Poster: Community Engagement for Cybersecurity Experimentation of the Future

David Balenson, Laura Tinnel
SRI International
Arlington, VA
{david.balenson|laura.tinnel}@sri.com

Terry Benzel
USC Information Sciences Institute
Marina del Rey, CA
tbenzel@isi.edu

***Abstract*—The ever-increasing cyber threat landscape demands new forms of advanced research and development coupled with new revolutionary approaches to cyber experimentation. SRI International (SRI) and USC Information Sciences Institute (USC-ISI) conducted the Cybersecurity Experimentation of the Future (CEF) study and produced a strategic plan and roadmap intended to catalyze generational advances in the field of experimental cybersecurity research [1]. These results represented the conclusions of our CEF study, conducted with broad participation by the cybersecurity research, research sponsor, and customer communities.**

USC-ISI, SRI, and the community have continued to advance the concepts behind the CEF study both through organized efforts such as the NSF Accessible Remote Testbeds (ART) Workshop [2] and the Sandia Workshop on Research Directions for Cyber Experimentation [3], and through the development of advanced experimentation infrastructure and capabilities.

Since the release of the CEF Final Report, the community has seen extensive growth in experimentation infrastructure, methods, and results across an ever-growing diversity of domains of interest. This proliferation of experimental infrastructures has matured the field beyond first generation *testbeds*. This diversity points to an increasing need for broad community engagement in order to realize transformational change as envisioned by the CEF study.

Consequently, SRI and USC-ISI launched the CEF Community Engagement Initiative. This large community undertaking will benefit from coordination, collaboration and establishment of open source development efforts. USC-ISI, SRI and colleagues have initiated work on the design of a CEF framework, development of a reference implementation, and establishment of community working groups. Central to expanding the CEF work is the engagement of the larger community, including research infrastructure developers, tool builders, and research experimental users. We are holding a series of Community Engagement Events in Spring 2018 and are in the process of establishing working groups that will jointly mature the CEF concepts as realized across the broad range of experimental infrastructure.

Keywords—cybersecurity; experimental research; research infrastructure; experimental methodologies and techniques; knowledge sharing; experimentation infrastructure; community

I. Introduction

Cybersecurity is a relatively young field. By nature, it focuses on worst-case adversary-driven system behaviors and rare events. This means that cybersecurity researchers must address a number of intrinsically hard challenges. Reliable research infrastructure is crucial to the cybersecurity experimentation process. It enables new research hypotheses to be tested, stressed, observed, reformulated, and ultimately proven before making their way into production environments.

The ever-increasing cyber threat landscape demands new forms of advanced research and development and in parallel new revolutionary approaches to experimentation. While the current state of the art in cybersecurity experimentation has recently had increased focus and investment, there is clearly a need for future research infrastructure that can play a transformative role for cybersecurity research well into the next decade.

Members of SRI International's Computer Science Laboratory (SRI) and the University of Southern California's Information Sciences Institute (USC-ISI) conducted the CEF study as a collaborative effort, with broad participation by members of the cybersecurity research, research sponsors, and customer communities. An Advisory Group, comprised of seven senior leaders from government, industry, and academia, helped inform and guide our work. Our current focus is on the CEF Community Engagement initiative as a step towards realizing the objectives of the CEF study.

II. Field of Experimental Cybersecurity R&D

It became clear at the outset of the CEF study that research infrastructure encompasses far more than just test apparatuses. Thus, the overarching finding of the study is that transformational progress in three distinct, yet synergistic, areas is required to achieve the desired objectives: (1) broad intellectual advances in the field of experimental methodologies and techniques, with particular focus on complex systems and human-technical interactions; (2) new approaches to rapid and effective sharing of data and knowledge and information synthesis that accelerate multi-discipline and cross-organizational knowledge generation and community building; and (3) advanced experimentation infrastructure capabilities and accessibility [1].

These three objectives point to a new direction for the field of experimental cybersecurity research and development. The importance of research into *the science of cybersecurity*

This material is based upon work supported by the National Science Foundation under Grant No. ACI-1346277 and ACI-1346285, and by the US Department of Homeland Security (DHS) Science and Technology (S&T) Directorate under Contract No. HSHQDC-16-C-00034 and HSHQDC-16-C-00024. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation or DHS, and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DHS or the US government.

experimentation is an overarching need. Any set of requirements or capabilities for cybersecurity experimentation must be backed by transformational progress in the science of experimentation. It is only by grounding our research in scientific methods and tools that we can realize the impact that experimentation can have. It should be noted that this call for research into the science of cybersecurity experimentation is different from the current fundamental research into the science of cybersecurity, though they are certainly complementary in their eventual goals. Along with establishing a field of research into the science of cybersecurity experimentation, substantial new approaches to sharing are needed in order to enable scalable, cross-discipline experiments. Needed new approaches to sharing include all aspects of the experimental science, from data, to designs, to experiments to the research infrastructure itself. In addition, cultural and social shifts in the way in which researchers approach experimentation and experimental facilities are needed. The final recommendation is that experimental facilities need new, advanced experimentation platforms that can evolve and are sustainable as the science and the community mature.

III. Community Engagement

SRI and USC-ISI have now embarked on Community Engagement Initiative to build and expand a community around the design, development, and deployment of CEF supportive infrastructures and tools for advanced cybersecurity experimentation. By its very nature the CEF community is multi-faceted. Our community efforts involve three groups:

- Research infrastructure builders/owners/operators
- Tool developers at the user, experiment, and infrastructure levels
- Experimental researcher user communities

We are focusing community engagement across three sets of activities:

- Community Survey
- Formation of a CEF Working Group
- Series of Community Engagement Events

Community Survey

USC-ISI developed a survey to help us first understand the range of community experimentation activities. The first order goal of the survey is aimed at understanding the degree to which researchers are undertaking experimentation, and if not why not. Following this line of inquiry are questions around understanding the kinds of research infrastructure being used, the benefits of the infrastructure, and the limitations. One area of particular interest is how the research community is conducting experimentation for scenarios that cross disciplines, such as cyber physical systems. Finally, the survey asks respondents about specific tools, methodologies, and any locally developed technologies that further their research experimentation.

CEF Working Groups

Development and operation of an overarching CEF framework will depend on an open source community effort. Initial design concepts explore the definition of API's for multiple testbed "resource providers" to contribute resources for experimentation, policy specification and controls for sharing of research infrastructure, tools, and data, and a myriad of user interface and accessibility options for designing, developing, and controlling experiments. Ongoing working groups (similar to IETF working groups) will provide the community engagement needed to address these issues and develop standards and early reference implementations.

Community Engagement Events

Community engagement is best fostered through shared initiatives and collaborative research and development. We seek to foster the connection of the right people through a series of Community Engagement Events. These events will take place over the Spring/Summer 2018. Each event will include presentation of concepts and plans, design concepts for a core CEF testbed that will build on an ISI design as the "stake in the ground" for starting the discussion, and discussion of cross-testbed experimentation. A key aspect of each event will be hands on sharing and collaboration that will foster ongoing working group activities.

IV. Conclusion

An emphasis on increasingly diverse infrastructure alone will fall far short of achieving the transformational shift in research and the supporting experimentation required to address cybersecurity in the rapidly changing cyber environment. Our fundamental conclusion is that a community-based approach to achieving strong, coupled, and synergistic advances across each of the CEF study areas outlined above will move the field beyond today's state of the art. Taken together, the three areas of community engagement provide a path for a new generation and community of experimental cybersecurity research – one that offers powerful assistance in helping researchers shift the asymmetric cyberspace context to one of greater planning, preparedness, and higher assurance fielded solutions.

References

[1] D. Balenson, L. Tinnel, and T. Benzel, Cybersecurity Experimentation of the Future (CEF): Catalyzing a New Generation of Experimental Cybersecurity Research, July 31, 2015. (http://www.cyberexperimentation.org/report/)

[2] M. Egerstedt and M. Govindarasu, Access Accessible Remote Testbeds: Opportunities, Challenges, and Lessons Learned, Workshop Report. (http://gritslab.gatech.edu/home/wp-content/uploads/2016/03/2015-Workshop-Report-Accessible-Remote-Testbeds-Opportunities-Challenges-and-Lessons-Learned.pdf)

[3] E. DeWaard, C. Deccio, D. Fritz, T. tanner, Research Directions for Cyber Experimentation: Workshop Discussion Analysis, Sandia Report, SAND2017-10965, October 2017. (https://www.osti.gov/scitech/biblio/1399831)

SRI International

Community Engagement for Cybersecurity Experimentation of the Future

USC Viterbi
School of Engineering
Information Sciences Institute

David Balenson[1], Laura Tinnel[1], and Terry Benzel[2]
[1] SRI International, Arlington, VA {david.balenson|laura.tinnel}@sri.com
[2] USC Information Sciences Institute, Marina del Rey, CA, tbenzel@isi.edu

BACKGROUND & MOTIVATION

Research Infrastructure for Cybersecurity Research

- Cybersecurity R&D relatively young field
- Intrinsically hard challenges
  - Worst case behaviors and rare events
  - Multi-party and adversarial/competitive scenarios
- Research infrastructure is crucial
  - New hypotheses tested, stressed, observed, reformulated
- New forms of R&D and new revolutionary approaches to experimentation

KEY FINDINGS

Transformational Progress in Three Synergistic Areas

1) Fundamental intellectual advances in experimental methodologies
2) Rapid and effective sharing of data and knowledge and information synthesis
3) Advanced, accessible experimental infrastructure capabilities

Research Infrastructure is More Than Infrastructure

- Scientific methodologies, experimental processes, and education are critical to effective use of machines and tools

RI > I

CEF COMMUNITY ENGAGEMENT INITIATIVE

- Driven by SRI International and USC-ISI collaborative team, supported by DHS S&T
- Engage academic, industry, and government organizations

Research infrastructure builders/owners/ operators

Tool developers at the user, experiment, and infrastructure levels

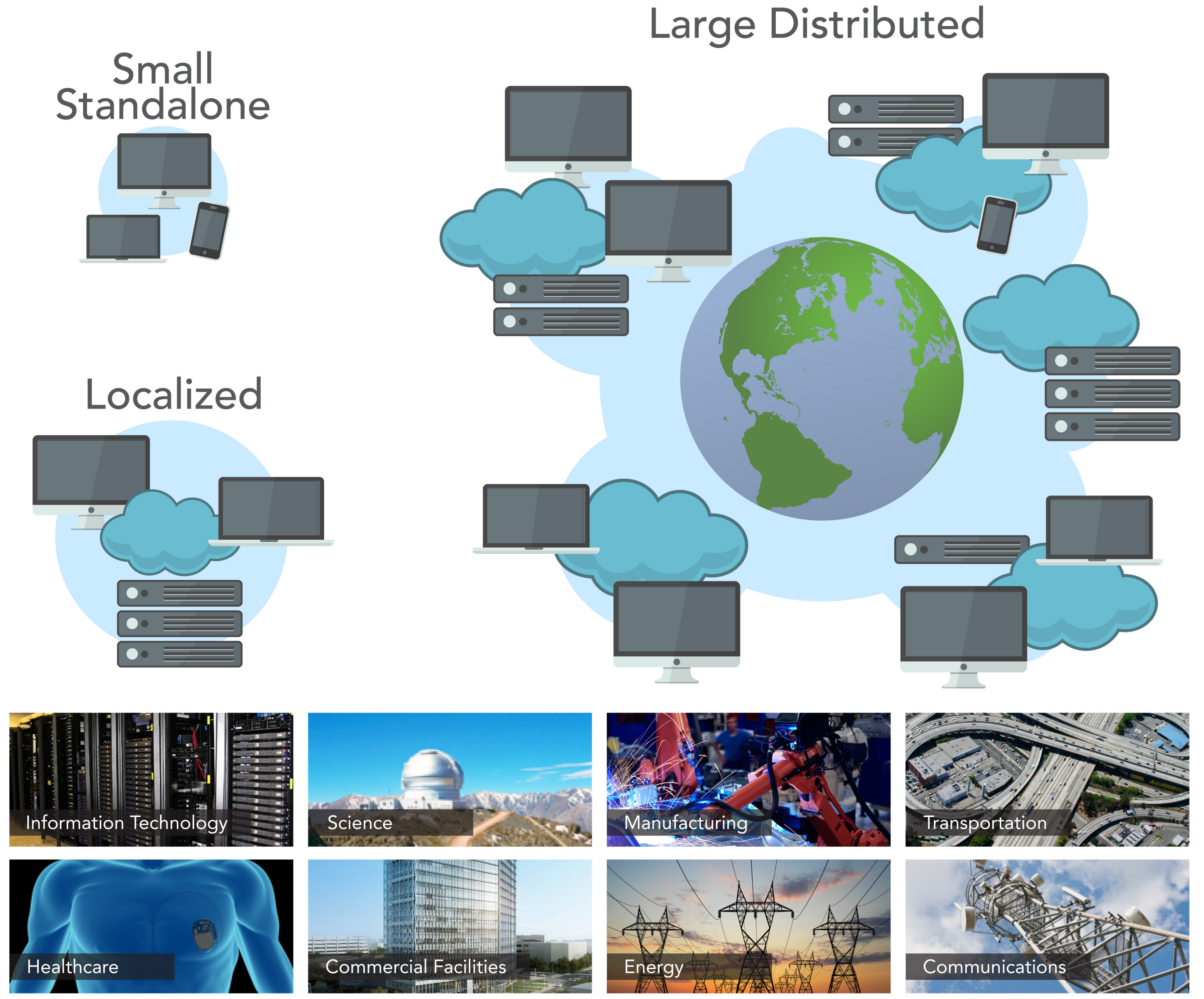
Experimental researcher user communities

Series of Community Engagement Events

Connect with key stakeholders, including infrastructure providers, tool developers & users, and researchers

- Discussion of cross-testbed experimentation
- Hands on sharing and collaboration to foster ongoing activities
- Present CEF vision, concepts, and plans
- Propose design concepts for core CEF testbed built on USC-ISI design to start the discussion
- Events will take place over Spring/Summer 2018

DIFFERENT CAPABILITIES SPANNING MULTIPLE DOMAINS



CEF COMMUNITY ENGAGEMENT INITIATIVE

Community Survey

Understand the range of community experimentation activities

- Degree to which researchers are undertaking experimentation, and if not why not
- Kinds of research infrastructure, its benefits, and the limitations
- How experimentation is conducted for scenarios that cross disciplines, such as CPS
- Specific tools, methodologies, and locally developed technologies

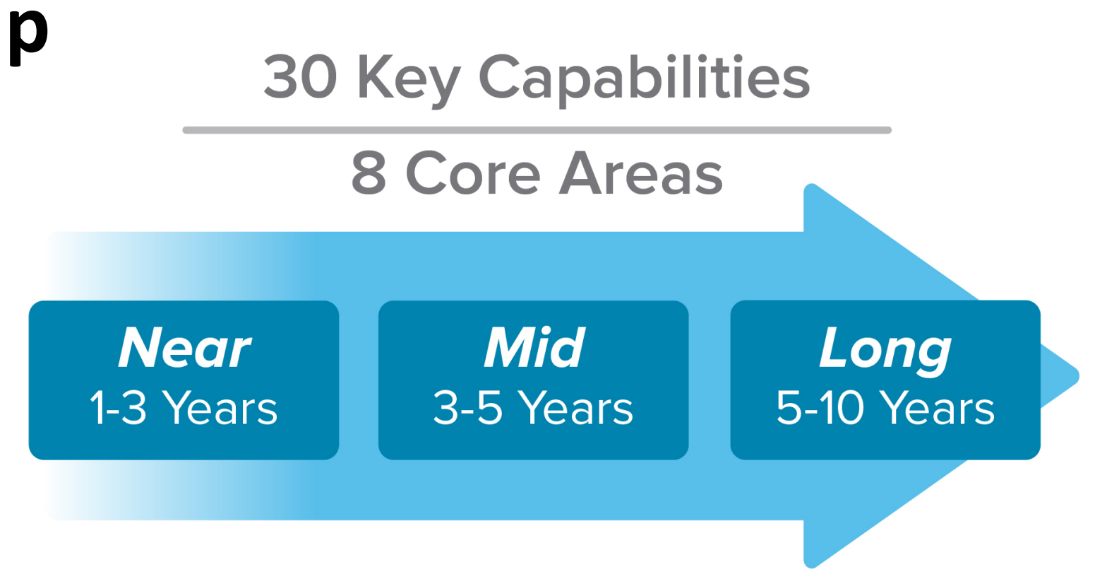
Formation of CEF Working Groups

Open community effort to develop overarching CEF framework

- Develop standards and early reference implementations
- Define API's for multiple testbed "resource providers" to contribute resources for experimentation
- Define user interface and accessibility options for designing, developing, and executing experiments
- Adopt mechanisms for sharing infrastructure, tools, and data

CEF ROADMAP

Strategic Plan & Enabling Roadmap



- Requirements, objectives and goals over 3 phases
  - Some build upon each other and others require new fundamental research over a long time period
- Key capabilities consider:
  - Current experimental cybersecurity research and supporting infrastructure
  - Other types of research facilities
- The roadmap presumes advances in key computer science disciplines
  - Ontologies, meta-data, libraries, and corresponding resource discovery

Download CEF Roadmap from: www.cyberexperimentation.org

FUTURE IMPACT

Science of Cybersecurity Experimentation

Source: https://www.nsa.gov/research/tnw/tnw192/article4.shtml

- New direction for field of experimental cybersecurity R&D
- Scientific methods and tools to fully realize impact
- Complementary with science of cybersecurity
- Share aspects of the experimental science – data, designs, experiments, and infrastructure
- Cultural shift in the way researchers approach experimentation
- Experimental platforms that evolve and persist as science and community mature

Future Cyber Experimentation Environments

- Shared, vetted capabilities as a solid foundation
- Reduce the time and money spent building one-off environments
- Vetted components and tools will improve experimental quality

Community Engagement for CEF envisions a new generation of experimental cybersecurity research – one that offers powerful assistance in helping researchers shift the asymmetric cyberspace context to one of greater planning, preparedness, and higher assurance fielded solutions

This material is based upon work supported by the National Science Foundation under Grant No. ACI-1346277 and ACI-1346285, and by the US Department of Homeland Security (DHS) Science and Technology (S&T) Directorate under Contract No. HSHQDC-16-C-00034 and HSHQDC-16-C-00024. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation or DHS, and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DHS or the US government.

NSF
Homeland Security
Science and Technology