

DHS SCIENCE AND TECHNOLOGY

CSD Project Overview

March 13 , 2018



**Homeland
Security**

Science and Technology

Dr. Ann Cox

Program Manager

Cyber Security Division

Science and Technology Directorate

CSD Mission & Strategy

REQUIREMENTS



CSD MISSION

- Develop and deliver new technologies, tools and techniques to defend and secure current and future systems and networks
- Conduct and support technology transition efforts
- Provide R&D leadership and coordination within the government, academia, private sector and international cybersecurity community
- 2016 Funding \$86M



CSD STRATEGY

**Trustworthy
Cyber
Infrastructure**

**Cybersecurity
Research
Infrastructure**

**Network &
System
Security and
Investigations**

**Cyber Physical
Systems**

**Transition and
Outreach**

Stakeholders

Government
Venture Capital
International

IT Security Companies
Open Source

Outreach Methods (Sampling)

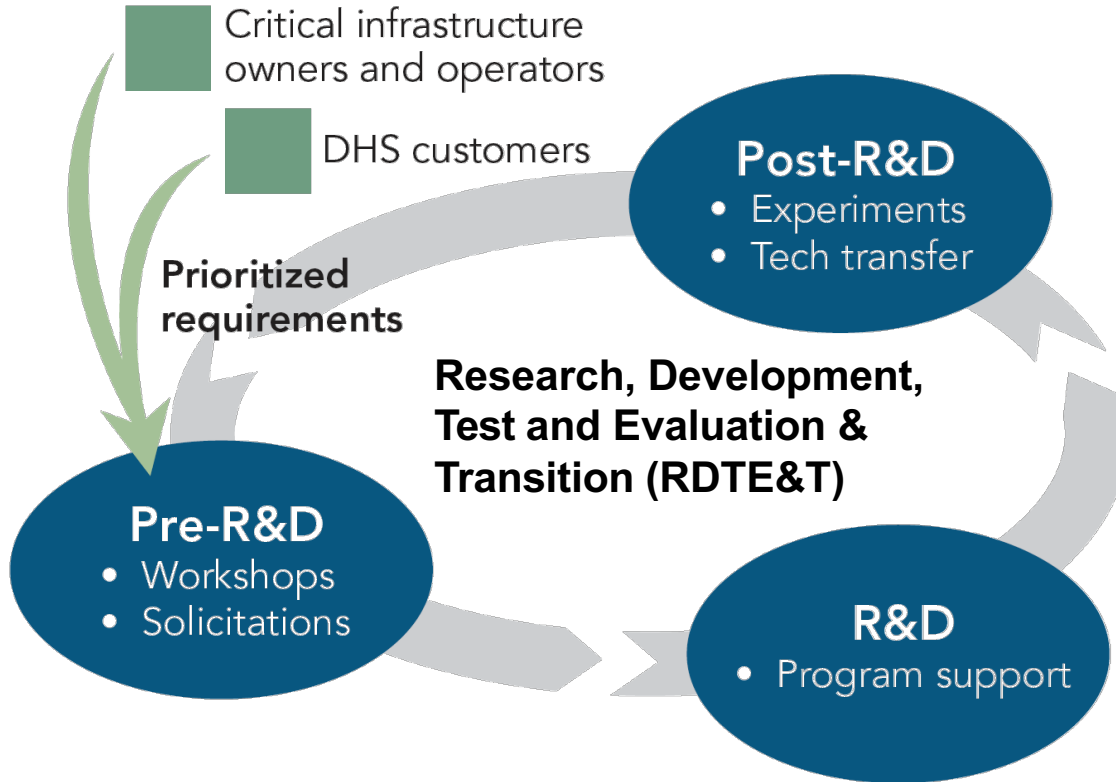
Technology Demonstrations
Speaking Engagements
Program Reviews

Social Media
Media Outreach

RESEARCH REQUIREMENT INPUTS



CSD R&D Execution Model



Successes

Over 30 products transitioned since 2004, including:

- 2004 – BAA 04-17
 - 5 commercial products
 - 2 Open Source products
- 2005 – BAA 05-10 (RTAP)
 - 1 commercial product
 - 1 GOTS product
 - 1 Open Source product
- 2007 – BAA 07-09
 - 2 commercial products
- 2011 – BAA 11-02 (more to come)
 - 1 Open Source product
 - 1 Research Infrastructure
- Law Enforcement Support
 - 2 commercial products
 - 1 Open Source product
 - Multiple Knowledge products
- Identity Management
 - 1 Open Source standard and GOTS solution
- SBIRs
 - 8 commercial products
 - 2 Open Source products

"Crossing the 'Valley of Death': Transitioning Cybersecurity Research into Practice,"

IEEE *Security & Privacy*, March-April 2013, Maughan, Douglas; Balenson, David; Lindqvist, Ulf; Tudor, Zachary

<http://www.computer.org/portal/web/computingnow/securityandprivacy>



Application of Network Measurement Science


Current Capability and Research Needs

- Research in such areas as Network Mapping and Measurement, Resilient Systems, Network Attack Modeling and Embedded System Security is essential for protecting critical infrastructure throughout the United States and the world.

- Progress in these areas has identified a need to understand and address issues related to widespread Disruptive Events to the Internet
- For Disruptive Events on the Internet, there is no standard definition, identification, or reporting process currently available. This makes prediction and attribution especially difficult.

Status Quo: Network Measurement Science Today

There are many individual measurements and tools, such as ping, traceroute in various versions, NetFlow, packet sampling, etc. but the data are rarely combined for more accurate analysis



Techniques for fusing data and analysis of the fused data are generally not available



Attribution analysis is still in its early development



Status Quo: With Prediction, Identification, Attribution and Reporting of NIDEs

There are many individual measurements and tools, such as ping, traceroute in various versions, NetFlow, packet sampling, etc. but the data are rarely combined for more accurate analysis

- *Network/ Internet Disruptive Events (NIDEs) are identified*

Techniques for fusing data and analysis of the fused data are generally not available

- *Identification and reporting of NIDEs is made in near real time*

Attribution analysis is still in its early development

- *Some attribution analysis will be available*

Shifts advantage toward defenders through identification, attribution, and reporting of Network/Internet Disruptive Events

Problem: Internet Disruptive Events

The measurement and monitoring that currently takes place is →

Government level, may be classified data ↓

The internet is vast and extremely difficult to “monitor”. Although many efforts to make individual measurements exist, they are limited in scope, and cannot detect or communicate Network/Internet Disruptive Events (NIDEs) until the event has already occurred.

Private sector, proprietary data

Academic, limited in scope



Problem: Advantage Favors Chaos

•Resources Costs Favor Attackers

- Attacks require fewer resources because they can be narrowly focused, whereas defenders must spread resources to cover all attack surfaces
- The size and scope of the internet allows small malicious actions to go undetected

• Problems may be caused by deliberate or accidental events, or as an unintended consequence of some other benign effort

- May exploit unknown vulnerabilities
- Will not be anticipated through monitoring

•Proprietary networks and a highly competitive environment discourage information sharing and broad based defense

- The development of systems to identify, monitor, attribute, and communicate NIDEs will encourage best practices and allow for a more uniform resiliency

TTA 1: Definition, Identification and Reporting of Network/Internet Disruptive Events

Definition and identification of Network / Internet Disruptive Events (NIDEs)

- Define a Network/Internet-scale Disruptive Event (NIDE) in terms of quantifiable metrics and classifications, as well as documenting required sensors and data to measure the NIDEs, and produce a NIDE Identification Document.

Reporting and operational production of Network / Internet Disruptive Events

- Develop an analysis methodology and techniques to sense and identify NIDEs, preferably for identification in near-real-time, and document the results in an NIDE Analysis Framework Document. Develop operational code for NIDE reporting.

Develop an API for communication of the identification, attribution and reporting of NIDEs

- Building on creating the NIDE identification document and NIDE analysis Framework document, create an interface to serve as a data source for external tools or additional analysis.

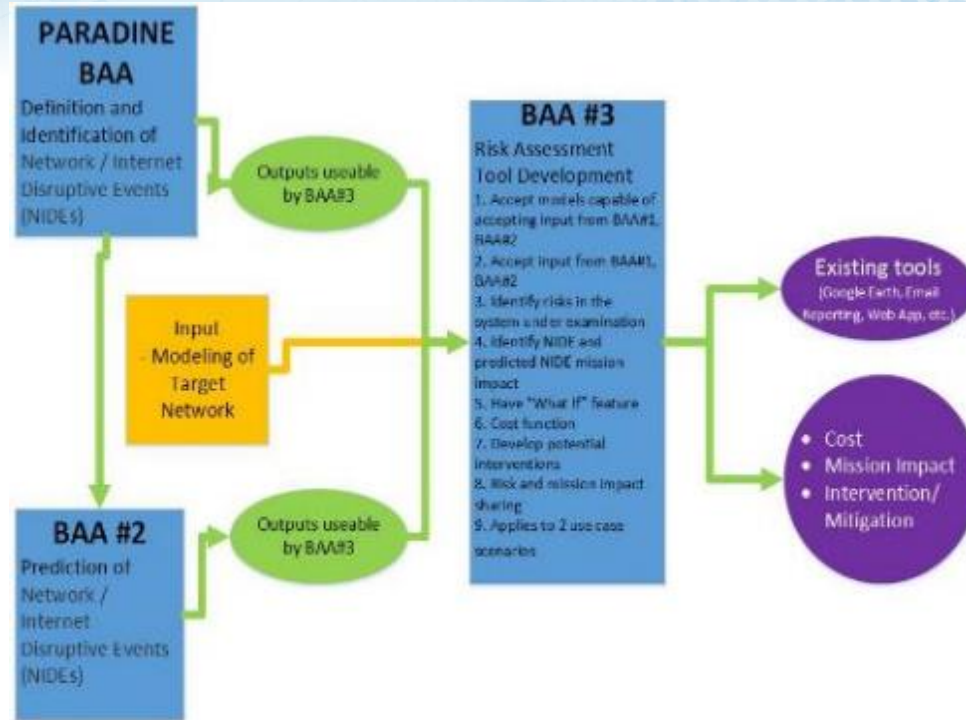
TTA 2: Attribution of NIDEs

This TTA leverages the techniques in TTA 1 to identify NIDEs and develop a framework to attribute NIDEs

- **NIDE attribution methodology**
 - Develop a methodology for attributing NIDEs including a framework to capture the confidence in the attributions. Root cause analysis is a desired outcome.
- **Develop a methodology to validate NIDE attributions**
 - The validation process will identify the data sources used and provide a detailed analysis of how close the NIDEs matched the observed NIDE attributions.
- **API for the communication, identification, attribution and reporting of NIDEs**
 - Building on the NIDE reporting methodology and associated NIDE identification and attribution validation, the third goal of TTA 2 is to create an interface that can provide data to external tools for further assessment

Application of Network Measurement Science

Predict, Assess Risk, Identify (and Mitigate) Disruptive Internet-scale Network Events (PARIDINE)



- TTA 1
 - Definitions
 - Algorithms
 - Operational Reporting

- TTA 2
 - Attribution
- Follow on BAAs
 - Prediction & Attribution
 - Risk Assessment & Attribution



Homeland Security

Science and Technology