Why Is R&D in the Cyber and Software Engineering Environment Different?

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Terry Roberts
April 28, 2010
Why Is Cyberspace Critical to All of Us?

- Why is cyberspace critical to all of us?
- What are the dynamics of cyberspace?
- What is the role that software engineering/cyber engineering plays in cyberspace?
- How is this field of science unique and what impact does that have on how we approach R&D in this arena?
- What major R&D work has been accomplished in the cyber assurance arena over the past ten years?
- How should that work impact an updated and comprehensive R&D vision?
- Where should we be focusing our efforts – where are some of the critical R&D gaps?
- What is the perfect trifecta?
What Is the Cyber Environment?

Includes all

- System of Systems
- Architecture
- Services
- Netted Hardware/Platforms
- People who digitally connect to cyberspace

*Cyberspace is where our daily work and our priority missions are conducted*
Growth of the Internet

350,000,000 – number of Facebook accounts created between Jan 2004 - Nov 2009

40,000,000 to 180,000,000 – increase in domain name registrations between Dec 2000 and Sep 2009

1 to 250,000,000 – growth of websites from Dec 1990 to Jul 2009

4 to 700,000,000 – growth of Internet hosts between Dec 1969 and Sep 2009

ARPANET Map — http://som.csudh.edu/cis/lpress/history/arpamaps/
The Global Information Grid (GIG)

The GIG connects:

- roughly 3 million computers
- 100,000 LANs
- 100 long-distance networks
- a multitude of wireless networks and devices

Federal IT Market Growth

In the next five years, IT contractors will see the federal market for their services increase by a compound annual growth rate of 5.4 percent to a total of $111.9 billion by 2015.

-- Ben Bain
*Federal Computer Week*
April 8, 2010
Increasing Software Lines of Code & Complexity

Why Is R&D in the Cyber and Software Engineering Environment Different?
Terry Roberts, April 28, 2010

© 2010 Carnegie Mellon University
What Is Today’s Cyber Environment?

Cyber environment\(^1\) refers to the entire set of conditions when interacting with computing and networking resources.

The cyber environment encompasses users, networks, devices, systems, software, hardware, data in storage or transit, applications, services, and processes that can be connected directly or indirectly to networks.

\(^1\) SEI definition with input from International Telecommunications Union: [http://www.itu.int/ITU-T/studygroups/com17/sg17-q4.html](http://www.itu.int/ITU-T/studygroups/com17/sg17-q4.html)

National Military Strategy for Cyberspace Operations
Continuous Migration of DoD/IC/Civil Missions & Functions to Cyberspace

1995 - 2002
- Administration
- Basic Comms & Logistics
- Non-Time Critical Ops Coordination
- Person-to-Person Communications
- Tasker Management

2002 - Today
- All Operational Planning and Execution
- Majority C4 and Intelligence
- Majority Training & Exercises
- All Personnel Management
- All Medical Management
- All Financial Management

What non-physical work today isn’t conducted in cyberspace?
Where Do the Disciplines of Software and Cyber Engineering Fit?

What is Cyber Engineering?

Could it be the discipline of software engineering body of knowledge and practices applied in a netted environment?

Software Engineering is Foundational to and Inextricably Linked to the Cyber Environment
The Impact of Software Engineering Today

Software is both foundational and pervasive

- IT Systems
- C4ISR
- Weapons

Software is mission critical

- 20-80% of weapons/platforms/systems is software dependent
- software failure can be catastrophic

Software is the heart and mind of your system
Challenges We Are Facing in Cyberspace

- Increasing dependence on large-scale, highly distributed systems, SOA, cloud computing, multi-core...
- Constantly evolving nature of the threat
- Ever-increasing number and potential impact of cyber attacks
- Software and system engineering and network monitoring tools are not keeping pace with changes in attack methods and technologies
- Increasing need for an advanced scientific body of knowledge and a mature engineering discipline underlying cyber assurance

All of the above must be addressed by cutting edge R&D focused on game changing technological advances that are based upon foundational scientific study
Cyber R&D Dynamics

• What is today’s cyber environment? …much more than the network
• What do we do in the cyber environment? …almost everything
• Will the cyber environment be there when we need it for financial transactions, for critical infrastructure, for National Defense, for telecommunications?
• Where does the U.S. government fit in the cyber arena? …it is dependent upon it, but does not own it (it is mostly owned, operated and serviced by International Industry)
• Is today’s cyber environment inherently fragile and unreliable?

How can industry and government fully leverage a comprehensive and responsive R&D approach to establish a resilient network for the near term and an assured network alternative for the future – in support of all essential missions and functions?
Institute for Information Infrastructure Protection 2009 Report Recommendations

1. **A coordinated and collaborative approach is needed.** Cyber security research and development efforts in the U.S. must be better coordinated; only through information sharing and collaboration can effective solutions emerge.

2. **Metrics for security are a broad enabler and must be developed.** Metrics are enablers, essential to helping companies, governments, and suppliers make better security decisions; they also strengthen the legal and policy framework.

3. **An effective legal and policy framework for security must be created.** A national strategy for cyber security requires a sound domestic legal and policy framework as well as an international doctrine.

4. **The human dimension of security must be addressed.** Technologists and policymakers must consider the human element carefully when developing security solutions.

Current DoD S&T Investments in Cyber Security and Information Assurance

OSD-Led Task Force Recommendations

- Address key points of the cyberspace S&T study from within S&T resources starting in FY10
- Examine and refine cyber protection needs in QDR 10
- Develop measures to assess how much cyber protection is enough for DoD
- Expand the role of the IA S&T Steering Council to include oversight of all defensive cyber S&T programs
- Reprioritize DoD S&T funding to increase Cyber Conflict S&T in coordination with Defense S&T Advisory Group
- Enhance cooperation between offensive and defensive communities to enable improved cyber defense

source: DoD S&T Investment in Cyberspace Security and Information Assurance Report from December 2009
Before Discussing an Optimal R&D Agenda

Think about it…

• How does R&D differ in this unique arena?

• Why is it an imperative that we embark on a comprehensive R&D approach today?

• How does an effective partnership with academia, industry, and government enable us to take the science to the next level?
Why Is R&D in the Cyber and Software Engineering Environment Different?

Terry Roberts, April 28, 2010

© 2010 Carnegie Mellon University

source: Dr. Thomas H. Killion, Enabling Future Technology Ultra-Large-Scale Systems in the Army
www.sei.cmu.edu/library/assets/killion.pdf
# Cyber Compared with Other Sciences

<table>
<thead>
<tr>
<th></th>
<th>Physical Science</th>
<th>BioScience</th>
<th>Computer/Software/Cyber Science</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Origins/History</strong></td>
<td>Begun in antiquity</td>
<td>Begun in antiquity</td>
<td>Mid-20th Century</td>
</tr>
<tr>
<td><strong>Enduring Laws</strong></td>
<td>Laws are foundational to furthering exploration in the science</td>
<td>Laws are foundational to furthering exploration in the science</td>
<td>Only mathematical laws have proven foundational to computation</td>
</tr>
</tbody>
</table>
| **Framework of Scientific Study** | Four main areas: astronomy, physics, chemistry, and earth sciences | Science of dealing with health maintenance and disease prevention/treatment | • Several areas of study: computer science, software/systems engineering, IT, HCI, social dynamics, AI  
  • All nodes attached to/relying on netted system |
| **R&D and Launch Cycle** | 10-20 years | 10-20 years | Significantly **compressed**; solution time to market needs to happen very quickly |
Software/Cyber Science: R&D Key Premises

- Few foundational laws; no enduring laws
- Mid-20th century invention—still in its infancy
- No systematic, globally accepted method for scientific discovery
- An environment of scientific study that is totally technological
- An environment that is not owned or controlled by government or industry
- R&D timelines are measured in seconds, minutes, days—not years

So much left to discover, research, analyze, codify, develop and test
CMU/Cylab/SEI-CERT Cyber R&D Review: Vision to Establish Preeminence in Cyber R&D

• Enable cyber research to keep pace

• Envision future needs: emerging trends, changes in technology, threat capabilities, and appropriate responses

• Maintain a contextual reference for what key cyber R&D is being done where unique contributions could be made

• Fully connect to and leverage current cyber R&D Body of Knowledge across all organizations and individuals focused on similar challenges or gaps

• Recommend usable and potentially high impact investments

...while establishing a foundational cyber science
Illustrative High-Impact Research Partnerships: Three Examples of Recent $1B+ Markets Created

Client/server computing

- Berkeley, CMU, CERN
- Parc, DEC, IBM
- Novell, EMC, Sun, Oracle

Parallel computing

- Illiac 4, CMU, Caltech, HPC
- IBM, Intel
- CM-5, Teradata, Cray T3D

Speech recognition

- CMU, SRI, MIT
- Bell, IBM, Dragon
- Dragon, IBM, L&H

source: B. Lampson (www.cra.org/govaffairs/images/Tire-Tracks-Color_lg.jpg)
Why Is R&D in the Cyber and Software Engineering Environment Different?

Terry Roberts, April 28, 2010

© 2010 Carnegie Mellon University

CMU/Cylab/SEI-CERT Cyber R&D Review: Technological Goals and Objectives

• Disruptive
  – Make a significant advancement in a fundamental approach to securing our information systems

• Sustainable
  – Have a long-term effect

• High Payoff
  – Result in qualitative improvement in the mid-term that justifies the investment

• Doable
  – Attainable and executable goals
CMU/Cylab/SEI-CERT Cyber R&D Review: Approach

• Look beyond current work

• Develop a broad view of all the areas that merit research

• Institute a framework that continually refreshes and refines research areas

• Engage active & complementary participation and collaboration from academia, industry, and government

• Continuously inform and renew research agenda priorities
CMU/CyLab/SEI-CERT R&D Review: Past Ten Years

• Conducted CERT Speaker Series – distinguished speakers presented ideas on current challenges and needed research
• Reviewed and categorized research recommendations from 1999-2009
• Held in-depth structured interviews with luminaries in the field to capture their ideas and recommendations
• Hosted CERT Technical Symposium to bring a concentration of bright minds together to describe challenges and future directions
• Leveraged Industrial Consortium to develop current needs
• Partnered with Carnegie Mellon University thought leaders in cyber security to share perspectives
CMU/CyLab/SEI-CERT R&D Review: Recommended Focus Areas

- Protect the Network Fabric
- End-to-End Trusted Systems
- Secured Software and Systems Development
- Resilient Systems Operations
- Effective Evaluation Tools and Techniques
- Offensive Operations
- Forensics
Establishment of an inclusive science of cyber engineering

• Define the new discipline, built upon Computer Science, Software Engineering, System Engineering and Mathematics
• Determine what foundational knowledge and core competencies are needed
• Develop the commensurate curriculum at the undergraduate and graduate levels
• Establish the profession across the workforce landscape
TWR Recommended R&D Priorities - 2

Develop an assured cyber ecosystem scale – mission and domain specific (eg. Levels: 1-Minimal, 2-Moderate, 3-Maximum)

Establishment of an optimal resilient architecture continuum to achieve the desired/needed level of assurance (for software & cyber physical systems)

- Software coding standards at the language and coding practice level
- Software architecture design, w/ performance measures
- Model for composing secure systems from resilient & non-resilient components
- Development of assured architectural interoperable approaches
- Effective architectural mapping, diagnostics, and identification of risks with the ability to isolate and contain probable threats or aberrant behavior
TWR Recommended R&D Priorities- 3

Create an enduring culture of performance & mission assurance

• Promote open discussion, debate, education and outreach

• Develop an economic model/ business case for building and designing w/ assurance in the forefront

• Determine high payoff and end-to-end approaches, models, technologies, with supporting metrics

• Establish a clearinghouse for high impact R&D prototyping, testing and transition technologies

• Draft technically informed and aware statute, policies and standards
The Intersection of Basic and Applied Science

“We need the minds of the basic scientist and the application engineer, those in universities, and those in industry.

And we need them working together in the cauldron created by the urgency and technical demands of defense.”

— Dr. Regina E. Dugan
Director, DARPA
Optimal Cyber R&D Collaboration Requirements...

From Universities
- Creative and out-of-the-box research
- Stability of innovative operations: 25 – 33% of all research funding
- "Nimble" R&D: 67 – 75% of all funding is competitive

From Industry
- Time-sensitive, marketable research
- Consistently focused: mid-range (3 – 5 years) focus
- Commitment to broad marketing of technology

From Government
- Longer term, high-end, transitionable research gaps/challenges
- Demonstrable successes, social vision
- Continuously leverage academia and industry top R&D
Cyber R&D Imperative: Institute a New Collaborative Approach Across Academia, Industry, and Government

The Cyber R&D Trifecta:

- Unique contributions from each
- Effective government R&D must engage industry and academia
- Focus on and discuss who does what and leverage each other

Successful Cyber R&D Requires All Three Communities

Government
- Very good at 6.1, 6.2 – Long-term research
- Not good at 6.3 – Transition

Academia
- Good at “big improvements” using $$$$
- Not good at 6.3 – Transition

Industry
- Good at 6.3 – Transition
- Not good at 6.1, 6.2 – Long-term research
Why Is Cyberspace Critical to All of Us?

• *Our society, our country and the world relies upon it.*
• What are the dynamics of cyberspace? Global, ever-changing, all encompassing.
• What is the role that software engineering/cyber engineering plays in cyberspace? Foundational disciplines & BoK – the mind & the engine.
• How is this field of science unique and what impact does that have on how we approach R&D in this arena? Driven by the pace of technology – an operational, time sensitive dynamic not seen in other sciences.
• What major R&D work has been accomplished in the cyber assurance arena over the past ten years? Mainly focused on near term solutions.
• How should that work impact our R&D vision? Need to focus on key gaps that map to our unique skill-sets and capabilities.
• Where should we be focusing our efforts – the critical R&D gaps? Many opportunities – need to prioritize according to customer requirements and assurance imperatives.
• What is the perfect trifecta? It is a seamless and complementary partnership among industry, academia, and government.
Contact

Terry Roberts
Executive Director
ASP/Interagency and Cyber
Carnegie Mellon, SEI
Telephone: +1 703.908.8236
Email: twroberts@sei.cmu.edu

Web:
www.sei.cmu.edu
www.sei.cmu.edu/contact.cfm

U.S. mail:
Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

Customer Relations
Email: info@sei.cmu.edu
Telephone: +1 412-268-5800
SEI Phone: +1 412-268-5800
SEI Fax: +1 412-268-6257