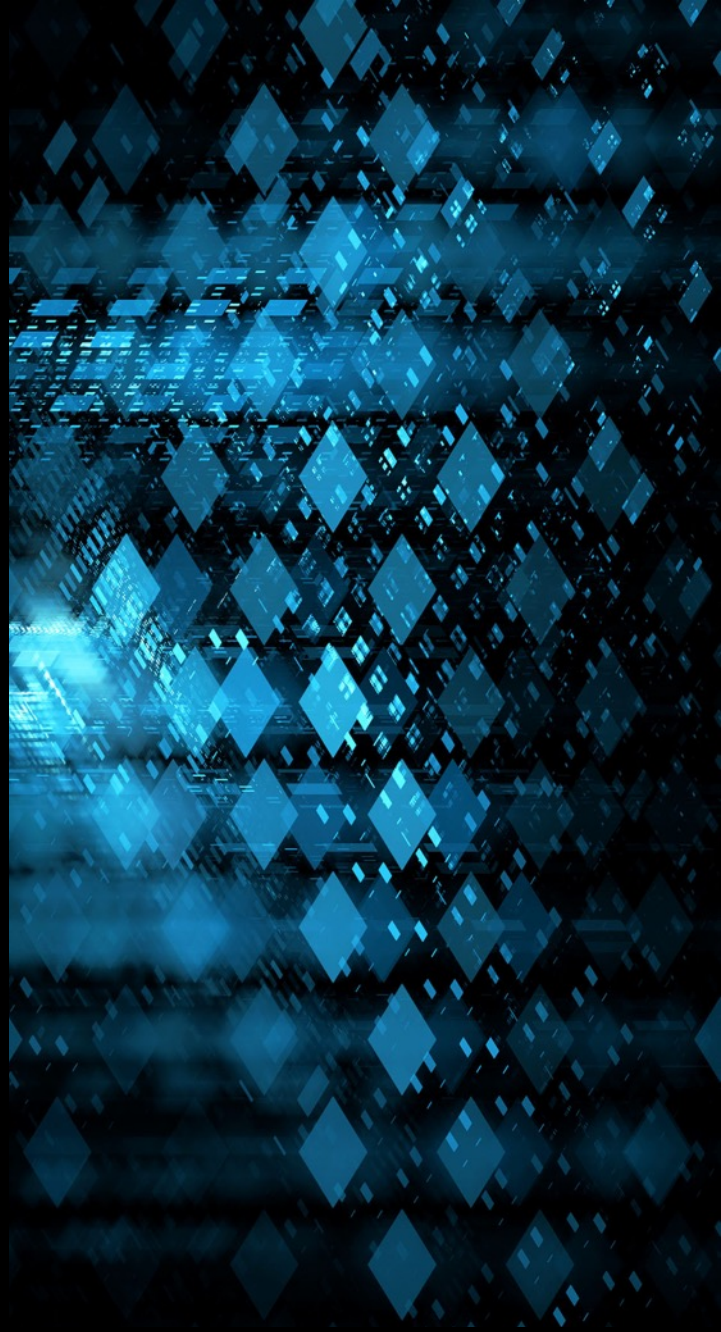
SEI Overview for 24th AF

Dr. Jeff Boleng
Chief Technology Officer (Acting) and Deputy CTO

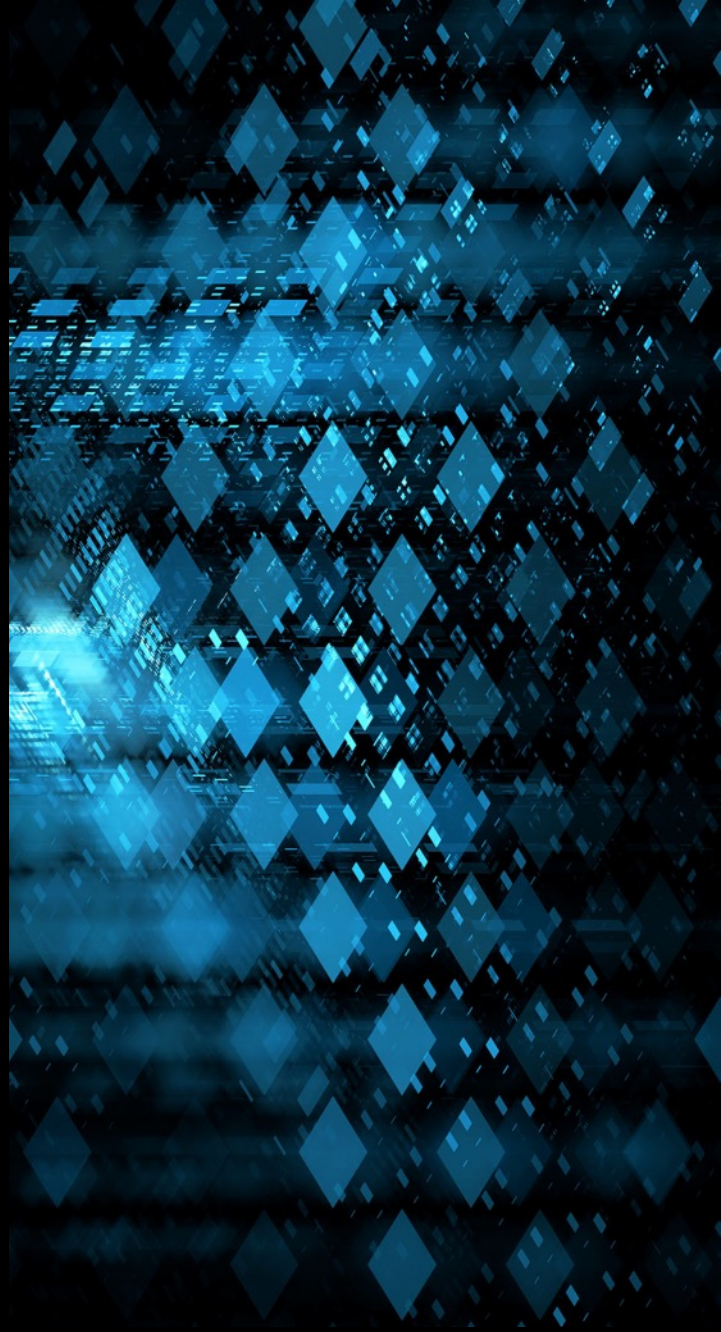


SEI Introduction and Overview

DoD Software Landscape

SEI Research Investment

CERT Introduction and capabilities



Vital stats:

Founded in 1984 at CMU as one of DoD's three R&D laboratory FFRDCs

~615 employees (ft + pt), with about 70% engaged in technical work

CERT cybersecurity program started 1988

Pittsburgh, DC, LA

About $145M funding [~$23M DoD Line]

Our Leadership

Paul D. Nielsen
Director and CEO

Robert Behler
Deputy
Director and
COO

Jeff Boleng
Acting CTO

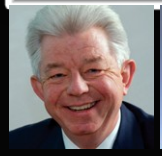
CERT Division

Bill Wilson
Acting Director

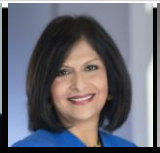
Greg Shannon
Chief Scientist

Roman
Danyliw
Chief Engineer

Software Solutions Division



John Bramer
Acting Director



Anita Carleton
Deputy Director

David Zubrow
Chief Scientist
(Acting)

Emerging Technology Center

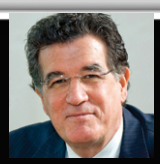
Matthew E. Gaston
Director

Eric Werner
Deputy Director

Chief Strategy Officer

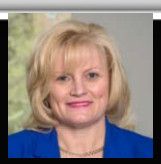
Mary Catherine Ward

CFO



Peter Menniti

General Counsel



Sandra Brown

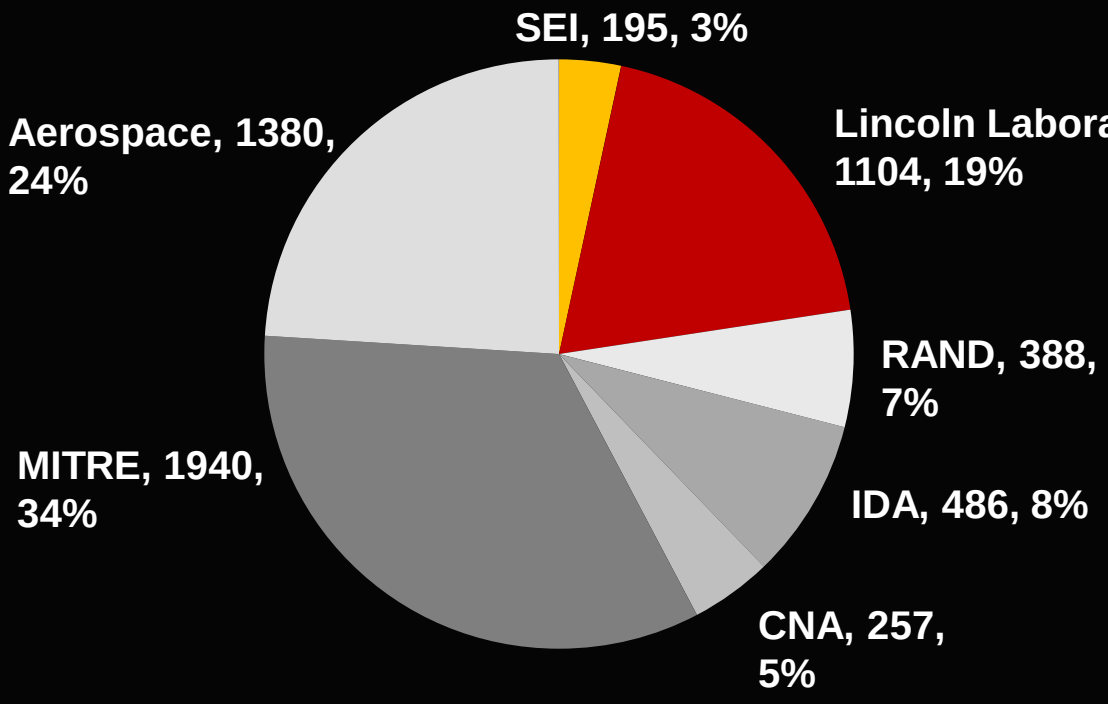
CIO

David Thompson

Chief of Staff

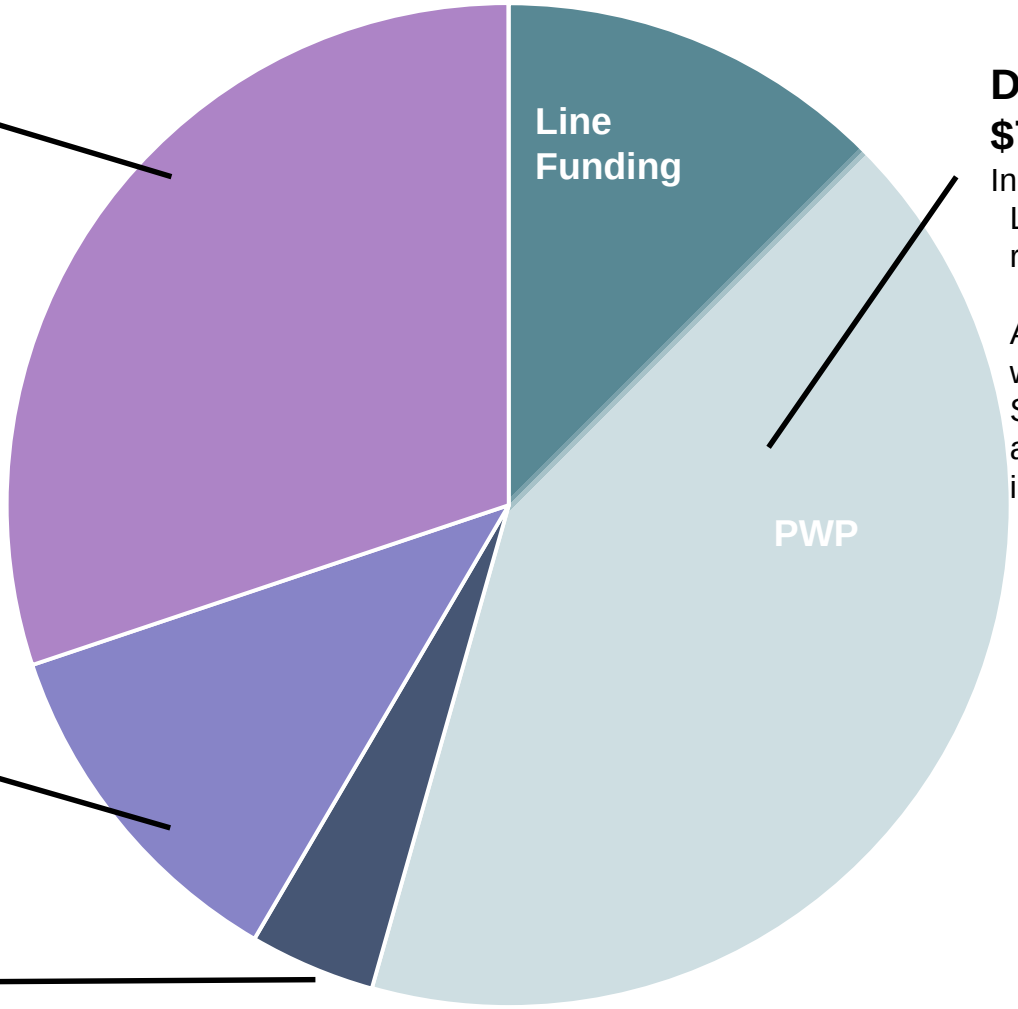
John Bramer

FY17 DoD FFRDC STE: initial allocations (total: 5750)



The SEI is the only FFRDC charged to improve the state of the art and practice of software engineering

Defense and national security: >80% of our funding



DHS ($43.9M)

Other Federal Not DHS ($16.7M)
Including
- USPS
- DoE
- HHS
- Secret Service
- Dept. of State
- Dept. of Treasury
- Dept. of Transportation
- Dept. of Justice

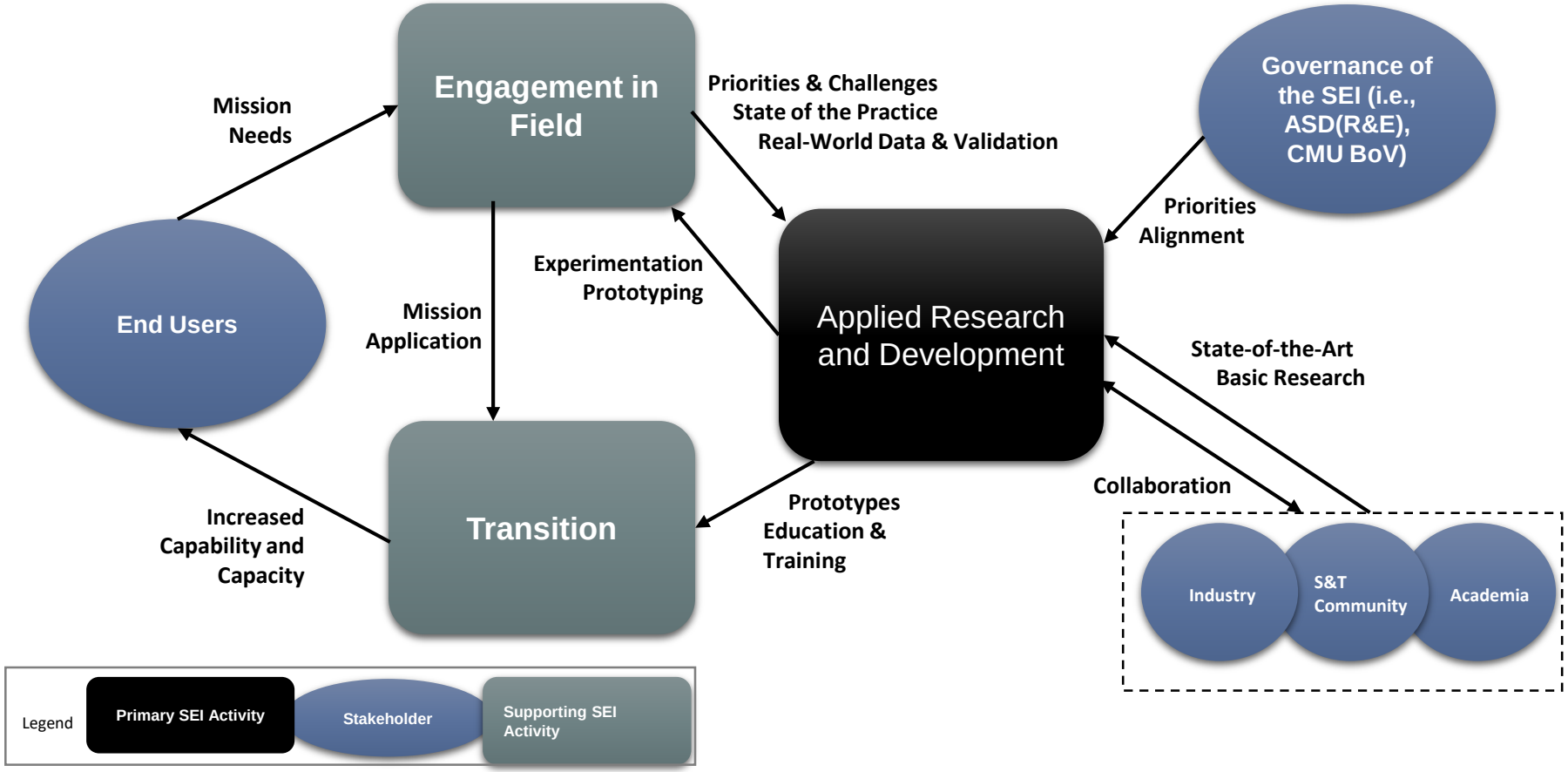
Non-Federal ($5.9M)
Including
- State of PA
- PNC Bank
- PPG Industries

DoD (ceiling, $79.4M)
Including
- Line-funded research

Approx. 150 project work plans with Service branches and agencies, including
- Air Force
- Army
- Navy and Marine Corps
- USCYBERCOM
- SOCOM
- NRO
- DARPA
- Missile Defense Agency
- NSA
- DC3

FY16 funding

SEI Execution Model



CMU SEI Solutions

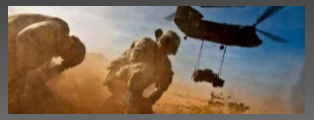
Enduring

Software Engineering & Information Assurance

Enable high quality, secure software-based systems in a predictable, affordable manner

Cyber Security

Develop improved systems, repeatable practices, and capable personnel to enable cyber missions



System Verification & Validation

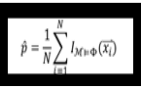
Enhance confidence in the systems engineering lifecycle with evidence-based methods and tools

Make software less costly and more resilient and mission capable by…

ruthlessly automating all aspects of design, development, integration, testing, deployment, operations, defense, and sustainment of software systems

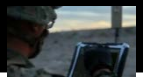
Emerging

Data Modeling & Analytics: Develop and apply mathematically rigorous data collection, analysis, and visualization techniques



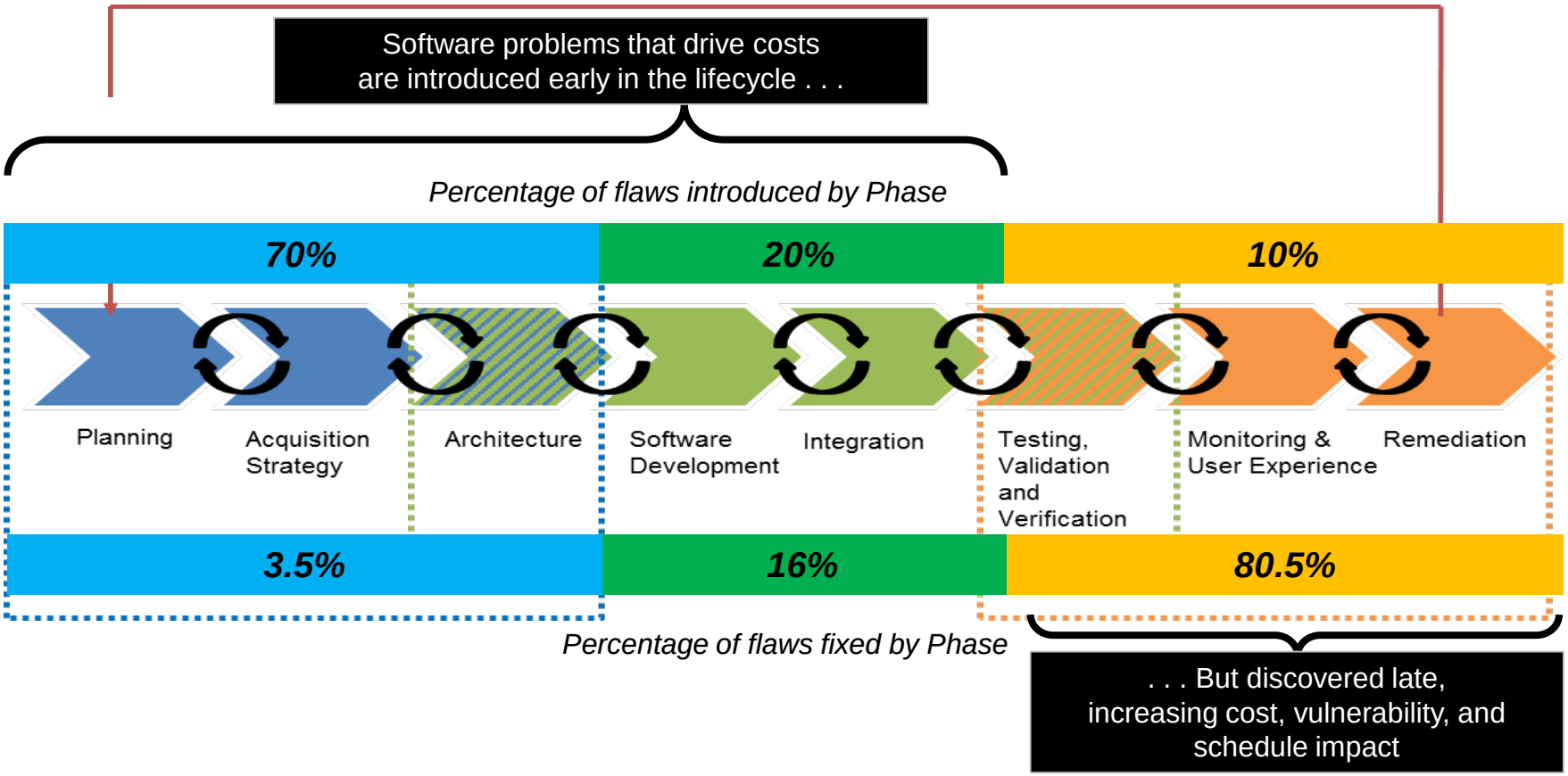
C4ISR Mission Assurance: Enable timely decisions that account for risk metrics personnel

Autonomy & Counter-Autonomy: Develop evidence that indicates the trustworthiness, dependencies, & vulnerabilities of autonomous systems



Human-Machine Interactions: Invent, assess, improve comprehensible, safe, and trustworthy technologies for humans to use and team with machines

Finding and Fixing Problems Late (rework) Drives Costs



Software Vulnerabilities put DoD Missions at Risk

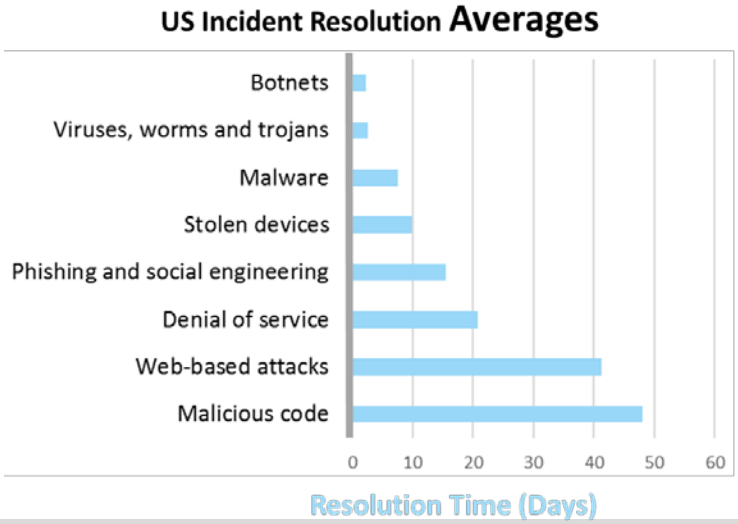
Latent Vulnerabilities

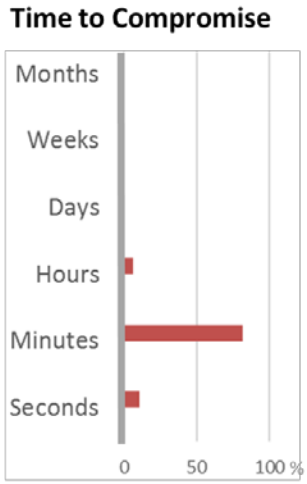
A 10M LOC Weapons Platform written in C will be delivered with 280 – 1,400 exploitable vulnerabilities

- 1 year after operation, 55% of these vulnerabilities will be present
- In sustainment new vulnerabilities will be introduced

Quality Data: *Capers Jones, NamCook Analytics, 2012*
Vulnerability Data: *SEI, Predicting Cybersecurity Using Quality Data, 2015 IEEE International Symposium on Technologies for Homeland Security*

Cyber Operations Response Lags



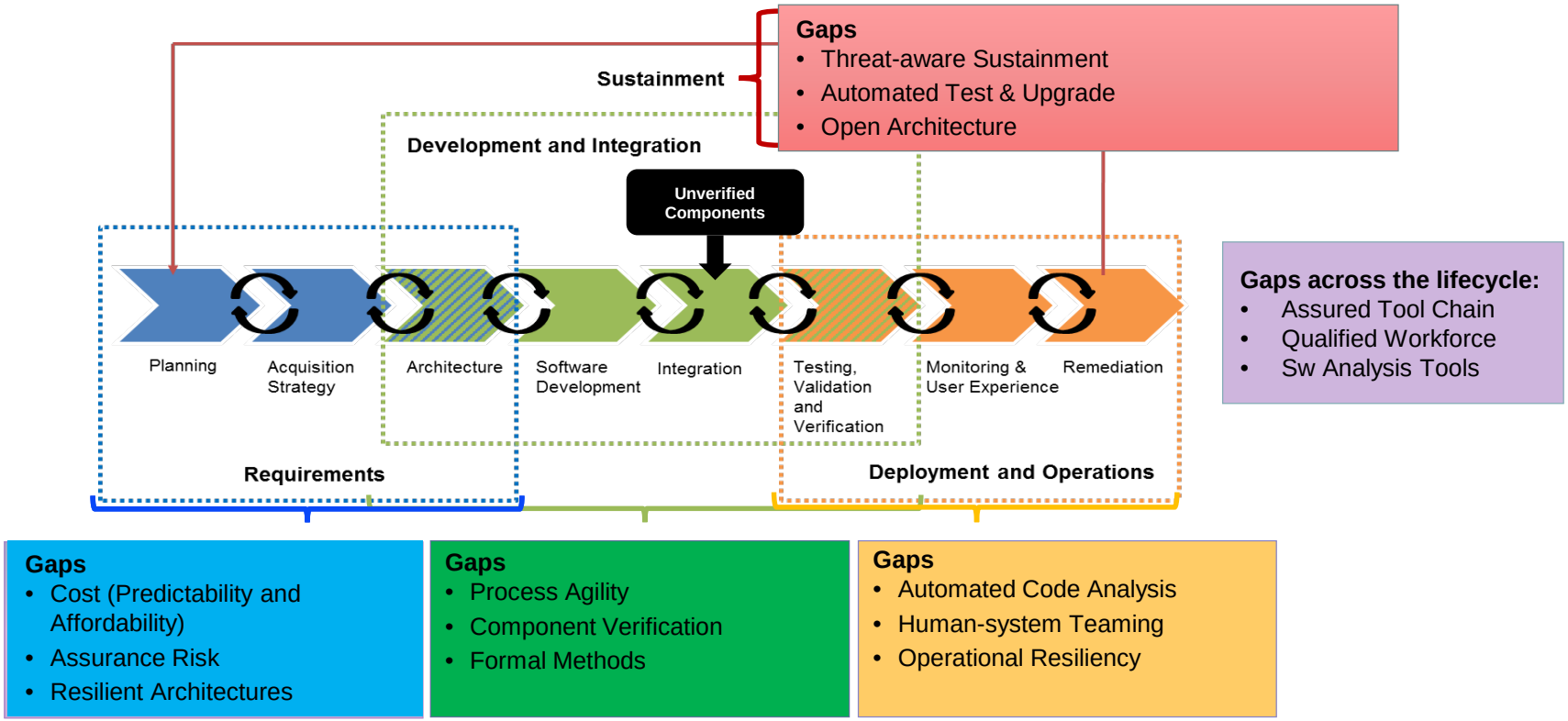


< 1 hour is the execution time of the vast majority (86%) of adversary offensive cyber maneuvers

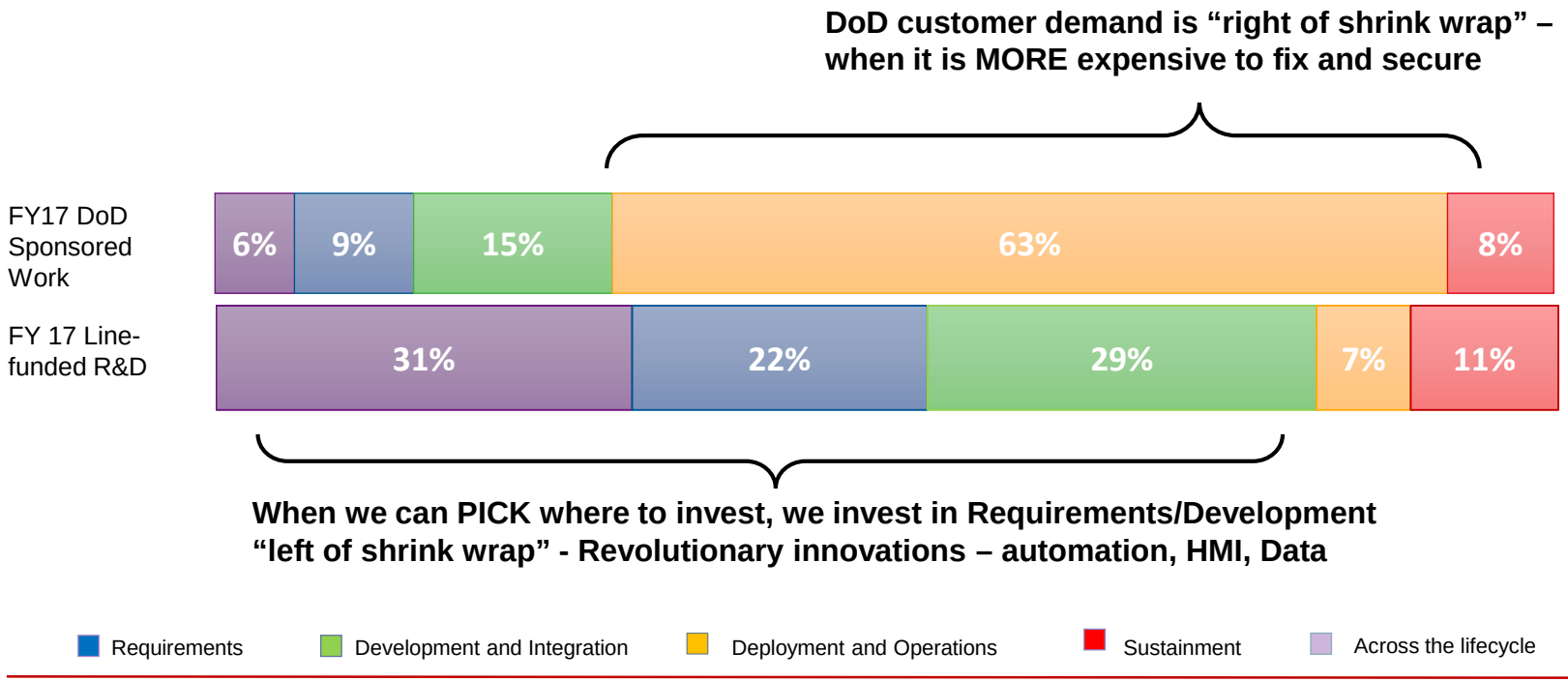
4 – 47 days is the average resolution time for defensive response and mitigation

Incident Resolution Data: *Ponemon Institute and HP Enterprise Security, 2015.*
Compromise Time Date: *Verizon Breach Report 2016*

Challenges Result from DoD Technology Gaps in the Software Lifecycle



In Software, Where You Invest to Address Gaps Determines Your "Bang for the Buck"



Our technical work (R&D and sponsored engagements)

- aims to introduce solutions earlier in the system/software lifecycle, where they can have the best impact
- aligns with DoD priorities expressed in Reliance 21 CoIs and ASD(R&E) guidance
- closes the loop with 'research-to-practice' and 'practice-to-research' activities across the lifecycle

Software delivers needed capabilities

- Limitless functionality
- Autonomy
- Flexibility and extensibility
- Interconnectivity
- Interoperability
- Affordable sustainment/evolution

CERT

Anticipating and solving the Nation's cybersecurity challenges

Enabling

Acquirers & Developers

Operators & Analysts

Decision Makers

Acquirers & Developers

Operators & Analysts

Decision Makers

Security-Aware Acquisition

Secure Development

System and Platform Evaluation

Threat-Aware Sustainment

Enterprise Risk

Network Situational Awareness

Cyber Intelligence

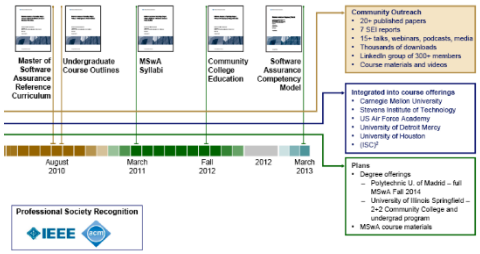
Digital Forensics

Insider Threat

Cyber Operator Development

Cyber Center Development

Security-Aware Acquisition



COCOMO® II

Addressing vulnerabilities and planning for threats earlier or more effectively in the lifecycle

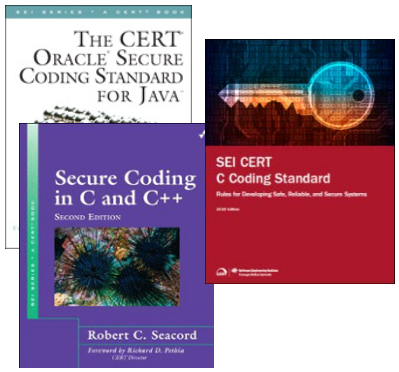
Current

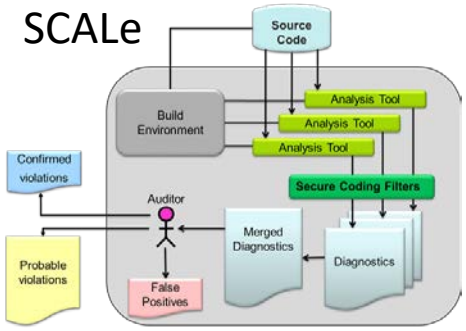
- Improving security requirements elicitation
- Operationally informed threat modeling
- Development-time evidence useful for accreditation
- Refining cost estimation of security controls
- Recommended contract language for measurable performance
- Assessing and predicting software assurance capabilities

Future

- Reusable secure architecture patterns

Secure Development





CERT Secure Coding Professional Certificates

Assuring and assessing platforms through the analysis of source code

Current

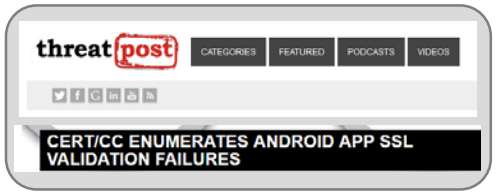
- Language-specific coding standards with automated enforcement
- Composition of static analysis capabilities
- Automated domain-specific code rewriting
- Architecture recovery
- Program correctness through model-checking
- Integrating security into Agile and DevOps

Future

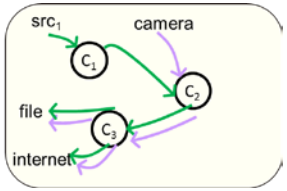
- Coverage of additional languages
- Comprehensive automated source code rewriting

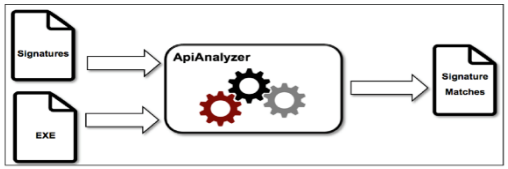
System and Platform Evaluation

Basic Fuzzing Framework
Failure Observation Engine



DidFail





Assessing software, devices, systems and platforms of unknown design or providence

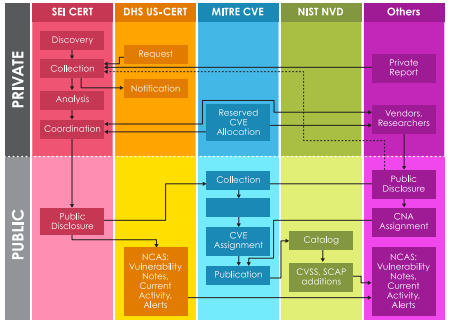
Current

- Repeatable approaches to find classes of vulnerabilities
- Focused analysis of features, behaviors, attack surface and implementation
- Automated characterization of capabilities or functionality
- Characterize the relationships between defects and vulnerabilities

Future

- Automated PoC exploit generation

Threat-Aware Sustainment



Reducing the window of exposure from known vulnerabilities in fielded systems

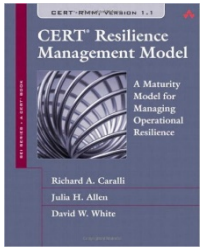
Current

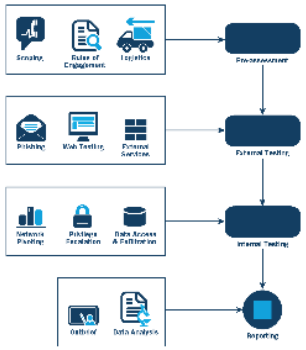
- Vulnerability coordination
- Timely watch-and-warning of new vulnerabilities and recommended mitigations
- Identifying systemic problems and emerging trends
- Guidance on establishing and operating a Product Computer Security Incident Response Team (PCSIRT)

Future

- Application and refinement of existing methodologies to new software ecosystems

Enterprise Risk





CSP FLIPBOOK

Carnegie Mellon University CIO Institute
Chief Information Officer Institute

Measurable practices and frameworks that enable an organization to measure and mitigate risk

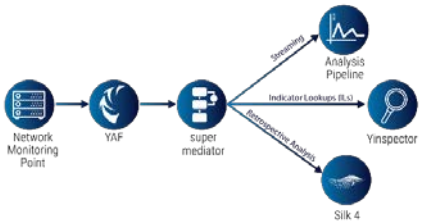
Current

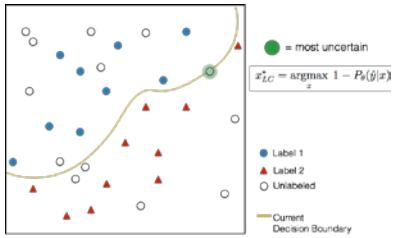
- Guidance on industry and government compliance and commonly-accepted practices
- Assessment approaches to identify capabilities and maturity
- Predicting security posture through practice and process evaluations, risk assessments and technical control data
- Economic models to prioritize investments and quantify their effectiveness

Future

- Cyber Maturity Model

Network Situational Awareness





Reasoning about the cyber terrain in context of the mission

Current

- Sensors that maintain visibility into the evolving network and platform technologies
- Analytical techniques that synthesize organizational, grey-space and cyber intelligence data to:
  - Characterize assets at risk
  - Measure scope and scale of adversary activity
  - Prioritize response to threat data
  - Resource planning and provisioning

Future

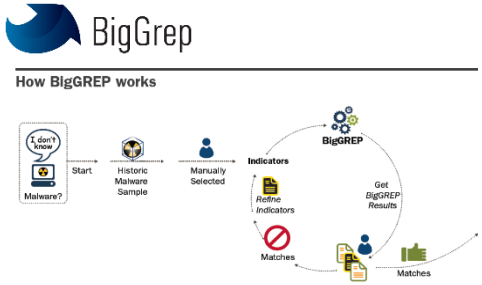
- Improved insight into the cyber-dependencies
- Cyber affordances

Cyber Intelligence

Pharos Framework

+

ROSE@LLNL



The Cyber Intelligence Research Consortium

Emerging Technology Center

Characterizing the behavior, capabilities and properties of adversary cyber tools and actors

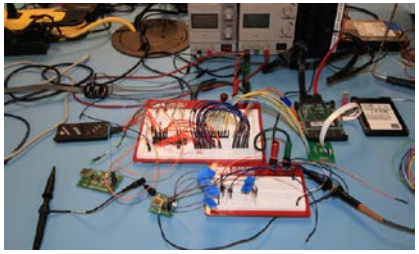
Current

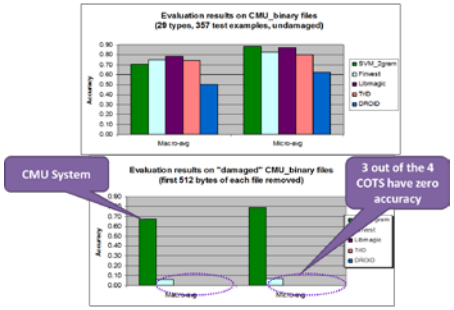
- Automation for reverse engineering
  - Deobfuscation and unpacking
  - Code comprehension
  - Dynamic analysis environments
- Creating indicators and identifiers for the detection and attribution of actors and malware families
- Trending emerging capabilities, tactics and targets
- Enabling threat modeling for system design

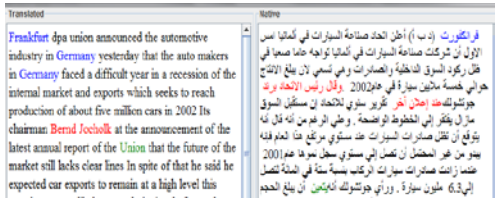
Future

- Automated code comprehension
- Automated malware classification

Digital Forensics







Enabling incident response and analysis activities as the technology and adversary evolves

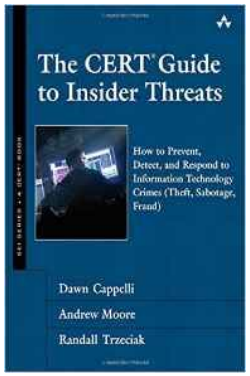
Current

- Forensic recovery techniques for data on emerging mediums
- Models to evaluate the efficacy of cyber effects and mitigations

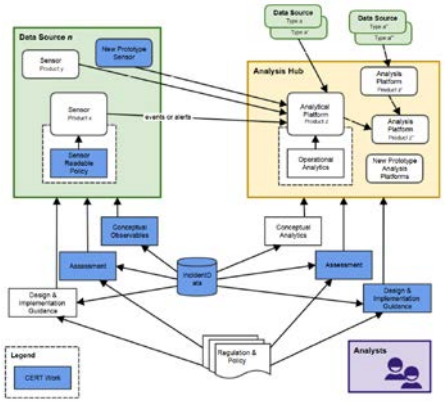
Future

- Increased capabilities in the analysis of:
  - Crypto-currencies and related infrastructure
  - Mobile application ecosystem

Insider Threat



CERT Insider Threat Certificates and Training



Detecting and mitigating the impact of and reducing the likelihood of insider threat

Current

- Indicators to use in end-point and hub analytics
  - Reactive – user activity monitoring
  - Proactive – behavior modelling
  - Preventative – aids and incentives
- Guidance on establishing and operating insider threat programs compliant with the EO 13587 and NISPOM

Future

- National Insider Threat Research Development Testing and Evaluation Facility

Cyber Operator Development

Growing and maintaining a cyber workforce at sufficient scale with a known readiness

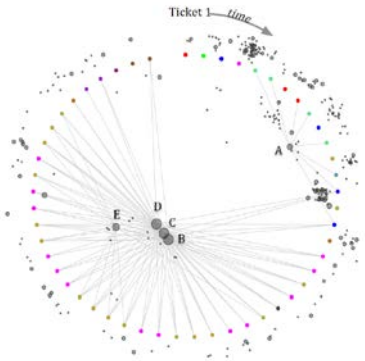
Current

- Designing and executing of Joint and Service-scale exercises
- Representative cyber environments for modelling and simulation
- Verifying role readiness of cyber operator
- Federated architecture to link cyber and kinetic simulators

Future

- Automated assessment of operators
- Improved trainee engagement through gamification

Cyber Center Development



Measurable and repeatable practices to improve and align operational security organizations

Current

- Models to guide investments and organization processes based on emerging threats, technology landscape and mission priorities
- Analytics of workflow data
- Automated information sharing
- International capability building

Future

- Improved capacity and capability models

Transitioning Capability from the Lab to the Field

Analysis **Prototypes** **Training**

www.cert.org

Jeff Boleng
Email: jlboleng@sei.cmu.edu
Telephone: +1 412-268-9595

U.S. Mail
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612 USA

Website
www.sei.cmu.edu/contact.cfm

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM17-0566

Cybersecurity and Wargaming

Automated Malware and Cyber Weapon Software Analysis

• DoD/NSA network defense

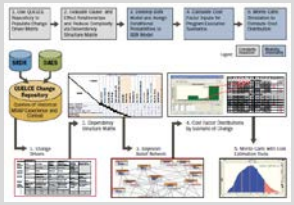
Results: Tools reduce analysis activities from hours to seconds and accelerate capability for analysts to keep pace with adversarial techniques**.** Ongoing collaboration with Lawrence Livermore National Lab (DoE).

Cyber Flag/Guard/Knight Exercises & Wargaming

• USCYBERCOM: Cyber Flag/Guard/Knight

Results: Successful validation of dozens of service Cyber Protection Teams (CPTs) due to infrastructure, scenarios, and exercises created by SEI. Over past 12 months, 2400+ cyber operators trained across USCYBERCOM, DISA, and Services

Data Modeling and Analytics



Quantifying the acquisition costs of software-enabled weapon systems

• Joint Space Program

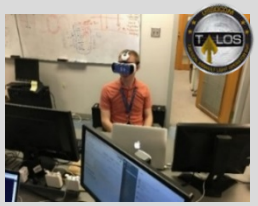
Results: Retrospective analysis found that 90% of estimated $60 million in significant unplanned costs could likely have been avoided.

Exploiting new hardware for important software algorithms

- Graph algorithms - collaboration with Indiana University and MIT Lincoln Laboratory.

Results: Standardizing ways of expressing and solving graph problems (using linear algebra methods) will reduce costs for DoD applications requiring high performance computational infrastructure available at reasonable costs

Prototyping & DoD/Software Expertise



Software Prototyping, Architecture and Design

• SOCOM TALOS (Tactical Assault Light Operator Suit)

Results: Early prototyping enables shorter time to operation, faster validation of innovative technologies, integration risk avoidance, and empirical evidence for decision support.

Analyzing and rectifying mission-critical software problems

• PMS-500 (DDG-1000) steering control

Results: Resolved steering system software issues by performing software analysis, reviews, and integration. Directly contributed to ship successfully meeting timeline for initial sea trials.

Autonomy and Counter-Autonomy

Definition and Approach	Examples of Technical Enablers
Build and understand the evidence that autonomous systems are trustworthy (and and the nature of their dependencies and vulnerabilities)	Pattern recognition and machine learning (ML), curated data sets, transfer learning

- Variable autonomy – selectable levels of delegation
- Software algorithms/frameworks for multi-agent autonomy and automation
- Cyber/EW effects as enablers for counter- autonomy
- CMU NREC collaboration (developers of CHIMP and Crusher; winners of DARPA Urban Challenge) on man-machine trust and testing of autonomous robots
- Propagating learning to a distributed system

PWP Work:

- SOCOM Special Operations Research, Development and Acquisition Center (SORDAC) – architecture, virtualization, and micro services in support of TALOS
- DHS S&T – moving target defense (cyber)
- DISA Spectrum – spectrum allocation in the context of Dynamic Spectrum Allocation/Management (DSA/DSM)

Line Funded Research:

- Effecting Large-scale Adaptive Swarms through Intelligent Collaboration
- Automated Decompilation of Malware
- Distributed Autonomous Real-time Verification Framework
- Automated Code Repair (also in Software Assurance)

Software for assuring missions using autonomous systems and ensembles

Formal description (DMPL language) of multiple cooperating autonomous agents.

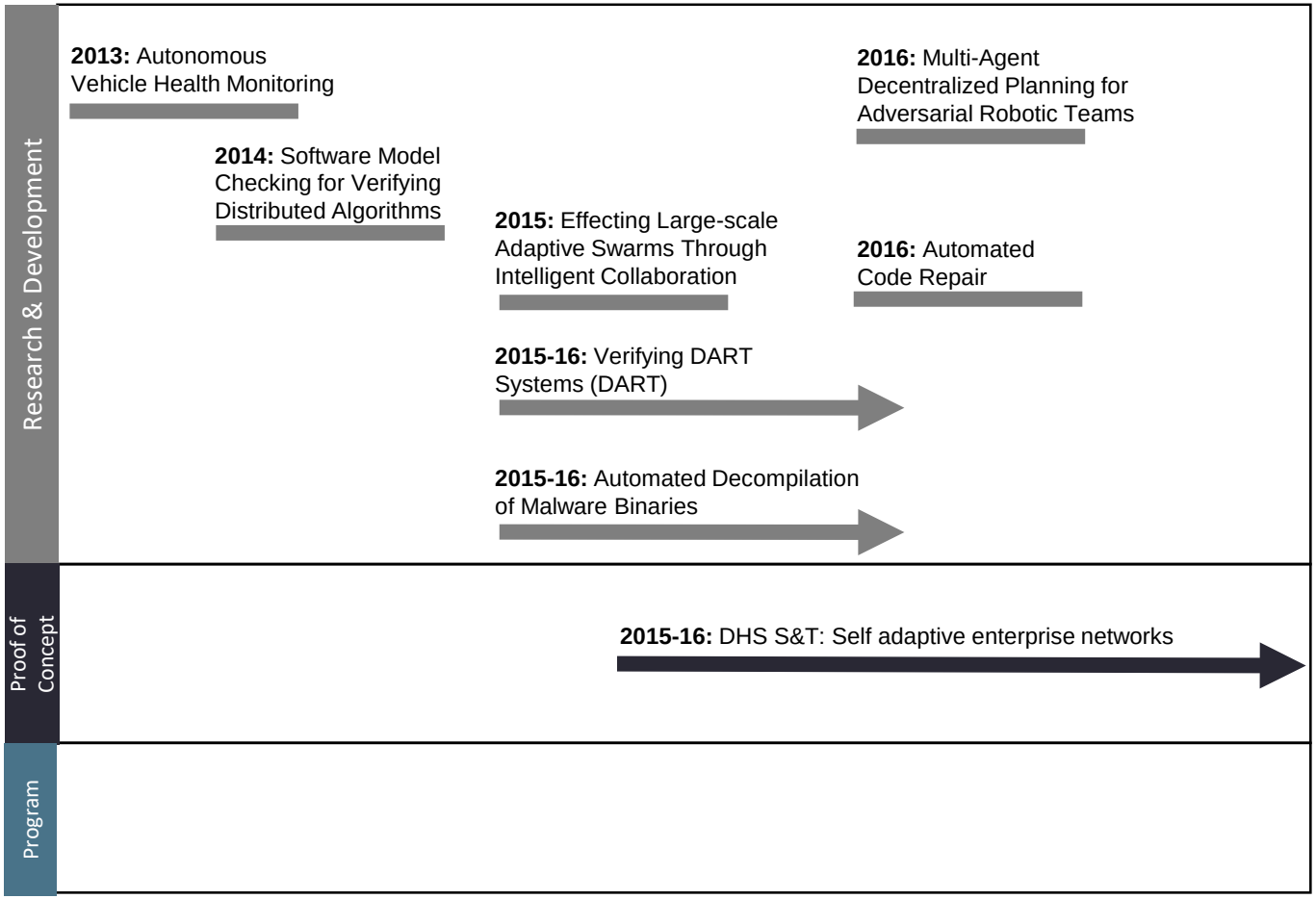
Application of model checking for validating autonomous behavior

SEI-developed open-source middleware to support operation of validated distributed autonomous agents

Security and vulnerability testing of connected vehicles

Developing tools and techniques for assessing security of network-centric vehicles. Recent analysis of remotely accessible “plug-in” onboard diagnostics (that can physically effect or track vehicles) used by USAF logistics and maintenance program discovered security and configuration vulnerabilities.

Autonomy & Counter-Autonomy



Looking Ahead:

Predictability of autonomous system behaviors; autonomous systems conveying intent through actions

Extend connected vehicle vulnerability research to related areas in transportation

- Exploitation of autonomous functions in self-driving vehicles, ground robotics, unmanned aerial systems (UAS)

Designed-in techniques for limiting the manipulation of algorithms during training and at run-time

- Use of redundancy and resiliency to limit the opportunity for data manipulation attacks and the impact of attacks
- Detection of adversarial data manipulation activity and intent using indicators such as drift and observed unusual patterns
- Scalable and *secure* operating systems for autonomous systems and ensembles of autonomous systems

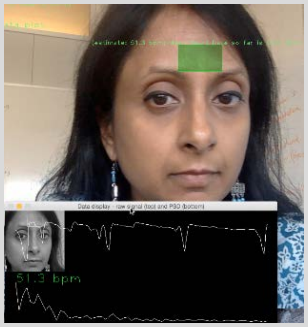
Human-Machine Interactions

Definition and Approach	Examples of Technical Enablers
Assess and improve comprehensible, safe, and trustworthy human-machine interactions at scale	Trust-enhancing planning, self-explanation, multi-agent ensembles ('swarm' controls)

- systems with context-awareness that can "explain" how and why they behave as they do
- Methods and algorithms for machines to assess the condition of human operators or team members as input to behavior planning
- Context-aware user interfaces to reduce cognitive load
- Understanding and modeling the drivers and behaviors of users that represent potential insider threats

PWP Work:
- Insider Threat (DARPA, Army G2, NETCOM, Navy SPAWAR, USAF, USMC, DHS I&A, NGA USAF)

Line Funded research:
- Cyber Security via Signaling Games
- Insider Treat Mitigation
- Human-Computer Decision Systems for Cybersecurity
- Why did the robot do that?
- Data Visualization for Large-Scale Analytics
- Workplace Violence – IT Sabotage



Allowing machines to better understand human users

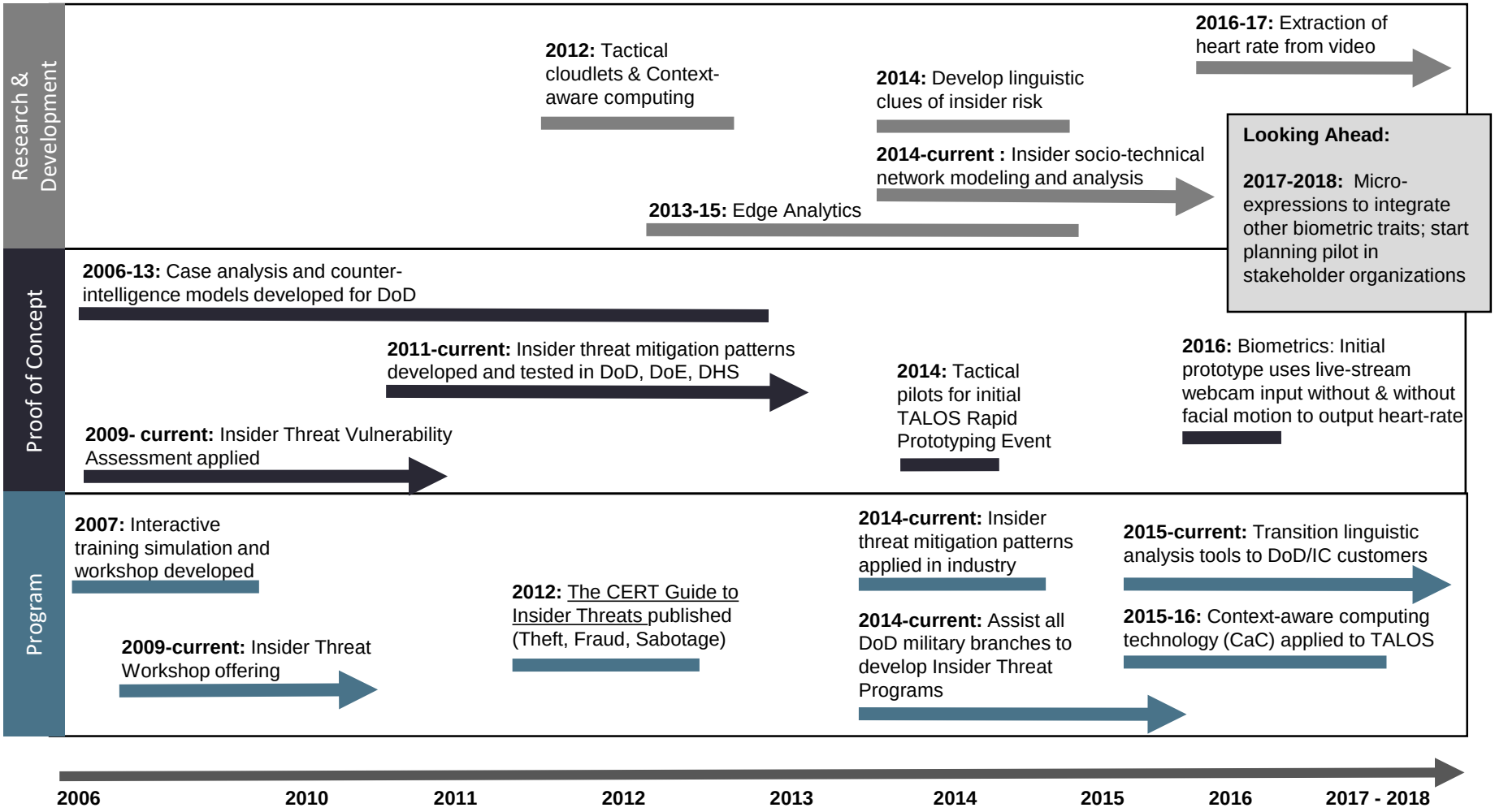
Prototype application that can extract heart rate in near real-time from video taken with commodity cameras.

Extracted heart rate in near real-time (~10-15 s) from both live-stream (standard webcam) and pre-recorded video of a non-stationary human's face.

Why did the robot do that? With semi-autonomy comes the need to make robots' actions "intelligible" (comprehensible, scrutable, transparent) to users

- Automatically generate explanations of robot actions and incorporate explanations into robot user interfaces
- Mathematical and algorithmic rules for translating popular sensing and planning algorithms into English explanations

Human-Machine Interactions



C4ISR Mission Assurance

Definition and Approach	Examples of Technical Enablers
Quantify and maximize the likelihood of mission success by enabling decisions to be made with the benefit of risk metrics in a timely fashion	Modeling mission components and failures, success metrics, courses of action

- Application of data analytics to C4ISR missions (e.g., image and speech processing, damage assessment) in web frameworks
- Dynamic Course of Action (CoA) recommendation systems
- Combine Bayesian Belief Networks (BBN) with Monte Carlo Simulation and Statistical Model Checking for predicting mission outcome success
- Architecture and implementation of mission analytics with selected DoD hardware/software environments and frameworks

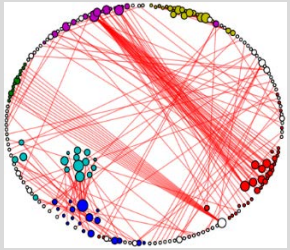
PWP Work:

- OSD – Decision Analytics (with other laboratories/FFRDCs)
- OSD DASD SE – software issues in DARPA QUES [Quickly Upgradeable Electronic Systems]
- DoD Joint Federated Assurance Center (JFAC) - new techniques in software test, vulnerability analysis, and malware

Line Funded Research:

- Benchmarks and datasets for evaluating big learning systems
- Applying IBM Watson Technology to Inform Mission Assurance
- Query Obfuscation of Open Source Intelligence

Graph Algorithms: Graph BLAS Consortium to develop portable high performance graph algorithms, including members from Intel, Center for Research in Exascale Technologies at Indiana University, and MIT Lincoln Laboratory



Graph showing editor conflict on the “Cyprus dispute” page, 2014

- Building benchmarks and datasets for evaluating big data learning systems
- Proposed standard for graph algorithm APIs on heterogeneous hardware

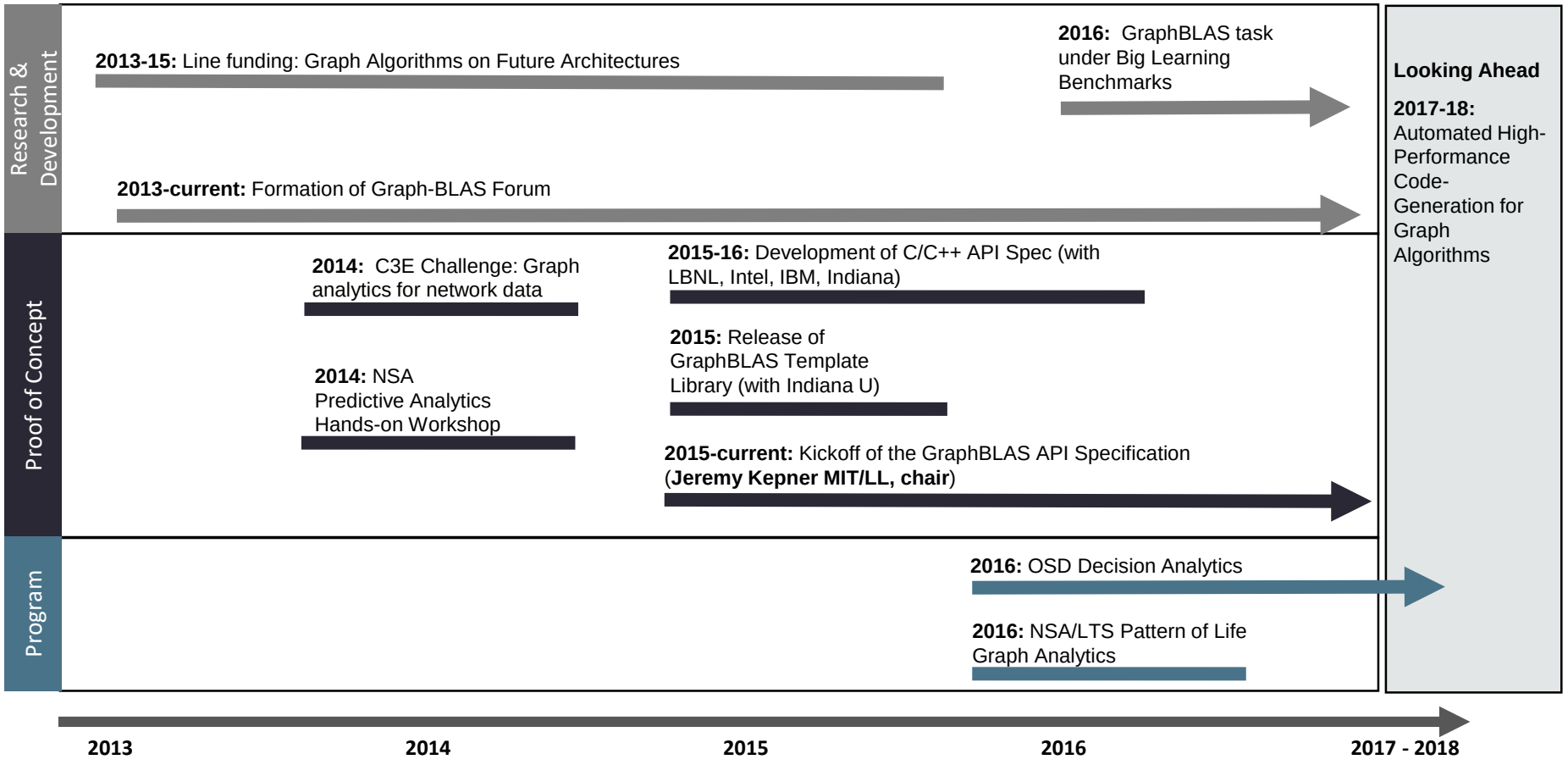
Statistical Model Checking: scaling model checking to large state spaces

$$\hat{p} = \frac{1}{N}\sum_{i=1}^{N} I_{\mathcal{M}\vDash\Phi}(\overrightarrow{x_i})$$

Future Direction: Run-time assurance for autonomous systems and autonomous system ensembles

Formal verification of monitors of system behavior that provide guarantees that systems will not enter undesirable state

C4ISR Mission Assurance



Data Modeling and Analytics

Definition and Approach	Examples of Technical Enablers
Develop and apply mathematically rigorous data collection, analysis, and visualization techniques	DoD program data analysis, natural language processing, ML, data sets

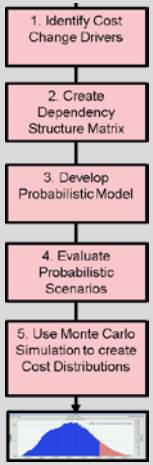
- Mathematically rigorous data collection, analysis and visualization techniques applied to problems of acquisition performance and operational decision aids
- Validate best practices at scale with evidence from DoD and non-DoD/industry simulated and live mission settings
- Improve predictions regarding cost, schedule, delivered capabilities and operational outcomes

PWP Work

- NSA/CSS NTOC – cyber intel research consortium (memberships), malware family and trend analysis
- NAVAIR AWL – evolution of model for F/A-18 advanced weapons lab sim

Line Funded research:

- Quantifying Uncertainty for Early Lifecycle Cost Estimation – statistical analysis of acquisition performance (QUELCE)
- Machine Learning for Big Data Systems Acquisition
- Enabling Evidence-Based Modernization (acquisition DA)
- Software Attributes Tradeoff Tool (w/systems engineering)
- Generalizing Supervised Latent Dirichlet Allocation (LDA) for Analyzing Open Source Intelligence Data

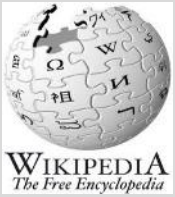


Prototype model for early lifecycle cost estimation (QUELCE)

Estimates using traditional methods fail to account for macro sources of uncertainty (Mission, CONOPS, Subcontractors, Open Source, Security, Assurance, etc…)

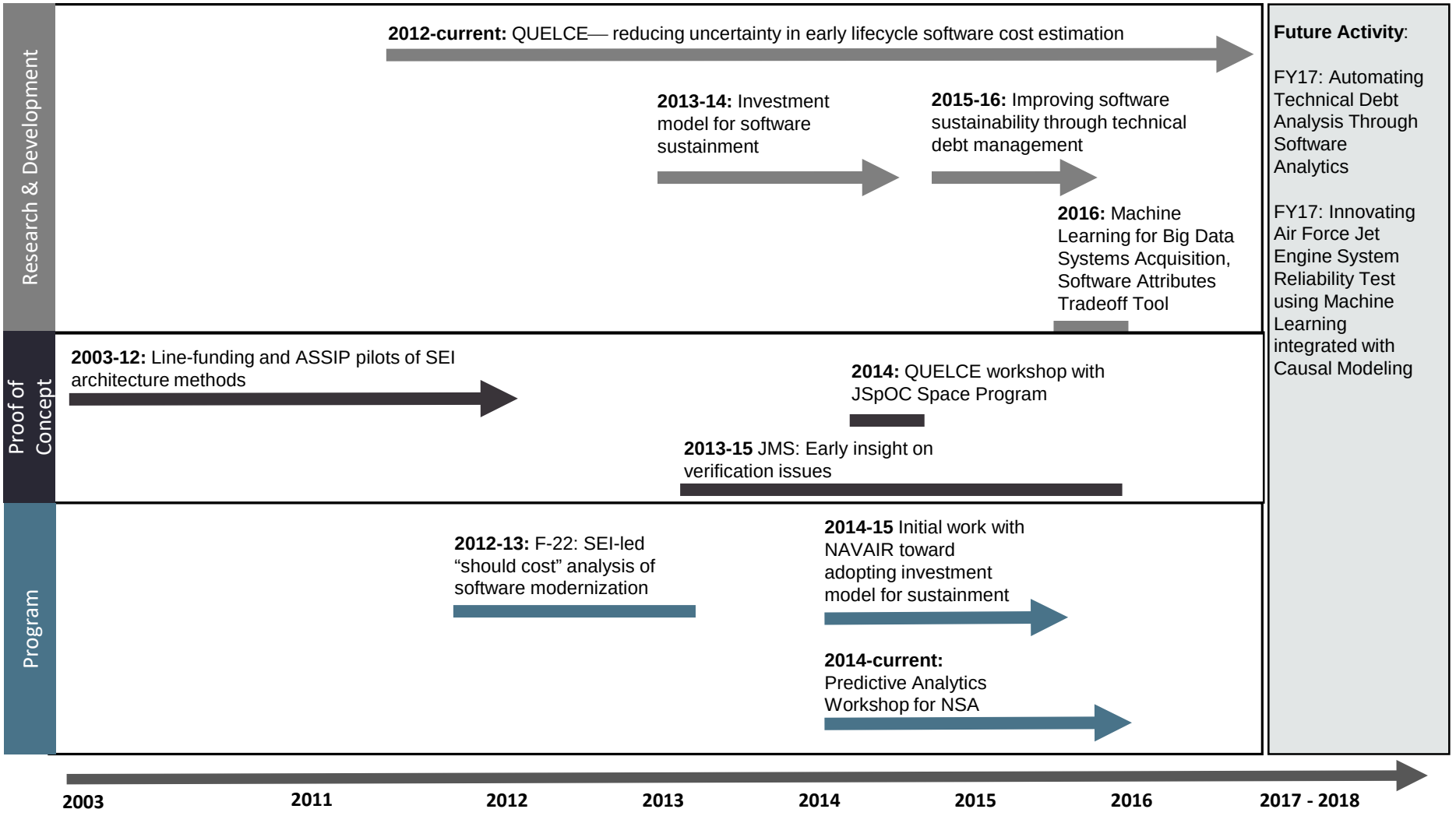
Results: For JSpOC Mission System: 50% of change drivers were not identified (at Milestone B) and 90% of unplanned costs could likely be avoided (retrospective analysis)

Predictive Analytics Workshop: Custom workshop for NSA to strengthen the design, development, and use of machine learning capabilities within mission organizations



- 1 week-long, in-person, hands-on workshop
- Presentations by research and industry experts
- Emphasis on hands-on experience with real data and real problems (Wikipedia and conflict detection)
- Analytics tools including: Python: scikit-learn, NLTK, matplotlib, iPython Notebook, Hadoop, Spark, Graph databases

Data Modeling and Analytics



ASSIP: the Army Strategic Software Improvement Program, a long-term effort focusing on acquisition programs, people, production and sustainment, and the institutionalization of continuous improvements. ASSIP funded SEI investigations into software architecture and systems-of-systems for the Army

Systems Verification and Validation

Definition and Approach	Examples of Technical Enablers
Build practical, mathematically grounded, and evidence-based methods and tools to enhance confidence in the entire systems engineering lifecycle	Model-based systems engineering, virtual prototyping, architecture and mission description languages

- Reduce rework/costs by preventing ambiguities and complexity in specifications, uncharacterized components, technical debt and conventional black-box testing for embedded software (e.g., IoT, DoD weapon systems)
- Develop tools for the generation of assurance/safety cases, testing protocols, and related software artifacts that can be verified at scale based on mathematical foundations via tools operating on requirements, assurance evidence, system models and software derived from un-assured supply chains

PWP work:

- AEGIS PEO IWS – work on conversion and restructuring from 32 to 64 bit environment
- NRO SE – architecture for ground segment
- PM Bradley – new software architecture and security issues
- USA PM CMDS – IFPC Incr1/2 counter UAS/OSA
- USA AMRDEC ADD JMR – Application of AADL for FVL

Line funded research:

- Parallel and Software Model Checking
- Effective Reduction of Avoidable Complexity in Embedded Systems
- Verifying Distributed Adaptive Real-Time (DART) Systems
- Incremental Lifecycle Assurance of Critical System Components
- Automated Assurance of Security Policy Enforcement
- Auto-Active Verification of Software with Timers and Clocks

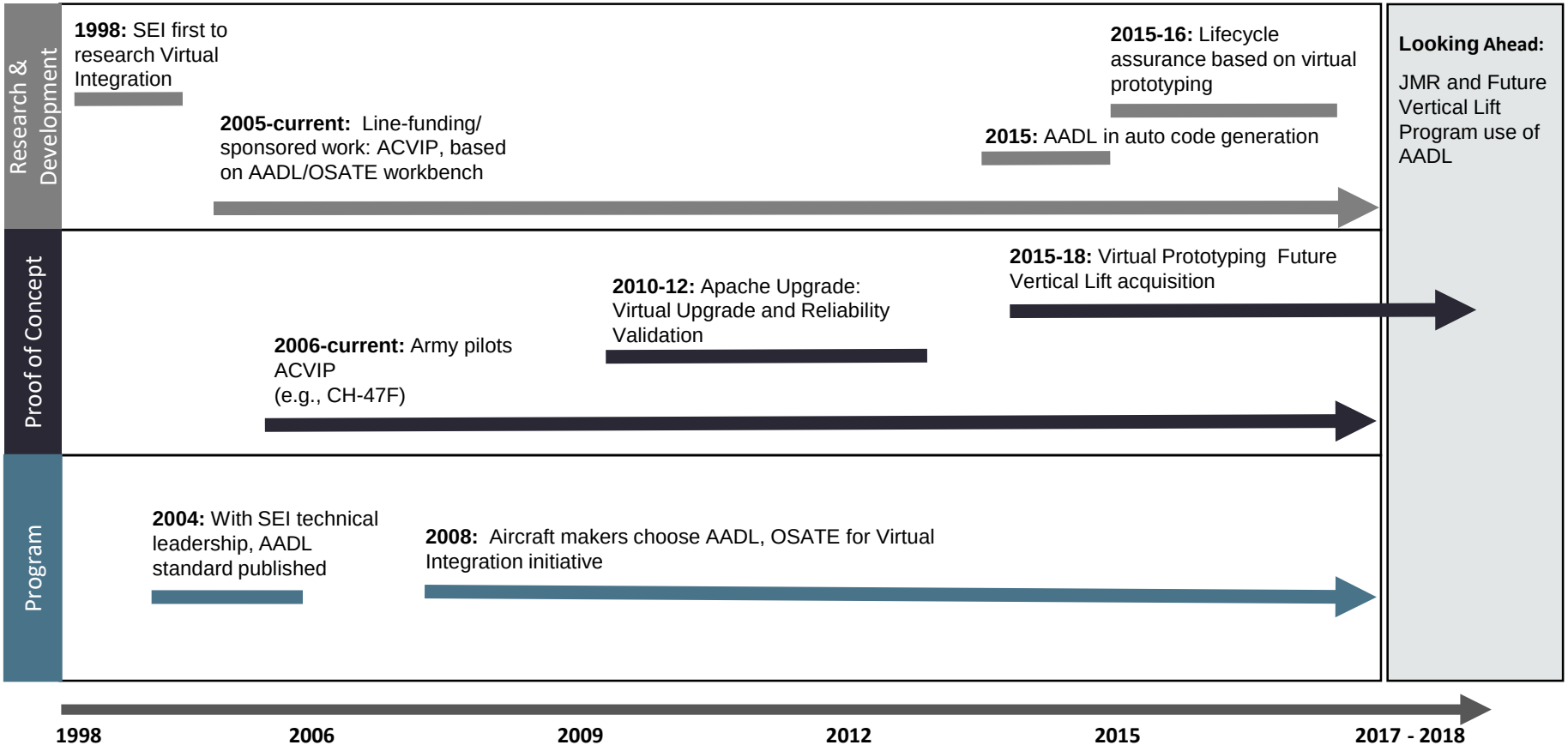
Virtual prototyping and integration: Architecture Analysis and Design Language (AADL) used in JMR TD Project

- Rapidly detected more than 85 potential integration issues in requirements phase that traditional approach missed
- Industry rework estimate: $100K per issue at integration → low-end saving estimate $8.5M
- Virtual Prototyping is now included in RFPs for FY2016-17 JMR projects

Software model checking and abstract interpretation for verification

- Award winning SeaHorn software verification framework (open source)
- Modular design separates verification and programming language semantics
- Supports varying levels of precision
- Simplifies the interface to other V&V tools using Horn clauses

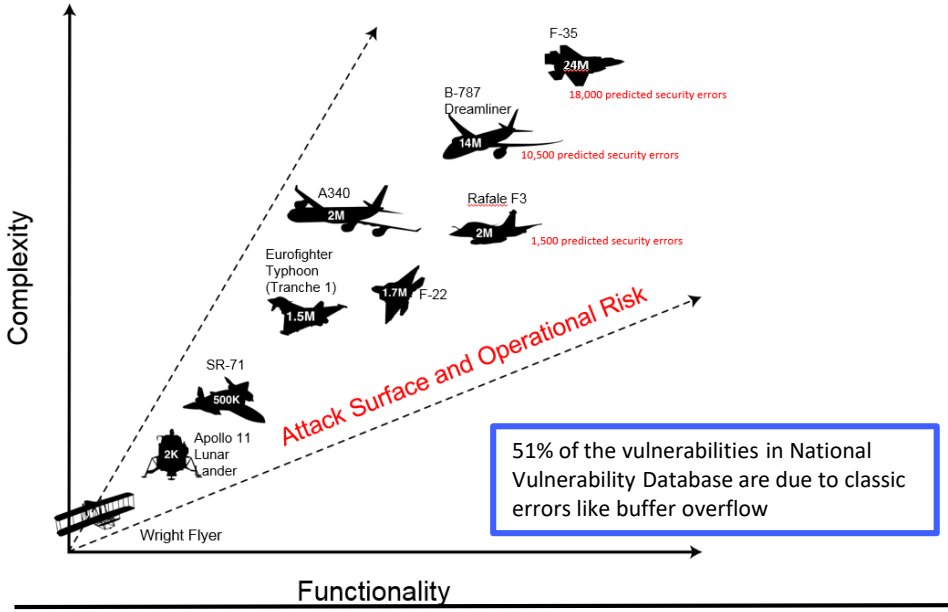
Systems Verification and Validation



AADL= Architecture Analysis & Design Language; OSATE = Open Source AADL Tool Environment; JMR = Joint Multi-Role Rotocraft

Software and Information Assurance

Definition and Approach	Examples of Technical Enablers
Reduce vulnerabilities in software prior to fielding/deployment and protect information, through mathematically grounded techniques and architectures	Code analysis, fuzz testing, automated software vulnerability discovery and exploit generation/testing

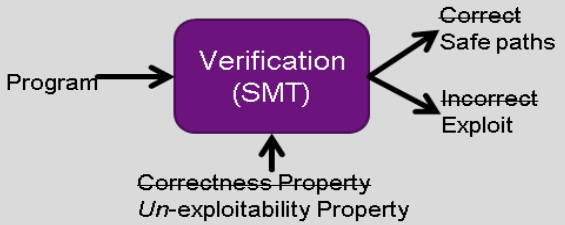


PWP Work:

- NSA/R2 – future R&D planning with Special Cyber Operations Research and Engineering (SCORE) program
- iARPA – help develop R&D focus areas across HPC/quantum/cyber
- Evaluations for DARPA TransApp, Bradley, Aegis, DDG1000, OMS, Redstone

Line Funded Research:

- Software analysis and attribution of Advanced Encryption Standard hardware
- Secure coding standards & generation
- Ease-of-use for security APIs and operational implications
- Sound vulnerability discovery
- Prioritizing vulnerabilities from static analysis



Automated vulnerability discovery in applications

- ForAllSecure Collaboration (start-up company)
- Use SMT solvers to determine variable assignments leading to particular paths
- Unsatisfiable predicate – constructive proof of path to vulnerability
- **Future:** Automated code repair

Secure Code Analysis Tool

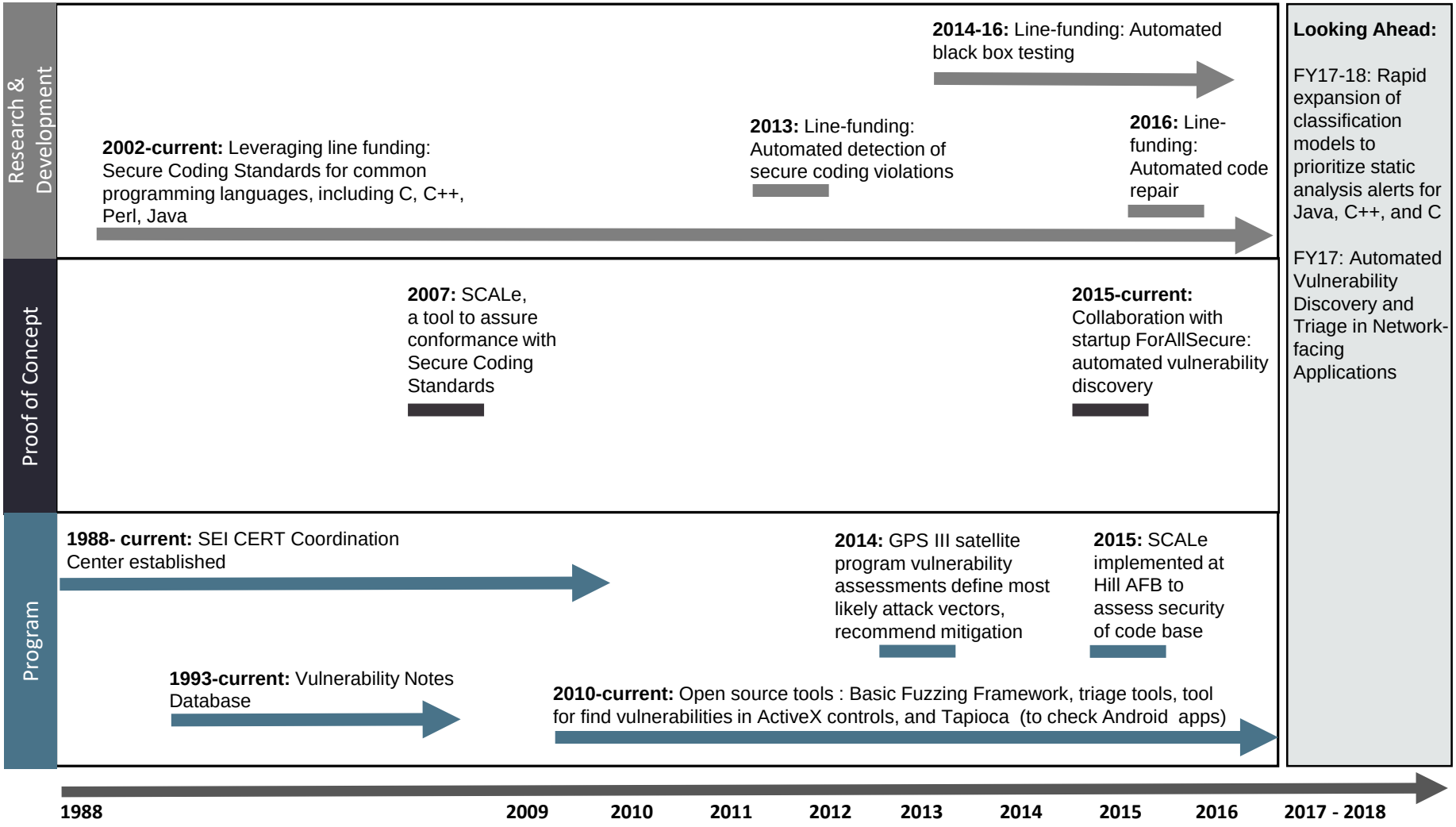
Source Code Analysis Laboratory (SCALe) **– ensemble static analysis**

Results: Hill AFB uses SCALe tool to analyze code for non-conformance to CERT Secure Coding standards

- Potential 1120 code defects at best-in-class density of 0.7/thousand lines of code
- $3.3 million potential rework cost saved with auto code repair ($30,000 per defect, if not fixed prior to operation)

Technology insertion discussions ongoing with ARDEC, NAVAIR, NAVSEA

Software and Information Assurance



Cyber Missions

Definition and Approach	Examples of Technical Enablers
Develop automated systems and capable personnel to improve operational cyber capabilities and outcomes	Network traffic analysis, malware triage, risk management frameworks, cyber exercises and wargaming

- Develop and increase the use of automation for analysis, moving target defenses, and operations (International Watch & Warning)
- Maintain large catalog of adversary tradecraft and online analysis tools for ground truth and testing
- Automate reverse engineering of code artifacts (including for embedded systems)
- Manage the analysis of network flows at enterprise scale
- Develop and assess workforce skills using advanced (adaptive) educational assessment techniques – exercises and wargaming

PWP Work:

- DHS Office of Cyber and Comms – network sensors, monitoring, and malware/response
- ARCOG – training and database updates
- DARPA TTO – cyber SA tools for new possible program
- NSA/R2 – SCORE
- DHS S&T
- iARPA

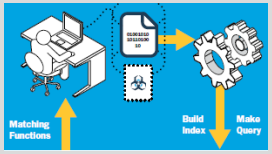
Line Funded Research:

- Automated Cyber-readiness Evaluator/Simulation Training Exercise Platform (ACE)
- Comparing Threat Modeling Methods
- Cyber-Kinetic Effects Integration (modeling and simulation)

STEPfwd and Virtual Training Environment (VTE)

SEI developed on-demand, realistic, Joint cyber-exercises to provide DoD units capability for simulation, training, and war gaming.

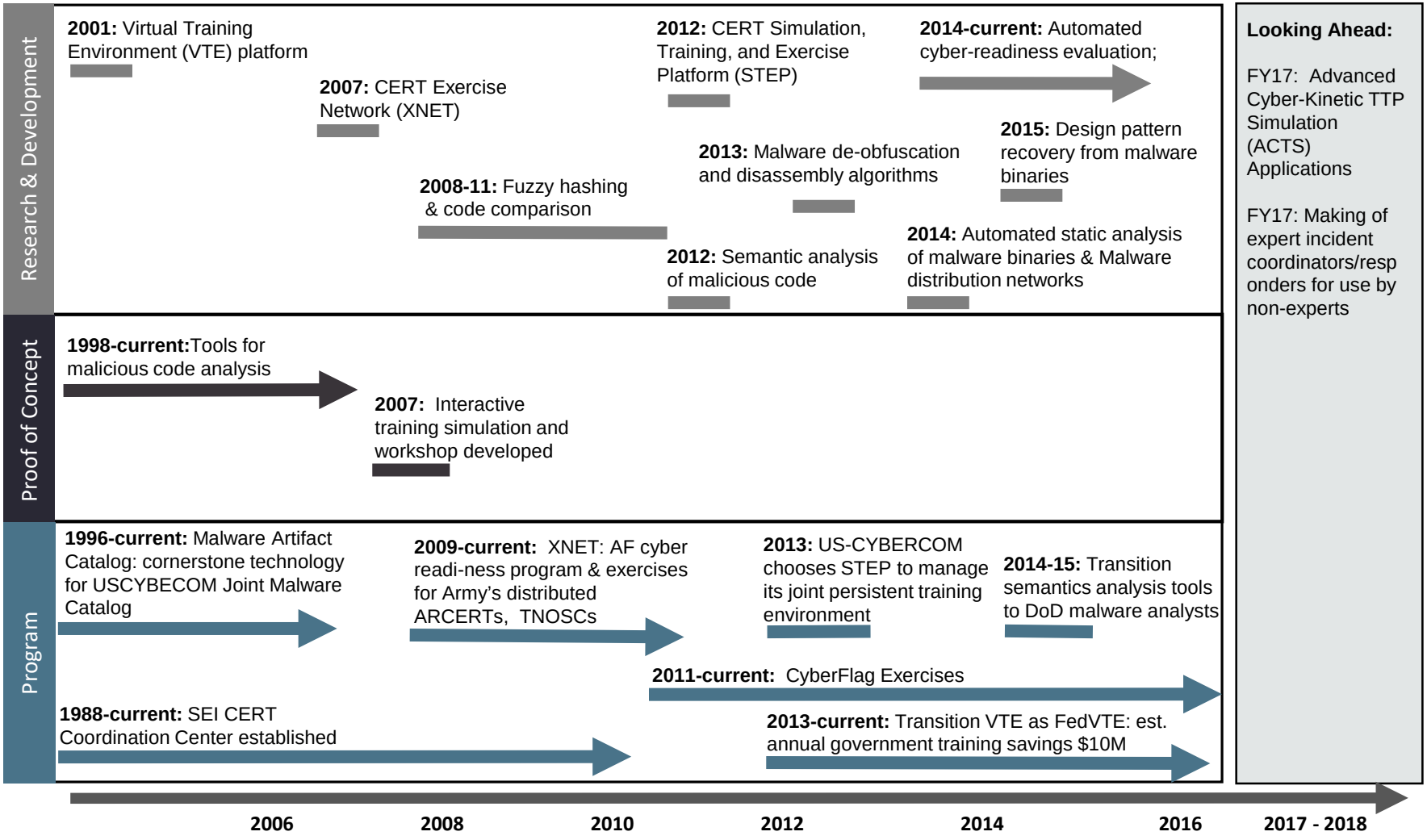
- Supports thousands of virtual hosts and a cluster of more than 200 servers that can support hundreds of cyber operators, including transition partners
- Enhancing the environment by working with world experts in computer vision at CMU to automate performance assessment of cyber operators



Automated Malware Analysis

- Automated tools for objected-oriented analysis and API call behavior identification operate 2 orders of magnitude faster than manual analysis
- Built using ROSE open source compiler infrastructure (developed at Lawrence Livermore National Laboratory)
- Future: Full open source de-compilation framework

Cyber Missions: Workforce Development & Malware



ARCERT = Army Computer Emergency Response Team; TNOSC = Theater Network Operations and Security Center