NICE Webinar Series

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

The Underserved Cybersecurity Workforce: Securely Provisioning our Future

October 10, 2018

National Cyber Security Awareness Month

- **October is #cyberaware month**
- **Week 2: Oct. 8–12: Millions of Rewarding Jobs: Educating for a Career in Cybersecurity**
- **For more information, see:**

  NIST National Cyber Security Awareness Month
  https://www.nist.gov/topics/cybersecurity/national-cyber-security-awareness-month

  National Cyber Security Alliance
  https://StaySafeOnline.org/ncsam

  U.S. Department of Homeland Security
  https://dhs.gov/ncsam

NICE Cybersecurity Workforce Framework

NIST Special Publication 800-181

Reference Resource for Cybersecurity Workforce Development

- **Audiences**

  Public and Private Sector Employers
  Education Providers
  Technology Developers
  Current and Future Cybersecurity Workers
  Training and Certification Providers
  Policymakers

- **Cybersecurity Workforce Categories** (7)

SECURELY PROVISION

OPERATE AND MAINTAIN

OVERSEE AND GOVERN

PROTECT AND DEFEND

ANALYZE

COLLECT AND OPERATE

INVESTIGATE

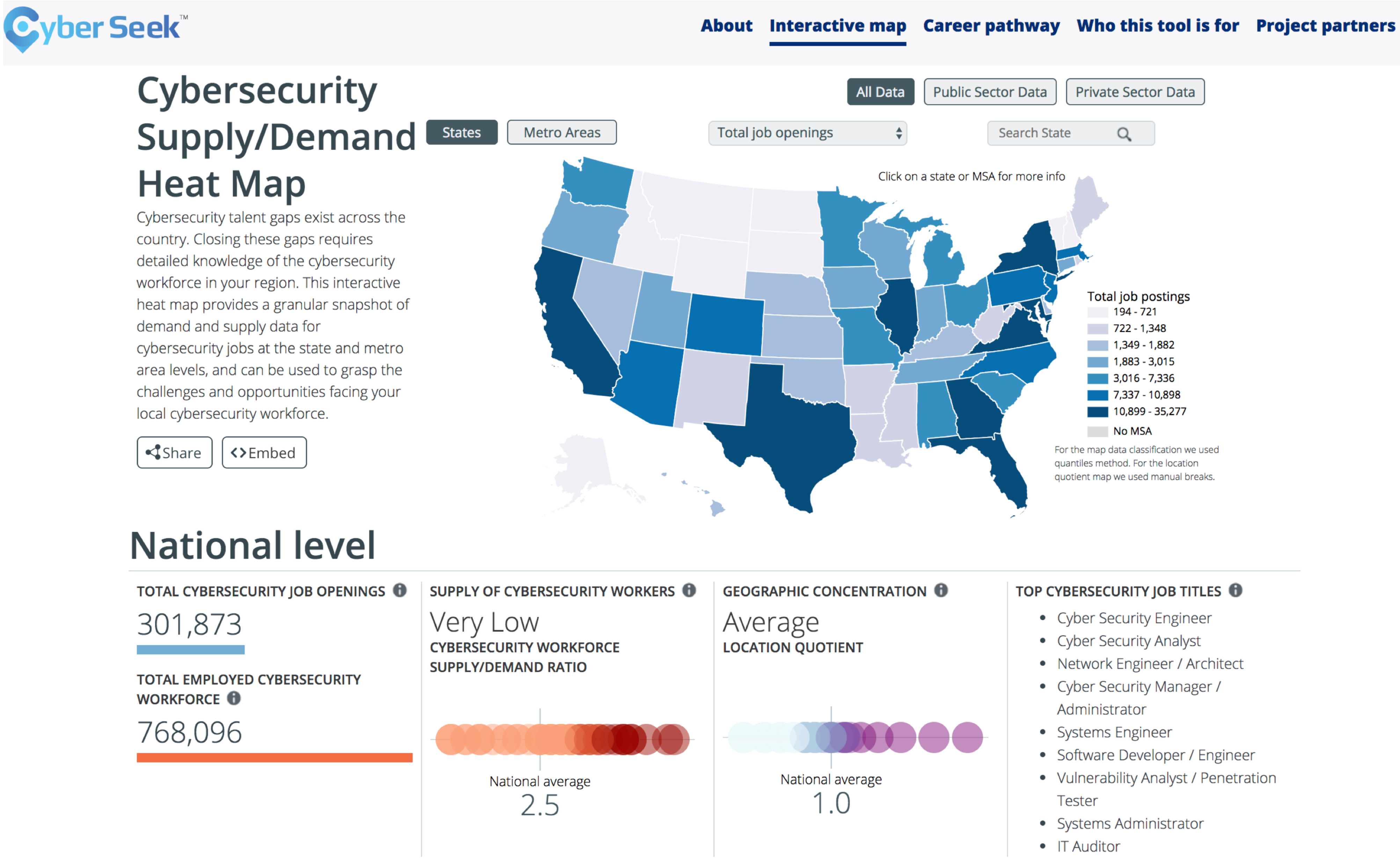
- **Specialty Areas** (33) – Distinct areas of cybersecurity work
- **Work Roles** (52) – The most detailed groupings of IT, cybersecurity, or cyber-related work, which include specific *Knowledge, Skills, and Abilities (KSA's)* required to perform a set of *Tasks*.

Category: Securely Provision

- Description: Conceptualizes, designs, procures, or builds secure information technology (IT) systems, with responsibility for aspects of system or network development.

- Specialty Areas, include:

  Risk Management
  Systems Requirements Planning
  Systems Development
  Test and Evaluation
  Technology R&D
  Systems Architecture
  Software Development



Cybersecurity Supply/Demand Heat Map

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

Click on a state or MSA for more info

Total job postings
194 - 721
722 - 1,348
1,349 - 1,882
1,883 - 3,015
3,016 - 7,336
7,337 - 10,898
10,899 - 35,277
No MSA

For the map data classification we used quantiles method. For the location quotient map we used manual breaks.

National level

TOTAL CYBERSECURITY JOB OPENINGS

301,873

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

768,096

SUPPLY OF CYBERSECURITY WORKERS

Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO

National average
2.5

GEOGRAPHIC CONCENTRATION

Average

LOCATION QUOTIENT

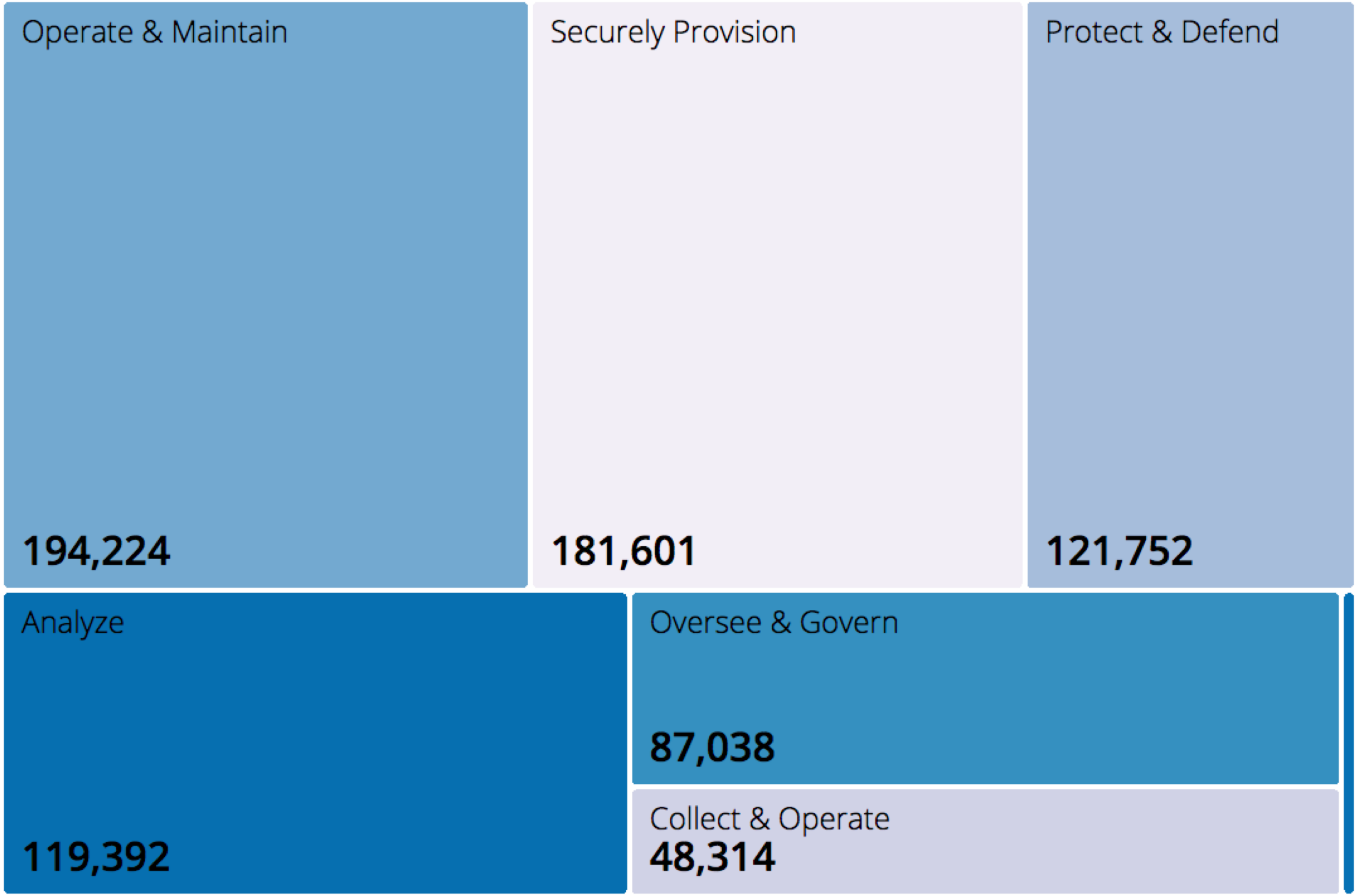
National average
1.0

TOP CYBERSECURITY JOB TITLES

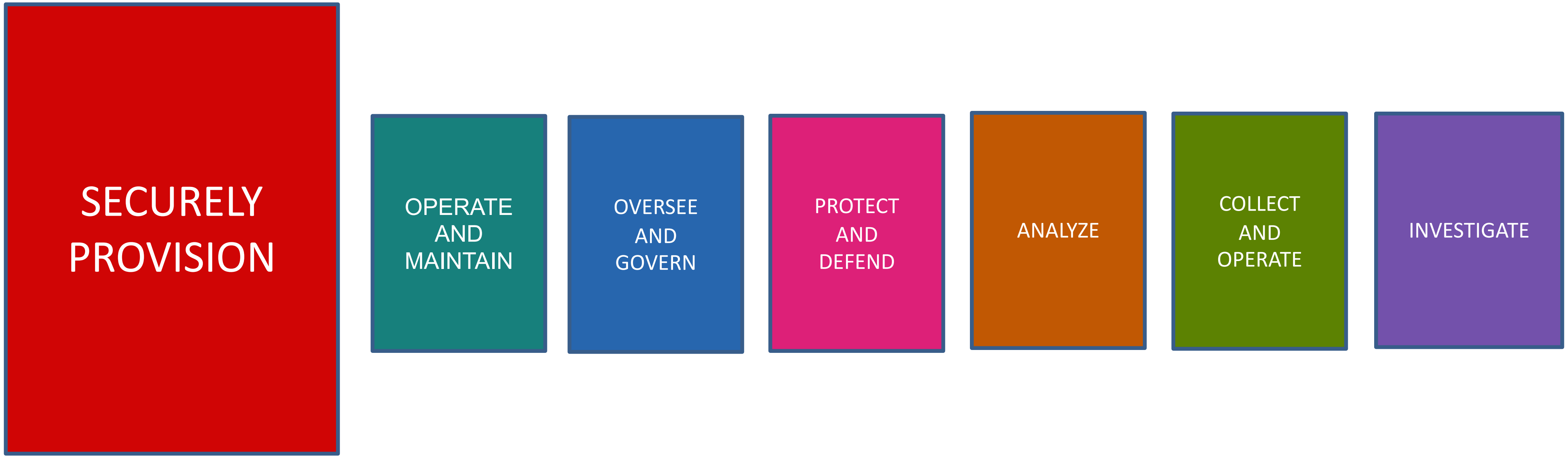
- Cyber Security Engineer
- Cyber Security Analyst
- Network Engineer / Architect
- Cyber Security Manager / Administrator
- Systems Engineer
- Software Developer / Engineer
- Vulnerability Analyst / Penetration Tester
- Systems Administrator
- IT Auditor

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

JOB OPENINGS BY NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY



NICE Framework Categories



SECURELY PROVISION

OPERATE AND MAINTAIN

OVERSEE AND GOVERN

PROTECT AND DEFEND

ANALYZE

COLLECT AND OPERATE

INVESTIGATE

```
_VER > 1000
#pragma once
#endif // _MSC_VER > 1000
#ifndef __AFXWIN_H__
    #error include 'stdafx.h' [illegible]
#endif
#include "resource.h"    // [illegible]
// CDMotionApp:
// See DMotion.cpp for the [illegible]
//
class CDMotionApp : public [illegible]
{
public:
    CDMotionApp();
// Overrides
    // ClassWizard [illegible]
    //{{AFX_VIRTUAL([illegible]
    public:
    virtual BOOL [illegible]
    //}}AFX_VIRTUAL

// Implementation
    //{{AFX_MSG([illegible]
    afx_msg void [illegible]
        // NOTE - [illegible]
        //    DO NOT [illegible]
    MSG [illegible]
```

Rethinking Cybersecurity from the Inside Out

An Engineering and Life Cycle-Based Approach for Achieving Trustworthy Secure Systems

Dr. Ron Ross

Computer Security Division
Information Technology Laboratory

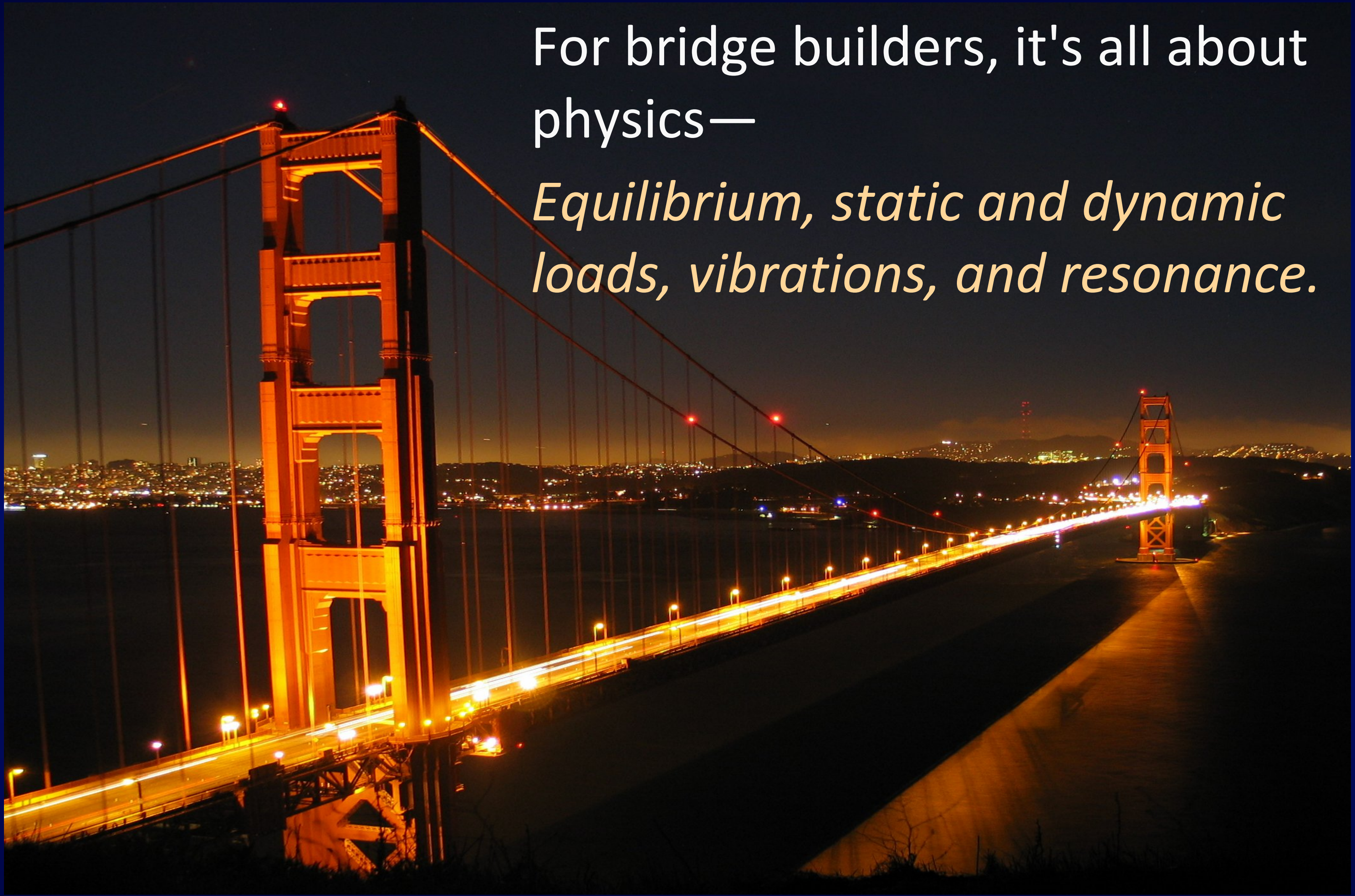
Complexity.

The n + 1 vulnerabilities problem.

Unconstrained due to increasing attack surface.

The hard cybersecurity problems are buried below the water line…

In the hardware, software, and firmware.



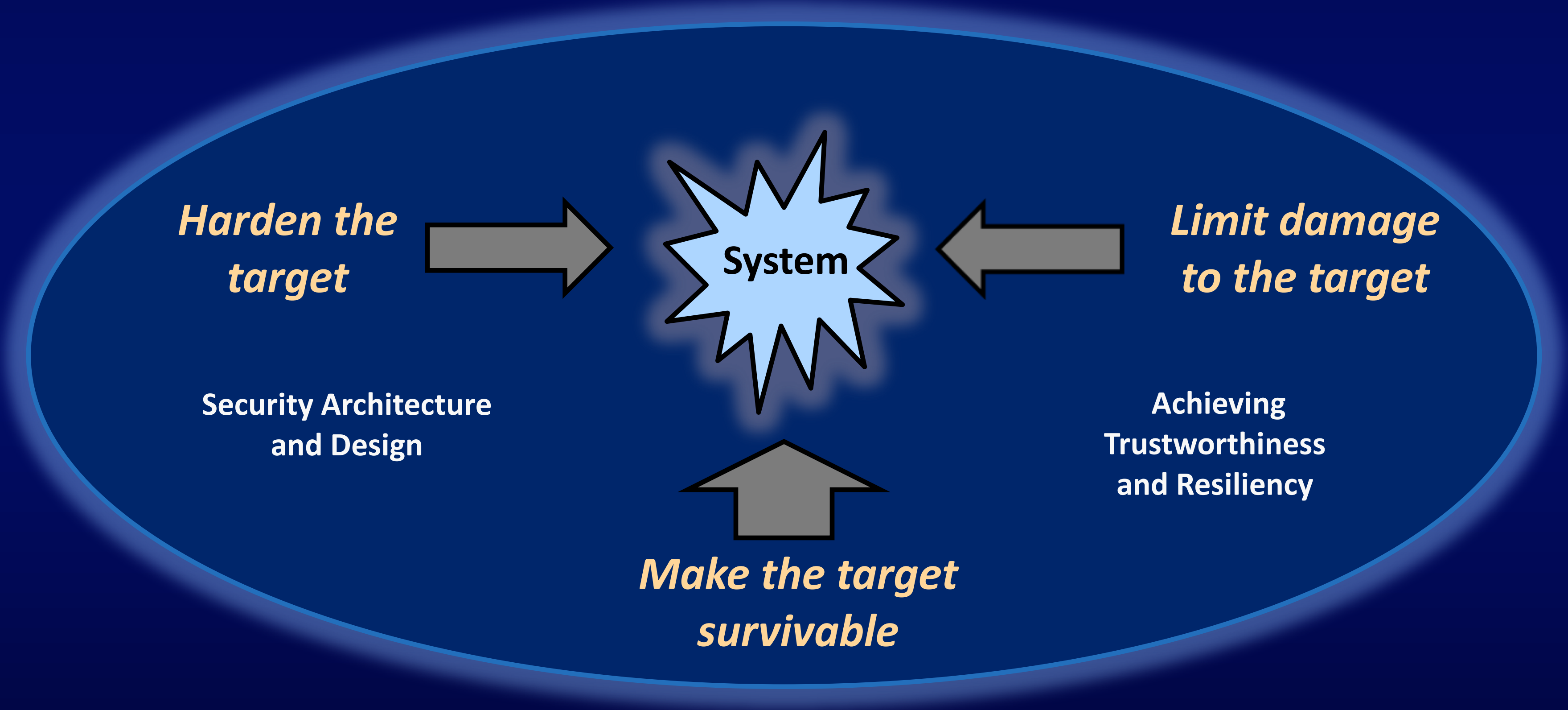
For bridge builders, it's all about physics—

Equilibrium, static and dynamic loads, vibrations, and resonance.

For information system developers, it's all about mathematics, computer science, architecture, and systems engineering—

Trustworthiness, assurance, penetration resistance and resilience.

Reducing susceptibility to ***cyber threats*** requires a multidimensional systems engineering approach.



Harden the target

Security Architecture and Design

System

Limit damage to the target

Achieving Trustworthiness and Resiliency

Make the target survivable

NIST Special Publication 800-160

Systems Security Engineering

Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

Security.

An emergent property.

Technical Processes

- Business or mission analysis
- Stakeholder needs and requirements definition
- System requirements definition
- Architecture definition
- Design definition
- System analysis
- Implementation
- Integration
- Verification
- Transition
- Validation
- Operation
- Maintenance
- Disposal

ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes

Nontechnical Processes

- Project planning
- Project assessment and control
- Decision management
- Risk management
- Configuration management
- Information management
- Measurement
- Quality assurance
- Acquisition and Supply
- Life cycle model management
- Infrastructure management
- Portfolio management
- Human resource management
- Quality management
- Knowledge management

ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes

Security should be a by-product of good design and development practices – integrated throughout the system life cycle.

Race to the Top

Better Security Through Engineering

Q & A

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Cybersecurity Criticality is Driven by Increased Software

Carol Woody, Ph.D.

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

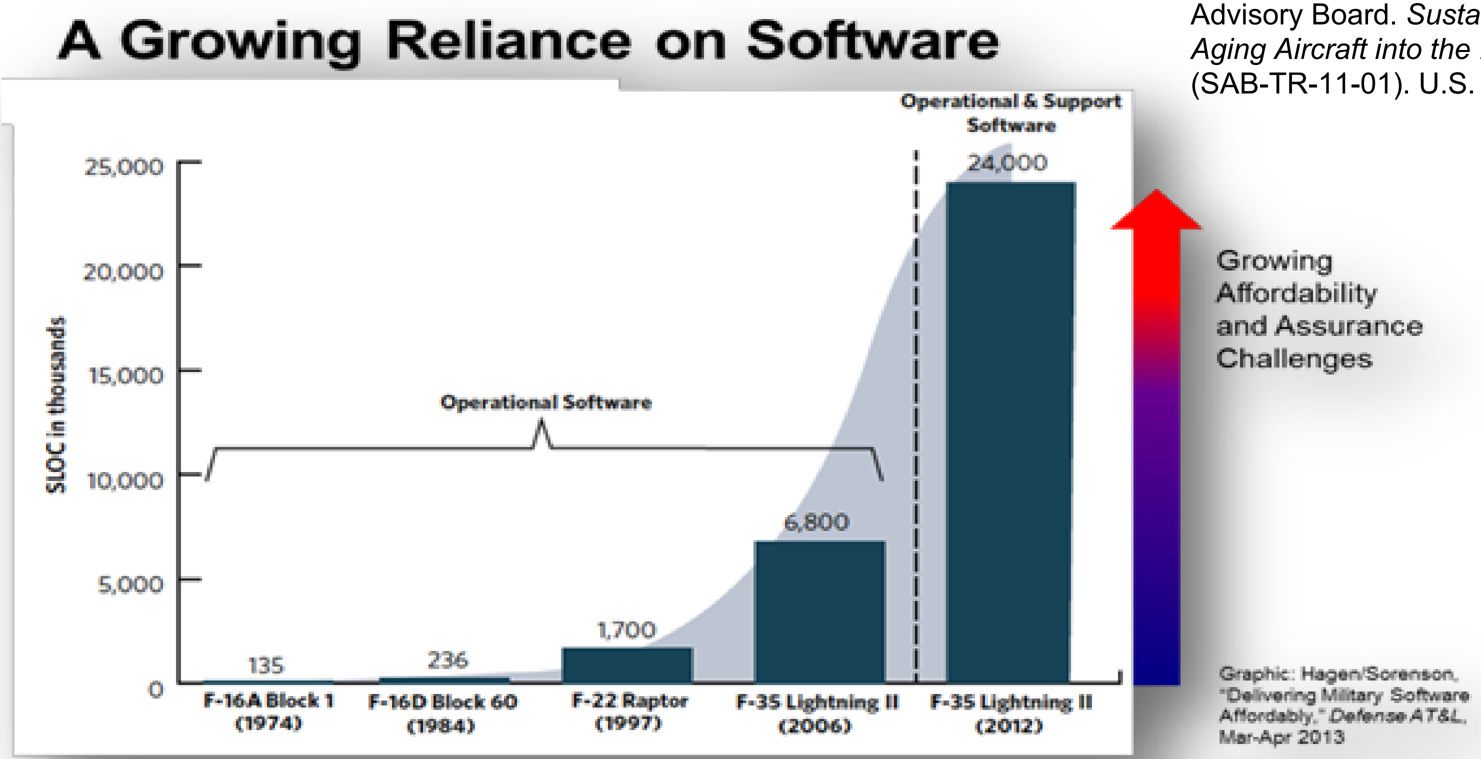
The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM18-1161

Software Reliance is Rapidly Expanding

Source: U.S. Air Force Scientific Advisory Board. *Sustaining Air Force Aging Aircraft into the 21st Century* (SAB-TR-11-01). U.S. Air Force, 2011.



A Growing Reliance on Software

Growing Affordability and Assurance Challenges

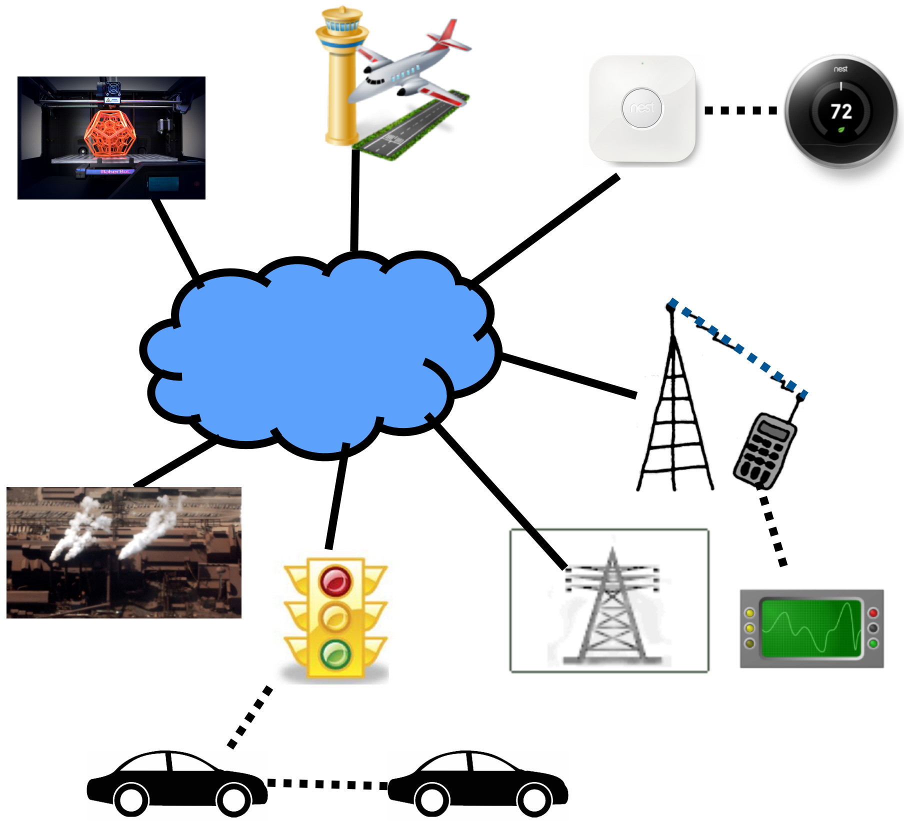
Graphic: Hagen/Sorenson, "Delivering Military Software Affordably," *Defense AT&L*, Mar-Apr 2013

Software as % of total system cost

1997: 45% ⟶ 2010: 66% ⟶ 2024: 88%

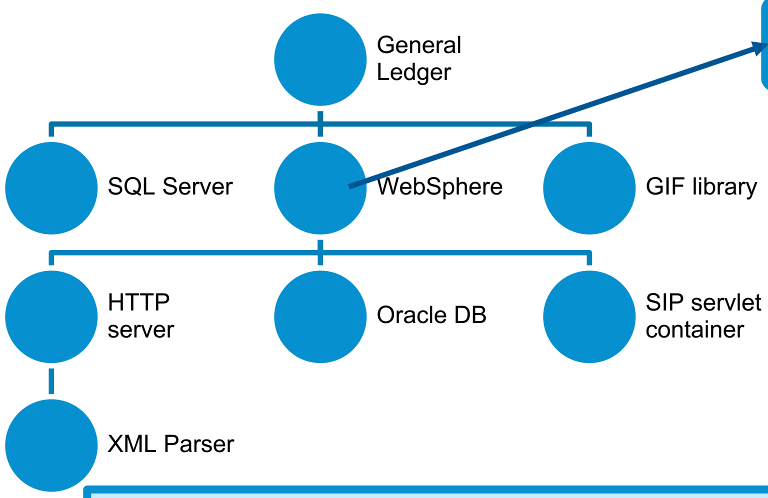
From 1997 to 2012, software industry production grew from $149 billion to $425 billion

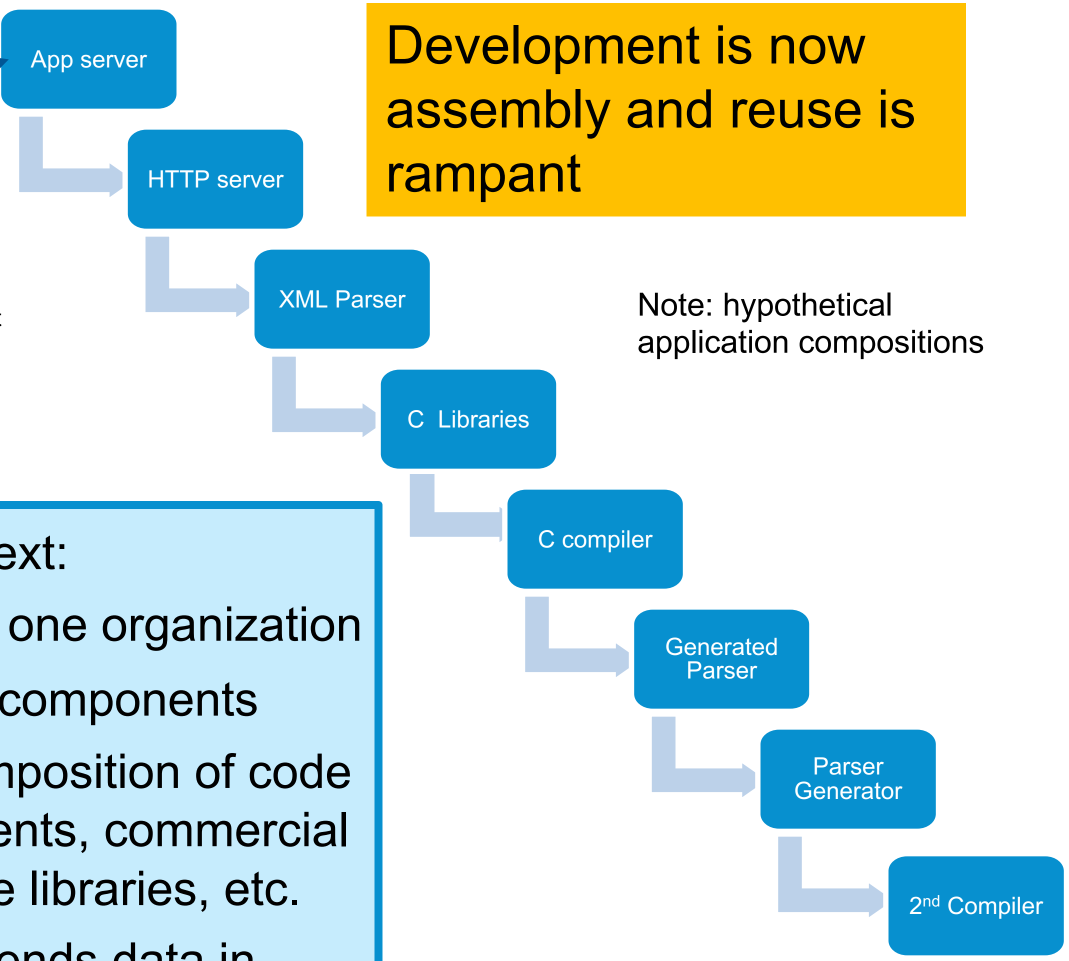
Software is Communicating to Other Systems



- Cellular
  - Main processor
  - Graphics processor
  - Base band processor (SDR)
  - Secure element (SIM)
- Automotive
  - Autonomous vehicles
  - Vehicle to infrastructure (V2I)
  - Vehicle to vehicle (V2V)
- Industrial and home automation
  - 3D printing (additive manufacturing)
  - Autonomous robots
  - Interconnected SCADA
- Aviation
  - Next Gen air traffic control
  - Fly by wire
- Smart grid
  - Smart electric meters
  - Smart metering infrastructure
- Embedded medical devices

Demand Drives Faster and Cheaper Approaches





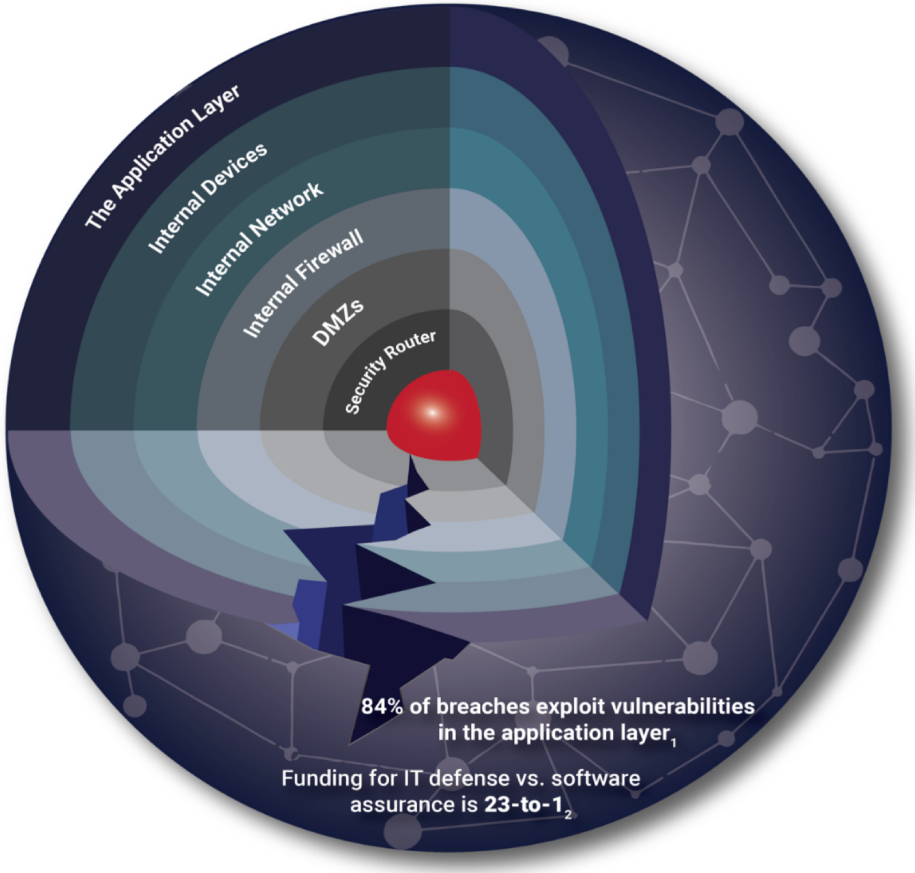
Development is now assembly and reuse is rampant

Note: hypothetical application compositions

Collective development – context:

- Too much specialization for one organization
- Too little value in individual components
- Each component is a decomposition of code collected from sub-components, commercial products, open source, code libraries, etc.
- Each collects, stores, and sends data in different file structures and formats using frameworks handle target infrastructure

84% of Security Breaches Exploit the Software Applications


The Application Layer
Internal Devices
Internal Network
Internal Firewall
DMZs
Security Router
84% of breaches exploit vulnerabilities in the application layer[1]
Funding for IT defense vs. software assurance is **23-to-1**[2]

Breaking this cycle will require engineering of the software we use to handle the realities of the operational environment. All fielded software needs good cybersecurity. However,

- "76% of U.S. developers use no secure application program process"[3]
- "More than 40% of software developers globally say that security isn't a top priority for them"[4]

1. Clark, Tim, *Most cyber Attacks Occur from this Common Vulnerability,* Forbes. 03-10-2015
2. Feiman, Joseph, *Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves,* Gartner. 09-25-2014. G00269825
3. *Horvath, Mark, Neil MacDonald, Ayal Tirosh: Integrating Security Into the DevSecOps Toolchain, Gartner. 11-16-2017. G00334264*
4. Microsoft[1]– http://visualstudiomagazine.com/articles/2013/07/16/majority-of-us-devs-dont-practice-secure-coding.aspx

Anyone Can Write Software but is it Good?

How To Raise The Next Zuckerberg: 6 Coding Apps For Kids

http://readwrite.com/2013/04/19/how-to-raise-the-next-zuck-6-coding-apps-for-kids/

TYNKER - We Empower KIDS to Become Makers

https://www.tynker.com/

How and Why to Teach Your Kids to Code

http://lifehacker.com/how-and-why-to-teach-your-kids-to-code-510588878

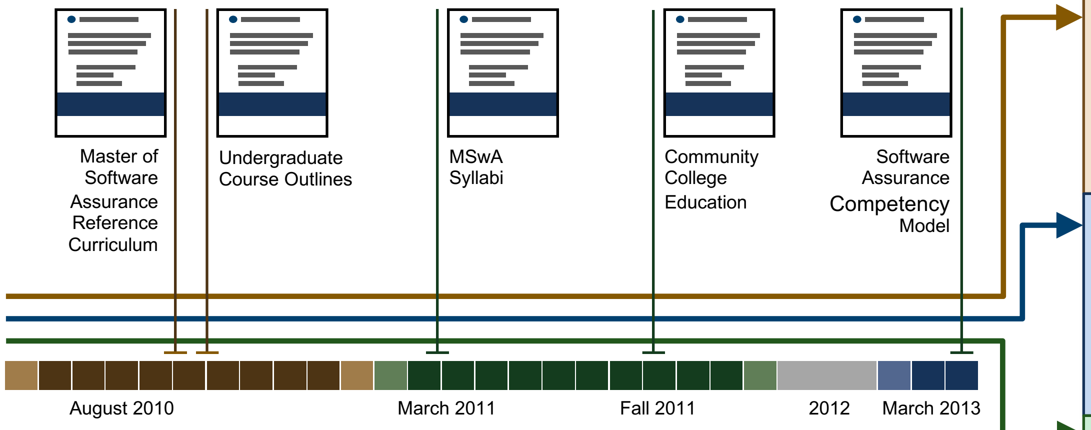
Best-in-class code: <600 defects per MLOC
Very good code: 600 to 1,000 defects per MLOC
Average quality code: 6000 defects per MLOC

Up to 5% of defects are vulnerabilities

Software Assurance Education for Improved Cybersecurity

Software Assurance Curriculum Project

Goals: Develop software assurance curricula
Define transition strategies for implementation



Master of Software Assurance Reference Curriculum

Undergraduate Course Outlines

MSwA Syllabi

Community College Education

Software Assurance Competency Model

August 2010

March 2011

Fall 2011

2012

March 2013

Community Outreach

- 20+ Published Papers
- 7 SEI reports
- 15+ talks, webinars, podcasts, media
- Thousands of downloads
- LinkedIn group of 500+ members
- Course materials and videos

Integrated into course offerings

- Carnegie Mellon University
- Stevens Institute of Technology
- US Air Force Academy
- University of Detroit Mercy
- University of Houston
- (ISC)^2

Transition

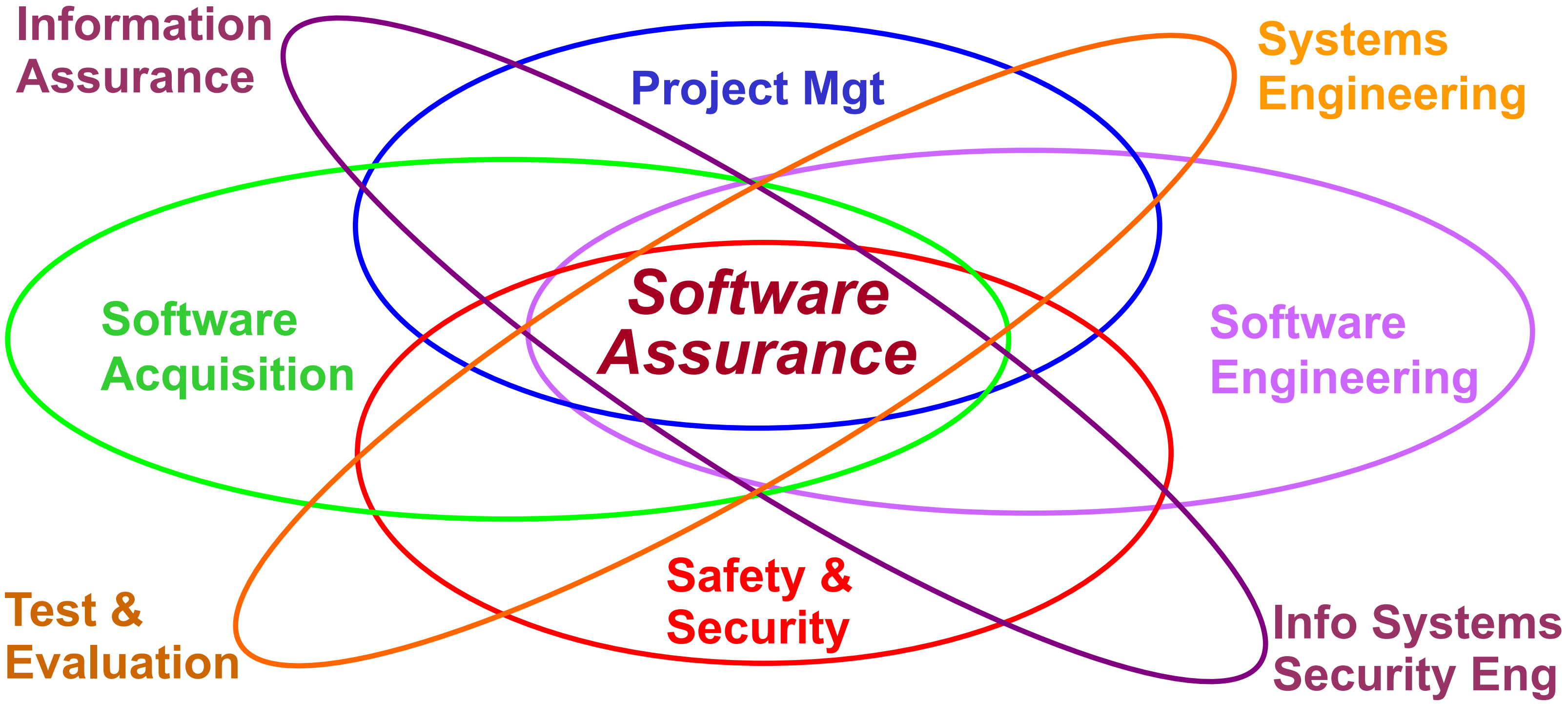
- Degree offerings
  - MSwA Curriculum Design:
    Polytechnic University of Madrid
  - Community College Programs:
    Illinois Central College
    Alamo Colleges
    Lincoln Land Community College
- SwA Courses
  - Assurance Management
  - Assured Software Dev't 1
  - Exec Course

Professional Society Recognition

IEEE acm

https://www.sei.cmu.edu/education-outreach/curricula/software-assurance/index.cfm

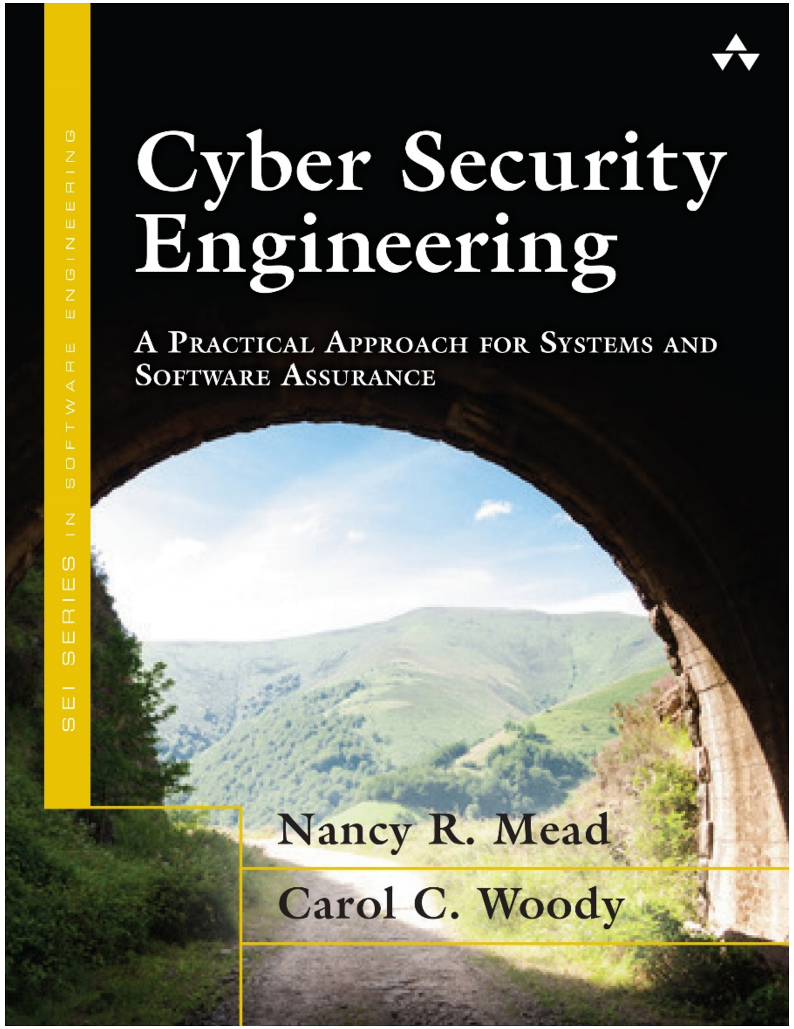
Many Disciplines Need Software Assurance Knowledge



In Education and Training, Software Assurance could be addressed as:

- A "knowledge area" extension within each of the contributing disciplines;
- A set of functional roles, drawing upon a common body of knowledge; allowing more in-depth coverage dependent upon the specific roles.

Publication to Support the Curriculum


Cyber Security Engineering
A Practical Approach for Systems and Software Assurance
SEI Series in Software Engineering
Nancy R. Mead
Carol C. Woody

Released November 2016 as part of the SEI Book Series

For more information see https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=483667

CERT Cybersecurity Engineering and Software Assurance Professional Certificate

Released March 2018

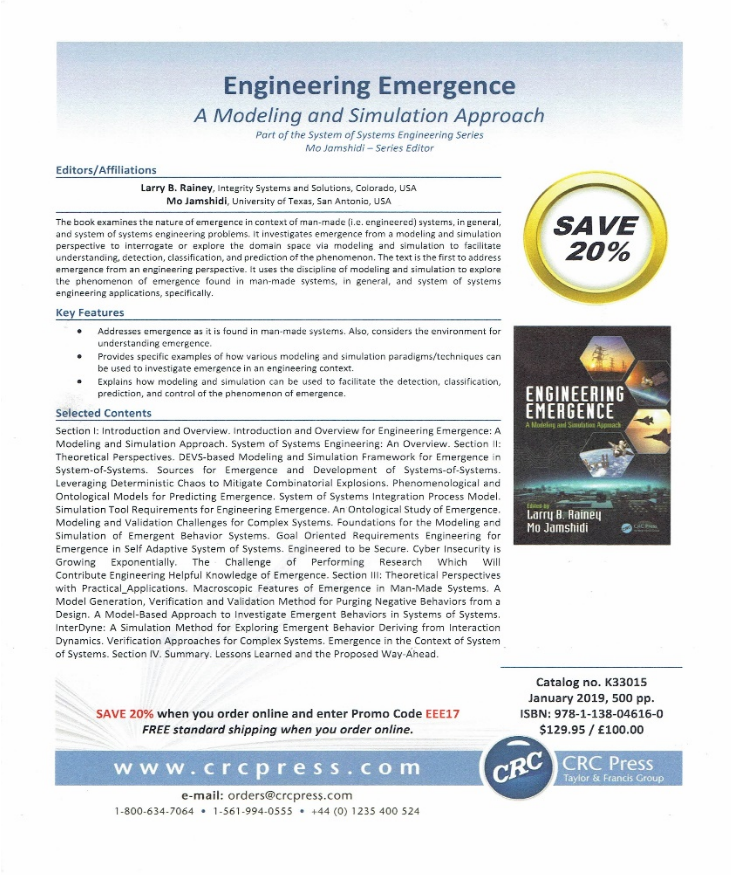
The program consists of five components

- Software Assurance Methods in Support of Cybersecurity Engineering
- Security Quality Requirements (SQUARE)
- Security Risk Analysis (SERA)
- Supply Chain Risk Management
- Advanced Threat Modeling

To learn more, visit https://sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=33881.

Additional Materials

SEI webpage for cybersecurity and software assurance:
www.sei.cmu.edu/go/cybersecurity-engineering



SAVE 20%
ENGINEERING EMERGENCE
A Modeling and Simulation Approach
Edited by
Larry B. Rainey
Mo Jamshidi

Engineering Emergence

A Modeling and Simulation Approach

Part of the System of Systems Engineering Series
Mo Jamshidi – Series Editor

Editors/Affiliations

Larry B. Rainey, Integrity Systems and Solutions, Colorado, USA
Mo Jamshidi, University of Texas, San Antonio, USA

The book examines the nature of emergence in context of man-made (i.e. engineered) systems, in general, and system of systems engineering problems. It investigates emergence from a modeling and simulation perspective to interrogate or explore the domain space via modeling and simulation to facilitate understanding, detection, classification, and prediction of the phenomenon. The text is the first to address emergence from an engineering perspective. It uses the discipline of modeling and simulation to explore the phenomenon of emergence found in man-made systems, in general, and system of systems engineering applications, specifically.

Key Features

- Addresses emergence as it is found in man-made systems. Also, considers the environment for understanding emergence.
- Provides specific examples of how various modeling and simulation paradigms/techniques can be used to investigate emergence in an engineering context.
- Explains how modeling and simulation can be used to facilitate the detection, classification, prediction, and control of the phenomenon of emergence.

Selected Contents

Section I: Introduction and Overview. Introduction and Overview for Engineering Emergence: A Modeling and Simulation Approach. System of Systems Engineering: An Overview. Section II: Theoretical Perspectives. DEVS-based Modeling and Simulation Framework for Emergence in System-of-Systems. Sources for Emergence and Development of Systems-of-Systems. Leveraging Deterministic Chaos to Mitigate Combinatorial Explosions. Phenomenological and Ontological Models for Predicting Emergence. System of Systems Integration Process Model. Simulation Tool Requirements for Engineering Emergence. An Ontological Study of Emergence. Modeling and Validation Challenges for Complex Systems. Foundations for the Modeling and Simulation of Emergent Behavior Systems. Goal Oriented Requirements Engineering for Emergence in Self Adaptive System of Systems. Engineered to be Secure. Cyber Insecurity is Growing Exponentially. The Challenge of Performing Research Which Will Contribute Engineering Helpful Knowledge of Emergence. Section III: Theoretical Perspectives with Practical_Applications. Macroscopic Features of Emergence in Man-Made Systems. A Model Generation, Verification and Validation Method for Purging Negative Behaviors from a Design. A Model-Based Approach to Investigate Emergent Behaviors in Systems of Systems. InterDyne: A Simulation Method for Exploring Emergent Behavior Deriving from Interaction Dynamics. Verification Approaches for Complex Systems. Emergence in the Context of System of Systems. Section IV. Summary. Lessons Learned and the Proposed Way-Ahead.

Catalog no. K33015
January 2019, 500 pp.
ISBN: 978-1-138-04616-0
$129.95 / £100.00

SAVE 20% when you order online and enter Promo Code EEE17
FREE standard shipping when you order online.

www.crcpress.com

CRC Press
Taylor & Francis Group

e-mail: orders@crcpress.com
1-800-634-7064 • 1-561-994-0555 • +44 (0) 1235 400 524

Two chapters are included in **Engineering Emergence** to be released January 2019 highlighting “Engineered to be Secure” and “Cyber Insecurity is Growing” for systems of systems.

Q & A

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Report to the President on Growing and Sustaining the Nation's Cybersecurity Workforce

Recommendations:

- The Executive Branch should strongly encourage educators, training providers, and employers to use the taxonomy and lexicon of the NICE Framework as the reference for building workforce development strategies.
- The federal government should partner with the private sector and academia to develop interdisciplinary cybersecurity curriculum guidance that addresses the need for widely accepted and shareable cybersecurity curricula that incorporate employers' cybersecurity needs.

https://nist.gov/nice/cybersecurityworkforce

Report to the President on Enhancing Resilience Against Botnets

Goal 5: Increase awareness and education across the ecosystem

Actions:

- Government should encourage the academic and training sectors to fully integrate secure coding practices into computer science and related programs.
- The academic sector, in collaboration with the National Initiative for Cybersecurity Education, should establish cybersecurity as a fundamental requirement across all engineering disciplines.

Q & A

National
APPRENTICESHIP
WEEK
NOVEMBER 12-18, 2018

National Apprenticeship Week

November 12-18, 2018

dol.gov/apprenticeship/naw/

National Cybersecurity Career Awareness Week

November 12-17, 2018

nist.gov/nice/nccaw

Thank You for Joining Us!

Upcoming Webinar: “Upskilling and Reskilling the Workforce for Cybersecurity Roles”

When: Wednesday, November 14, 2018 at 2:00pm – 3:00pm EST

Register: https://nist-nice.adobeconnect.com/webinar-nov2018/event/registration.html

nist.gov/nice/webinars

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION