SANDIA REPORT
SAND2017-10965
Unlimited Release
Printed October 2017

Research Directions for Cyber Experimentation: Workshop Discussion Analysis

Elizabeth DeWaard, Circuit Media

Casey Deccio, Brigham Young University
David Fritz, Sandia National Laboratories
Thomas Tarman, Sandia National Laboratories

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: http://www.ntis.gov/search

SAND2017-10965
Printed October 2017
Unlimited Release

Research Directions for Cyber Experimentation: Workshop Discussion Analysis

Prepared by:
Elizabeth DeWaard
Circuit Media
elizabeth@circuitmedia.com

Program Committee:
Casey Deccio, Brigham Young University
David Fritz, Sandia National Laboratories
Thomas Tarman, Sandia National Laboratories

From notes provided by:
Christopher J. Symonds, Cyber Systems Assessments
cjsymon@sandia.gov

Thomas D. Tarman, Emulytics Initiatives
tdtarma@sandia.gov

Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-MS0671

Abstract

Sandia National Laboratories hosted a workshop on August 11, 2017 entitled "Research Directions for Cyber Experimentation," which focused on identifying and addressing research gaps within the field of cyber experimentation, particularly emulation testbeds. This report mainly documents the discussion toward the end of the workshop, which included research gaps such as developing a sustainable research infrastructure, expanding cyber experimentation, and making the field more accessible to subject matter experts who may not have a background in computer science. Other gaps include methodologies for rigorous experimentation, validation, and uncertainty quantification, which, if addressed, also have the potential to bridge the gap between cyber experimentation and cyber engineering. Workshop attendees presented various ways to overcome these research gaps, however the main conclusion for overcoming these gaps is better communication through increased workshops, conferences, email lists, and slack channels, among other opportunities.

ACKNOWLEDGMENTS

The 2017 Research Directions in Cyber Experimentation committee would like to thank the following individuals for their help in organizing and running this year's workshop:

- Jeff Boote, Zach Benz, and David White for their guidance, support, and funding,
- Lynde Farhat-Corbett, Tara Olsen, Stephani Pease, Megan Sabo, and Jenni Hidalgo for organization and logistical support, and
- Chris Symonds for his detailed workshop notes

And we would especially like to thank the following workshop presenters:

- David Balenson, SRI
- Terry Benzel, USC ISI
- Ryan Goodfellow, USC ISI
- Steve Schwab, USC ISI
- Rob Ricci, University of Utah
- John Floren, Sandia
- Ron Minnich, Google
- Steven Elliott, Sandia
- Jon Crussell, Sandia

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Research Directions for Cyber Experimentation workshop brought together experts in the cyber experimentation community to discuss several topics relating to understanding and fulfilling user needs and determining and overcoming research gaps. Its purpose was to examine research directions and address current challenges the cyber experimentation field faces. The workshop built upon previous work[1] that identified lack of communication, accessibility, and a research infrastructure as current shortcomings in the field if cyber experimentation. Their discussion centered around proposing solutions to these challenges in order to move their field forward.

The workshop consisted of seven presentations from varied topic areas. Though the topics were diverse, they shared a common theme of recognizing research gaps and current ways they are being addressed. Presentations were followed by a thorough discussion period, in which workshop attendees were presented four questions (discussed in detail in this report): What are the user needs?, How can the user select the right tool for the experimental question?, What are the research gaps?, and How can [developers and researchers] address the gaps? These questions were intended to provide a launching point and guidance for the discussion. These questions were addressed in the presentations and revisited throughout the workshop discussion.

Workshop attendees determined that in order to move the cyber experimentation field forward, a sustainable infrastructure must be developed. They cited a current lack of this foundation as central to many of their current research gaps. Developing a more fine-tuned infrastructure and foundation for their field would allow for cyber experimentation that is increasingly rigorous and sustainable. This requires a balance between standardization and innovation, so that infrastructure development addresses users' needs while pushing the state of the art. Attendees worked to understand and identify user needs to better inform their experiment and tool design. Understanding one's users allows researchers and developers to create tools that are better accessible to users who may not have a cybersecurity background.

Much of the workshop was focused on cyber experimentation testbeds, particularly emulation testbeds, and associated research gaps. Researchers and developers require tools that are tested thoroughly but are also predictive of real world systems. Accomplishing many of the research gaps expressed in the workshop requires increased communication and collaboration within the cyber experimentation field. Workshop attendees recommended conferences, workshops, mailing lists, and slack channels as ways to promote communication. By doing so, members of the field can build a community-based research infrastructure organically. Overall, the workshop offered many solutions and next steps for expanding the cyber experimentation field, which are examined within this report.

[1] http://www.cyberexperimentation.org/report/

NOMENCLATURE

Abbreviation	Definition
CEF	Cyber Security Experimentation of the Future Report
DETER	Defense Technology Experimental Research
LDRD	Laboratory Directed Research and Development
QUE	Quantify Uncertainty in Emulations

1. INTRODUCTION

On August 11, 2017, Sandia National Laboratories hosted a workshop entitled Research Directions for Cyber Experimentation, where leaders and experts in the field of cyber security experimentation met to discuss critical advances, research gaps, and future direction of their field. Sandia invited speakers to submit abstracts of their chosen topic area for selection and presentation at the workshop. Tom Tarman and David Fritz, of Sandia, and Casey Deccio, of Brigham Young University, organized and led the workshop and discussion that followed. The purpose of the workshop was to gather cyber security experts to discuss present research challenges for cyber experimentation frameworks (particularly emulation environments). The workshop centered around the idea that the field of cyber security requires a framework or infrastructure in order to provide users tools that can be used to rigorously and safely evaluate systems before implementation and operation. In the workshop introduction, the following objectives were identified: safe and secure experimentation, rigorous methods and defensible results, and predictive multi-fidelity modeling with validated applicability to the real world. With these needs in mind, workshop organizers aimed to promote information sharing, identification of unmet needs and research gaps, and how to address and mitigate these gaps.

1.1. Cyber Experimentation of the Future (CEF) Report

Since release of the Cybersecurity Experimentation of the Future (CEF) report in 2015, the cyber experimentation field has grown to adopt some of its key findings.[2] The report identified several objectives, including information sharing between groups and stakeholders, further experimental methodologies, and advances in experimental capabilities. This report inspired the need for this workshop to revisit and expand upon its core ideas. The report offers five recommendations to the field, which the workshop addressed throughout the day:

1. Domains of applicability;
2. Modeling real world for scientifically sound results;
3. Frameworks and building blocks;
4. Experiment design and instillation; and
5. Meta-properties.

These recommendations aim to transform the field into one that is grounded in the scientific method with a strong foundational infrastructure, is accessible and community based, and allows for extensive cyber experimentation.

1.2. Workshop Format

The workshop format included eight presentations around the central focus of determining the research directions of their field. The presentations were followed by a discussion period, where discussion questions were raised and a synthesizing of ideas

[2] http://www.cyberexperimentation.org/report/

could take place. This report mainly documents the discussion period that occurred at the end of the workshop. The following discussion questions were presented to attendees:

1. What are the user needs?
2. How can the user select the right tool for the experimental question?
3. What are the research gaps?
4. How can [developers and researchers] address the gaps?

These research questions will be examined in detail in this report based upon the discussion and presentations from the August 11 workshop. Each section addresses a specific discussion question and a focus on next steps discussed during the workshop. The presentation slides will be made available by Sandia National Laboratories.

2. USER NEEDS

2.1. Determining and Understanding User Needs

The first discussion topic asked the question: What are the user needs? Understanding and identifying user needs is central to the challenge of moving the cyber experimentation field in directions that users and decision makers find useful. In order to determine which direction the field should grow, cyber experts should look to their users' needs, challenges, the experimental questions they wish to ask, and desired outcomes and decisions. User needs vary; from being better able to select a tool that fits their needs, having a tool that is matched to their skill level, or a tool that has been simplified to "point and click" functionality.

Participants of the Research Directions for Cyber Experimentation workshop recognized that user needs change based on many factors. The discussion evolved from establishing every user need, since they may be infinite, and shifted toward ways to better understand users. Acknowledged by many at the workshop, a researcher or developer must first understand their various users, then understand the diverging needs of these users. User bases are diverse in nature, from university academics to network researchers, and require a targeted system, program, or tool. Users may have differing levels of technological adeptness, as one user may be an expert and another may be a student. Researchers and developers might need to balance between making something usable by "super" users and creating something "point and click" accessible to a more general audience. Identifying this before or during the experimentation and building process will ensure tools are operational and approachable by every intended or potential user.

In addition to understanding diverse user needs, one must recognize how those needs differ from a researcher or developer's needs. As users are implementing these tools in real-world applications, they may have an inherent focus upon cyber engineering (operational, finished products), rather than cyber experimentation (testing and evaluation phase). With their focus on operational functionality, these users require tools that are real-world applicable. However, some users may be more interested in the experiment itself and how it is designed, and less concerned with the "busy work" of model construction. These users would benefit from a set of model libraries that are actively maintained.

2.2. Understanding How Users Apply Specific Tools

Understanding how a user applies a specific tool is equally as important as understanding your user. As mentioned above, users want approachable, usable tools. Model results and conclusions can be invalidated when users struggle to determine which tool to apply and when. In order to move forward, researchers and developers must be cognizant of how the user utilizes different tools, hardware, or software, and help users select and apply the right tools. Sometimes, the intended use may not match the operational use. The tool designer may aim for it to be used in a specific way and build the program or system to correspond with that objective; however the user may

apply it in a completely different way and produce results that were not desired. In this regard, there are a few approaches researchers and developers may take:

1. Anticipating their user's desired outcomes to create something that is broad and wide-reaching in its use and outcomes; or
2. Creating a tool in which its use and outcomes are clearly defined, while avoiding standardization.

3. HELPING USERS SELECT THE CORRECT TOOL

3.1. Educational Support

At the workshop, attendees identified education as a key way to bridge the gap between user needs and what researchers and developers are providing in order to help users select the right tool. A focus on education will alleviate differing levels of skill or technological adeptness, effectively making it easier for researchers and developers to create tools that are more wide-reaching. Bringing users to a higher level of understanding will increase a developer's ability to create tools aimed toward a few sets of specific users, rather than many. Therefore, tools become more accessible and work to ensure "super" and sophisticated users are not alienated by a tool that is too simple.

Education can be used as an empowerment tool to move the field in a desired direction. Not only does it offer the capability to grow users' abilities and gain information based on their trial and error of different tools, but developers and researchers in the cyber security field can also use education as a way to grow their field in a structured, yet organic way. Growth may be structured through a formal classroom setting or through applying the scientific method rigorously. However, growth may also be organic by applying a bottom-up approach to learning and advancement of the field. Education is a way to invest in the field and promote growth by creating a more inclusive ecosystem of users and developers that encourages the spread of knowledge.

The presentation "The Science of Cyber Security Experimentation: The DETER Project and Beyond" discussed how education is currently promoted by the DETER project, started by the University of Southern California's Information Sciences Institute (ISI).[3] The DETER project, a testbed experimentation facility for cyber researchers, is a controlled study of large, complex networks that allows experimentation and emulates real-world applications. The project focuses primarily on research, but also invests in community and education-based knowledge sharing. It actively supports classes and other furthering education opportunities. The principal participants are university, high school, and international students, who are provided hands-on experience using and testing real-world systems. They are exposed to real attacks and targets, rather than simulations.

Through testing and experimentation with these tools, the students identify any pain points and allow tool developers to understand what should be troubleshot or re-designed. Weaknesses or limitations are identified earlier in the process, rather than when a particular tool is launched. The benefits are twofold:

1. Users receive expert-led educational opportunities; and
2. Experts receive valuable user feedback and a population to actively test their tools prior to their release for operational use.

[3] https://deter-project.org/

This exemplifies only one approach to increasing educational support throughout the cyber security community. There are many other informal ways to increase education, understanding, and expertise within this field, as discussed in the workshop.

3.2. Accessibility

Accessibility was a recurring theme during the workshop talks and discussions. Accessibility within the field of cyber experimentation means making tools that are understandable and easy to use, even by non-experts, while ensuring they maintain high levels of integrity and validity. As many users require tools that are understandable and translatable to suit their varied needs, workshop attendees recognized that this is an area of need for their field.

3.2.1. Creating Usable, Valuable Tools

Making usable tools and recognizing a user's skill level are complimentary. Accessible cyber experimentation testbeds require a design that focuses on an intended or possible users assumed or known technological skill level or field expertise. Knowing one's users allows for a better design outcome. If testbeds are built inaccessibly, their productivity and usefulness levels diminish. Designing tools with a usability in mind is central to accessibility and ensures that tools are not only usable but also produce the desired outcomes and results.

3.2.2. Building a Terminology Lexicon

A number of the workshop attendees expressed a desire for a well-defined terminology lexicon, in both a formal and informal sense. The central idea of this being the sharing of knowledge and converging of opinions on what terms and ideas mean within the field. This acts to add rigor to the field and minimize misunderstanding and misuse. Since the field is young and still maturing, this is a necessary step to increase its legitimacy as a science-based field. A well-defined lexicon will promote well-informed, common understanding for everyone within the field, from experts to students, and help protect against misuse.

3.2.3. Promoting a Broader Understanding

A broader understanding of the cyber security field encompasses the earlier ideas of making usable tools and building a terminology lexicon, but as the idea implies, extends beyond them as well. However, what a 'broader understanding' means differs between every person and is hard to define in exact terms. Some potential ideas were presented during the workshop, such as more educational opportunities or increased conferences that promote networking and idea sharing. No matter how these manifest themselves in the community and academic field, they act to further the overall accessibility and promote knowledge-sharing.

3.3. Improving Understanding of Users' Needs

Workshop attendees discussed a (real or perceived) disconnect between developers and users. Developers may be removed from their users, therefore may not know their needs or what issues they are trying to overcome. The workshop offered three potential solutions for better understanding users.

The first is the idea of a more community-based approach to experimenting and developing tools. Actively engaging with a user community allows the developer to gain intimate knowledge of a user's needs and concerns. This may manifest itself in ways similar to the DETER project's emphasis on hands-on student interaction with real-world tools or a form of 'market research' where developers gather information on their intended or potential users to inform their design. However, this may not be possible in all instances and workshop participants acknowledge that user needs can be hard to anticipate.

Therefore, instead of anticipating each user need, a second solution may involve a developer focusing on engaging a more targeted user group, allowing them to build to this group's identifiable needs. By attracting a more appropriate user group, misuse and misunderstanding will be mitigated as the tool better fits their needs.

A third way to better understand user needs is to encourage collaboration between co-interested groups to define their needs together. Since they have similar interests and goals in applying a specific tool, streamlining their needs allows developers to create a more robust and productive tool overall. In general, workshop attendees focused on their role in improving the way users are understood in order to make experimentation and tool design more productive and effective for everyone within the cyber security field. The workshop demonstrated a clear effort to emphasize understanding user needs.

4. RESEARCH GAPS

Growth in the cyber experimentation field is increasing rapidly; however, workshop attendees expressed concern that growth may be misdirected and constrained due to several pressing research gaps. The workshop worked first to identify present research gaps in order to alleviate those strains. The following research gaps apply to advances in tools and experiments in the field that have yet to be created or are more methodological or philosophical in nature. The research gaps are diverse, yet share a common goal of building a more robust and prolific field of cyber security experimentation through adequately addressing these gaps. This section discusses particularly pressing research gaps the group addressed, though many others exist.

4.1. Research Infrastructure

The workshop described methodological and philosophical gaps within the field of cyber security as *meta gaps*, where the field at large lacks a foundational base to grow from. The workshop identified the absence of a foundational research infrastructure as a major limitation to growth within the cyber security field. Widely accepted methodologies or best practices are still being derived and founded, putting current developers and researchers at a disadvantage since they lack the fundamental basis that takes time to manifest. The workshop conceded that the field is still emerging as compared to other science fields that have existed for centuries. This lack of a foundation proves detrimental to helping the cyber community better understand this field. Attendees hypothesize that conducting meta-research will increase researcher effectiveness to perform testing and evaluation. Developers may be operating at different levels of expertise due to this research gap. This does not refer to their skill-level, but rather refers to the lower maturation of the field at large. One of the key ideas gained from the discussion on research gaps is that encouraging the field to flourish in the right direction and promoting a shared knowledge requires a strong infrastructure to guide that growth. Attendees hypothesize that conducting meta-research will increase researcher effectiveness to perform testing and evaluation.

4.2. Expanding Cyber Experimentation

A principal research gap is the ability to rigorously test and experiment to reach specific results. Addressing this gap would allow for more verifiable and defensible results since they were tested more rigorously. In the workshop, attendees expressed a desire to apply the scientific method more precisely and critically to produce valid results that better support decision makers' needs. Advances may include tools that smoothly transition from the virtual to real world, better methodologies and approaches, and/or more rigorous and thorough testing before application. Filling these research gaps would allow developers and researchers to use testbeds to host specific experiments that simulate real-world applications in a more complex and complete way.

4.2.1. Limitations

A current limitation to expanding cyber experimentation ties specifically to user needs, namely their need for cyber engineering rather than cyber experimentation. At times,

engineering comes before understanding. An example of this given in the workshop is developers trying to solve today's problems with yesterday's solutions. If a system is built prior to a rigorous understanding of its challenges or potential flaws, developers and users place themselves at a disadvantaged position for solving its complex issues. Attendees believe that increased experimentation will allow developers to rigorously test first and engineer later. However, results from the experimentation process may take time to produce desired engineering results.

Another limitation researchers face is the challenge of maintaining and continuing projects beyond the originally funded portion of the project. Keeping projects sustainable requires further funding and resources from sponsors. This is one way where cyber experimentation meets cyber engineering. Once the tool is developed, it requires maintenance such as hardware upgrades and system updates and improvements, which is typically considered engineering. Workshop attendees expressed that getting the attention of sponsors is a key way to overcome this limitation.

4.3. Uncertainty as a Variable

Cyber experimental (e.g. emulation) models operate under a certain level of uncertainty regarding its correspondence to the real-world system it is modeling. This uncertainty may be *epistemic*, where the uncertainty is due to limits in the knowledge about how a real-world system operates, or *aleatory*, where the uncertainty is due to inherent randomness. There are many sources of epistemic uncertainty in cyber experimentation, including configuration parameters, model assumptions, and model fidelity, among others. Uncertainty also applies to adversarial threat models, and the challenges developers and users face defending those threats. Additionally, researchers face limitations on how to quantify and convey uncertainty in their results. Therefore, it presents a significant research gap that has yet to be overcome.

The goal of emulation testbeds is to model certain environments to allow for testing and experimentation; however there is no guarantee it will translate from the virtual to the real world. This points to an on-going research need in methods to check the validity of emulation models. And while advances have been made to attempt to reduce uncertainty, methods for quantifying residual uncertainty are needed. Workshop attendees reflected on ways uncertainty limits their work, how they can better express uncertainty in their results, and the immense challenges in overcoming this research gap.

5. ADDRESSING THE RESEARCH GAPS

In order to overcome these and other research gaps, the workshop examined concrete ways to address these gaps and ways they are currently doing so. Since the research gaps are numerous and diverse in nature, so were their proposed remedies. However, in the workshop two ideas repeatedly presented themselves: building a distinct research infrastructure and improving cyber experimentation methodology. Nearly each presentation centered on these ideas of building a foundation for moving forward and then expanding and advancing how cyber experimentation takes place. Another central focus was strengthening the community within the field, which is discussed in the next section, Next Steps.

5.1. Research Infrastructure

Building a research infrastructure, defined as a meta gap, requires developers to determine what fundamentals are crucial to the field of cyber security since these fundamentals will guide the field into the future. Taking on this significant challenge appears to be on the forefront of the field's conscience. These fundamentals are more than hardware, software, and tools, they include standards and methodologies determined to be essential to the field. However, concrete specification of these standards and methodologies should be avoided because it could impede innovation. Standardization could interfere with innovation and lead to *bit rot*, or abandoned code, because test and application environments are constantly evolving faster than standards can track. Similar to restricting a tool to only one use, the research infrastructure needs to be broad in nature in order to promote growth instead of constrict. Instead, this infrastructure should promote innovation by providing development methodologies that are flexible and adaptable to many applications.

Current infrastructure has focused on creating tools and foundations users can apply to build informed experiments. One solution is increasing the capability of testbeds and using them to guide the design of experiments. Testbeds are platforms that allow for testing and experimentation in a safe, controlled environment. The idea of *Interactive Realization* was discussed in the workshop, which allows the testbed to guide the experiment design by providing a foundation to build upon, rather than an experimenter starting from the ground up. Though almost philosophical in nature, workshop attendees are currently taking steps to address this gap in real, substantial ways. One example discussed in the workshop is CloudLab. CloudLab is a current testbed that provides users a foundation for building models of their cloud programs that are easily tested and customized prior to launching.[4] A user selects a system and chooses a set of parameters and the program will then provide users with a topology of their system. This flexible system is a platform that reduces risk and encourages innovation because it acts as a guide, rather than a strict set of guidelines. Other foundational structures are still being built and workshop attendees focused on what next steps they should take, discussed in the next section.

[4] https://www.cloudlab.us/

5.2. Advances in Cyber Experimentation to Limit Uncertainty

The workshop centered around determining the direction and development of cyber experimentation. Expanding the field to include new areas and approaches is vital to innovation and growth. This requires methodological and technological advances. Creating new methodologies will expand how researchers and developers can conduct experiments, from simple things such as developing better ways to measure results to groundbreaking ways to accomplish goals and address complications. Many within the community have already begun addressing this gap in diverse ways. One such example is the DETER project's DETERLab.[5] This facility is a platform for modeling and emulation with a specific focus on cyber security experimentation and testing. The lab's focus is expanding cyber experimentation to produce valid and verifiable outcomes that lead to implementable tools. The lab also has an innovative and unique human-centered approach to experimentation to addresses how human behavior affects certain outcomes. Through its human modeling tools, the lab gains a more vigorous understanding of their experiment. This multi-faceted approach represents how the field is changing to encompass new areas. Expanding cyber experimentation to include a human element makes it more realistic and translatable to the real world, as adversarial actions and human impact is taken into account within the experimentation phase.

Another example of an expansion in cyber experimentation discussed in the workshop is Staghorn, an analysis platform developed by Sandia that helps users identify problems and debug systems through taking a full-system snapshot. This snapshot is taken per the user's specifications or selected trigger (time or packet based). Instead of running a program only to have it malfunction, Staghorn allows users to operate in an offline mode to examine their system thoroughly and without risk. This approach represents an expansion within cyber experimentation, giving users, researchers, and developers capabilities they did not have previously.

Improved cyber experimentation methodologies may also diminish uncertainty. Allowing experiments to be tested securely and rigorously, researchers and developers can better anticipate variables that were once uncertain. Cyber experimentation testbeds are crucial to cyber experimentation since they allow researchers to more rigorously test their experiments before releasing them for operational use. The degree of uncertainty within emulation testbeds is currently being addressed through the Laboratory Directed Research and Development's (LDRD) project Quantify Uncertainty in Emulations (QUE). The purpose is to expose how emulation testbeds differ from the real world to aid in understanding its appropriate application, which is critical to making emulation more useful to cyber experimentation. Uncertainty will always play a role, but workshop attendees recognize ways they can act to minimize its impact and limitations.

[5] https://www.deterlab.net/

6. NEXT STEPS

The final part of the discussion emphasized concrete next steps to realizing the themes and ideas discussed during the workshop. It asked the question that given all of these challenges and ideas, where does that lead the attendees and field as a whole? The people gathered in the workshop share a common goal of determining what steps should be undertaken to realize these changes. The group discussed several next steps, but the overwhelming consensus was the need for more collaboration. Attendees expressed a perceived lack of opportunities within their field to share ideas, knowledge, and breakthroughs. They suggested that the fragmented nature of their field is hindering growth and innovation, since they lack avenues to work collectively toward solving a research question or overcoming complications and setbacks. Currently there are opportunities to meet annually or bi-annually, but more opportunities are needed to move the field forward constructively.

One way to encourage collaboration is through future workshops, networking events, and collaborations between stakeholders and groups in the cyber security field. Tele-conferences were also discussed as a possibility to make it more widely accessible. Slack channels and mailing lists were suggested as ways to sustain communication between conferences. This works to build a community base that is founded on knowledge-sharing. Another proposed solution is designating user groups to connect disparate testbed communities. This idea provided attendees with an action item: creating a cyber experimentation mailing list to connect user groups virtually to promote communication, collaboration, and knowledge-sharing. These user groups can be further broken down into sub-groups with a specific focus to better reach their goals.

Attendees of the workshop were realistic in recognizing that the field is not going to evolve overnight and that the field is constantly changing. But in identifying user needs and research gaps and determining ways to lessen those gaps and fill the needs, they came one step closer to accomplishing those goals.

DISTRIBUTION

1	MS0899	Technical Library	9536 (electronic copy)


Sandia National Laboratories