop Grumman Information Systems | USC Information Sciences Institute |

# Reducing the Challenges to Making Cybersecurity Investments in the Private Sector

- Primary Objective: to understand more fully the challenges associated with making cybersecurity investments in the private sector and to recommend policies for facilitating the appropriate level of such investments (emphasis will be given to firms that own and/or operate assets critical to the national infrastructure).

- In pursuing this objective, we begin by developing a conceptual framework for making cybersecurity investments. In other words, since cybersecurity investments compete with other investment opportunities available to firms, they need to be justified by showing that the benefits exceed the costs, in terms of NPV.

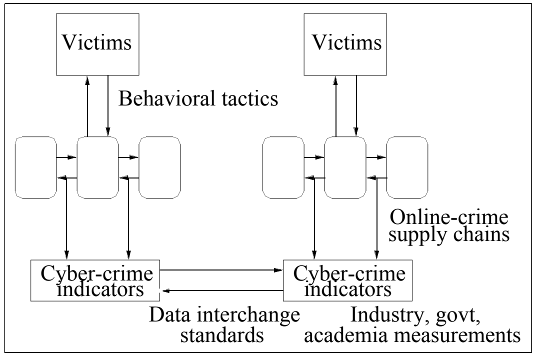
$$PV = -C_0 + \sum_{t=1}^{n} \frac{\mathrm{B}_t - \mathrm{C}_t}{(1+k)^t}$$

# Understanding & Disrupting the Economics of Cybercrime

BAA Number: Cyber Security BAA-11-02
Title: Understanding and Disrupting the Economics of Cybercrime

Offeror Name: Carnegie Mellon University
Date: October 10, 2012

Photograph or artist's concept:



Victims
Victims
Behavioral tactics
Online-crime supply chains
Cyber-crime indicators
Cyber-crime indicators
Data interchange standards
Industry, govt, academia measurements

Holistic view of cyber-criminal economics

The figure represents the different areas of investigation and their connections with each other

**Operational capability**:
**Performance targets**: achieve operational understanding of how cyber-crime supply chains work, taxonomy of behavioral tactics used by malfeasants to compromise their targets, data interchange standards for sharing cyber-crime data, design of a set of cyber-crime indicators.
Performance of key parameters will be evaluated by their usefulness to law enforcement and industry; as well as peer-reviewed publication output.
No cost of ownership: knowledge and standards will be publicly disseminated.
Project directly addresses all four main topics of TTA #9.

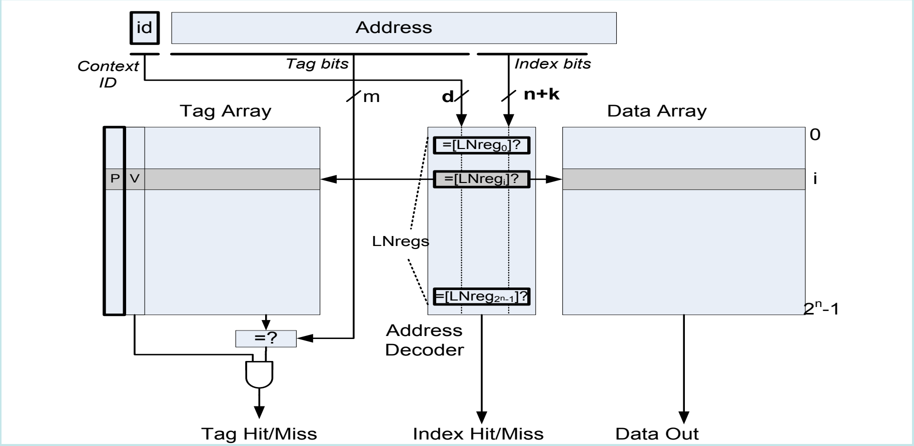
**Proposed Technical Approach**:
Directly addresses all main topics (g(1), g(2), g(3) and g(4)) of TTA#9, "Cyber Economics."
**Tasks:** (1) Designing cyber-crime indicators, (2) Designing data interchange formats and standards, (3) Modeling online-crime supply chains, and (4) Modeling attackers' behavioral psychology.
**Current status:** Fundamental research; design phase.
**Actions done to date:** considerable expertise in acquiring cyber-crime data; preliminary published research in behavioral economics applied to online crime; industry partnerships under way.

This research inscribes itself into the research agendas of all five PIs.

**Schedule, Cost, Deliverables, & Contact Info**:
Three years, Type I project (New Technologies). Yearly retreat planned to refine objectives and assess progress.
**Deliverables**: Peer-reviewed publications related to all four tasks describing recommended algorithms and methodologies; data interchange standard drafts; subset of online crime data that could be shared through PREDICT; (if applicable) software prototypes of online crime detection algorithms;
**Corporate Information**: Offeror: Carnegie Mellon University; **Administrative P.O.C.:** Kristen Jackson; Office of Sponsored Programs; 5000 Forbes Ave, Warner Hall, 4th Floor; Pittsburgh, PA 15213; **Technical P.O.C.:** Nicolas Christin; CIC Room 2108; 4720 Forbes Ave; Pittsburgh, PA 15213

# Using Moving Target Defense for Secure Hardware Design

Homeland Security
Science and Technology



**•Novel leak-free cache design that also improves performance!**

## Proposed Technical Approach:

- Novel cache design modifies a direct-mapped cache with:
  - ➢Dynamic memory to cache mapping
  - ➢Random replacement algorithm
  - ➢Circuit re-design of address decoder
  - ➢Longer cache index
- Proposed Tasks:
  - ➢Demonstrate system performance improvement due to the use of Newcache via a behavior level simulation.
  - ➢Demonstrate the security enhancement, overcoming the side channel attack vulnerability of all existing cache designs.
  - ➢Design and fabricate a Newcache chip to show actual physical size, power and performance compared to existing offerings.
- Base technology and feasibility established at Princeton.
- World-class custom circuit designers, Analog Bits, Inc., for chip design.

## Operational Capability:

- Goal: To secure the processor's cache from information leakage through cache side-channel attacks.
- No software impact. No code changes required.
- Best-in-class performance: access time similar to direct-mapped cache designs with cache miss performance equal to set-associative caches.
- Physical die area and power similar to direct-mapped cache implementations of equal size.
- After initial design, no known impact to cost of ownership.
- Uses Moving Target Defense to design secure, leak-free cache memories needed by all computing products

## Schedule, Cost, Deliverables, & Contact Information

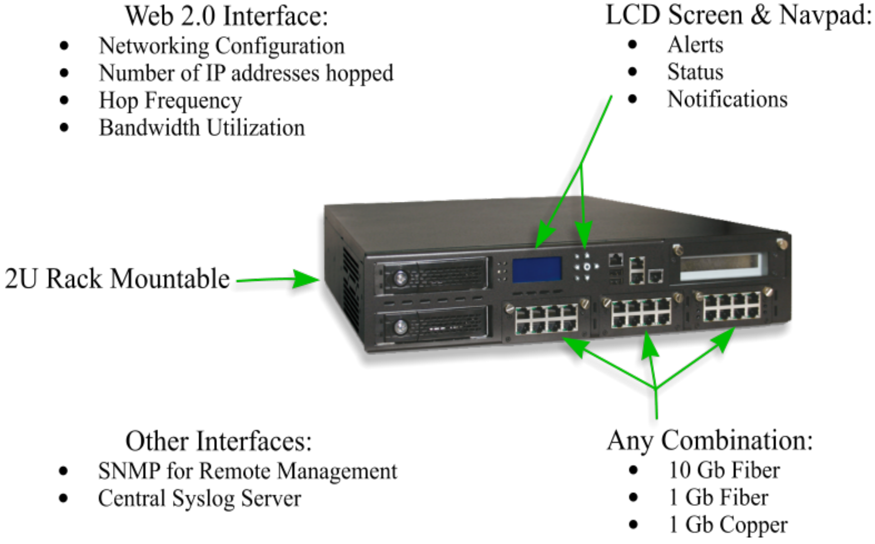
- Schedule: 24 months.
- Deliverables:
  - ✓Behavioral model of Newcache
  - ✓Document of cache miss performance for various applications
  - ✓ Test chip with custom circuit design of Newcache
  - ✓ Document of chip design, testing and evaluation.

Contact Information: Prof. Ruby B. Lee
Dept. of Electrical Engineering,
Princeton University
Princeton, NJ 08544
Tel: 609.258.1426
E-mail: rblee@princeton.edu

# Appliance for Active Repositioning in Cyberspace (AARC)

Homeland Security
Science and Technology

NORTHROP GRUMMAN



**Operational Capability:**

1. Operate the ARCSYNE technology as close to 10 Gbit/sec as possible
2. Move position in cyberspace at least 10 times/sec while handling the high-bandwidth network traffic
3. Abstract the complexity of IP hopping by developing configuration, reporting, and status services
4. The AARC development will help users obtain the advantages of moving-target defense without the technology becoming a liability

**Proposed Technical Approach:**

1. Port the existing ARCSYNE IP hopping system funded by the Air Force to a high-performance system with advanced system management tools
2. Test and benchmark AARC performance, develop system management services to abstract chaos and complexity
3. Internal AFRL testing, Northrop Grumman testing in a laboratory environment and on the Internet, and used in events such as ACE Hackfest
4. The core ARCSYNE technology and investigation of its effectiveness are ongoing

**Schedule, Deliverables, & Contact Info:**

Period of Performance: 12 Months

**Deliverables:**

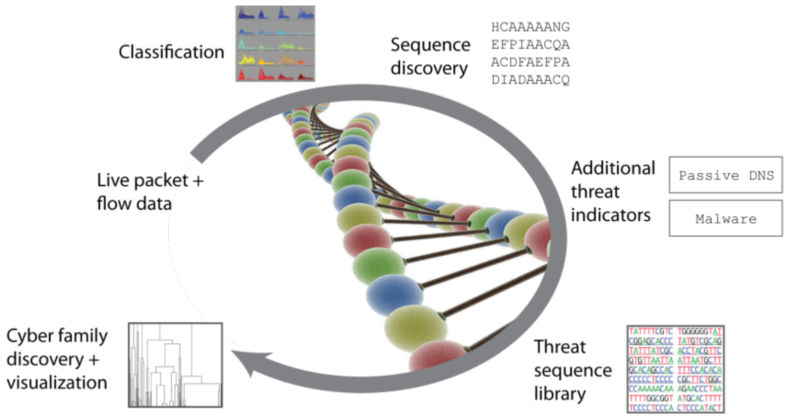
3 High-Performance AARCs
AARC Software Source Code
User Guide, Performance Benchmarks, Etc.

**Corporate Information:**

POC: Jeffrey L. Foley
7902 Turin Road, Suite 1
Rome, NY 13440
Phone: (315) 338-5404
jeffrey.l.foley@ngc.com

# LINEBACkER: LINE-speed Bio-inspired Analysis and Characterization for Event Recognition

- Cyber Security BAA 11-02 — Pacific Northwest National Laboratory
- **LINEBACkER: LINE-speed Bio-inspired Analysis and Characterization for Event Recognition**
- **Biosequence-based discovery of evolving threats** — TTA# 13



**Operational Capability:**

1. Ability to discover malicious network activity through sequence analysis across the U.S. research and engineering computing infrastructure
2. Construction of sequences from packet/flow data at rates exceeding 10 billion records per day
3. Support for submission and correlation of sequence patterns in the Research and Education Network Information Sharing and Analysis Center (REN-ISAC) Security Event System

**Proposed Technical Approach:**

1. Apply high-performance biosequence analysis that enables inexact string matching of streaming network traffic. Approach is robust to polymorphic threats and supports “family resemblance” attribution.
2. **Tasks**: Characterize baseline behavior, convert raw packets to bio-representation, construct family tree of cyber event types, create visual interface, deploy at REN-ISAC for the Global Research Network Operations Center
3. **Current status**: Builds upon existing MLSTONES (TRL 3) and CLIQUE (TRL 7) applications

**Schedule, Cost:**

Type II (2.5 yr)

**Deliverables:**

Operational product/tech transfer of biosequence-based threat detection for use in 300+ institutions collaborating via REN-ISAC

Ability to deliver capability to US-CERT as part of existing operational relationship

**Corporate Information:**

Pacific Northwest National Laboratory
Christopher Oehmen
PO Box 999, MSIN J4-33, Richland, WA 99352
(509) 375-2038; email: christopher.oehmen@pnl.gov

# Bio-Inspired Anomaly Detection

*Distributed Intelligence*

finds the *elusive* adversary

**Operational Capability**

*1. Performance targets:* Basic principles in 12 mo; Proof of concept in 24 mo; (Option) field testing and tech transfer in 36 mo.

*2. Quantify performance for key parameters:* Key performance measures derived in Year 1 will be used to evaluate effectiveness for appropriate botnet detection scenarios

*3. Cost of ownership:* None. Project results will be in public domain

*4. Address how the proposed development addresses the goals in the BAA.* Provides scalable distributed intelligence for detecting hard-to-find malware-induced behavior; leverages biological understanding of bees and ants to design communication protocols;

results in significant tech transfer

**Proposed Technical Approach**

*1. Addressing goals in the BAA:* Models biological systems for new methods for cyber-health plus technology transfer.

*2. Base Period tasks:* Define distributed detection algorithms; Implement and test software simulations to test algorithms on simple network topologies; Build networking substrate; Test and evaluate anomaly detection performance on a diversity of anomalies.

*3. Current status:* The biological phenomena have already been studied by the proposer. Proposed work will marry this with cyber security.

4. *Describe any actions done to date.* None. This is a fresh proposal.

*5. Describe any related ongoing effort by the offeror:* Distributed correlation capability is on a short term list in at least one HP security product unit and in HP networking.

**Schedule, Cost, Deliverables, Contact Info**

*Milestones:* Biology-based detection algorithms designed and evaluated December 2012; ProCurve Networking prototype delivered December 2013; Tech transfer December 2014

*Period of performance:* 3 years

*Deliverables*: Application of basic principles of bio-inspired distributed detection;

Enhanced network switches with detection;

Decentralized switch protocols for data sharing; Consolidated prototype; Tech transfer

*Corporate Information:*

Sarah Dumais, Rutgers University, 3 Rutgers Plaza, New Brunswick, NJ 08901, phone: 732-932-0150 x 2107, fax: 732-932-0162, email: dumais@grants.rutgers.edu

# Summary

- Cybersecurity research is a key area of innovation needed to support our future
- DHS S&T continues with an aggressive cyber security research agenda
  - Working to solve the cyber security problems of our current (and future) infrastructure and systems
  - Working with academe and industry to improve research tools and datasets
  - Looking at future R&D agendas with the most impact for the nation, including education
- Need to continue strong emphasis on technology transfer and experimental deployments

***Douglas Maughan, Ph.D.***

***Division Director***

***Cyber Security Division***

***Homeland Security Advanced Research Projects Agency (HSARPA)***

***douglas.maughan@dhs.gov***

***202-254-6145 / 202-360-3170***

For more information, visit

**http://www.cyber.st.dhs.gov**

Homeland Security

Science and Technology