Project Summary

Effective cybersecurity experiments are challenging to today's network testbeds for a number of reasons. Examples of these are:

- **Scale** - experiments that involve complicated composite behaviors, rare event detection and emergent effects may need to be quite large and complex to be accurate or indicative.
- **Risk** - cybersecurity experiments by their fundamental nature may involve significant risk if not properly contained, yet these experiments may well require *some* degree of interaction with the larger world to be useful.
- **Multi-party nature** - many interesting cybersecurity experiments involve more than one logical or physical party, due to the challenge-response nature of the problem as well as the distributed, decentralized nature of the networked systems environment.

We address these challenges with a suite of transformational advances to today's state of the testbed art, which taken together move the concept of "testbed" from simple hardware infrastructure towards powerful and effective user-oriented facility.

Central to the proposal is our work in three synergistic research areas:

- A unique model for *risky experiment management*; enabling researchers to carry out experiments that interact with their larger environment while retaining both control and safety.
- A model and structure for *experiment health monitoring;* which ensures that the underlying conditions and invariants required for an experiment to be valid do in fact hold.
- A model and mechanism for *dynamic federation*; which allows different testbed facilities to come together on demand to support large-scale, complex, heterogeneous, multi-party experiments.

To synthesize our area-oriented research results into a coherent and easily accessible whole, we develop new abstractions and functions for our SEER experiment control toolkit. With these new capabilities in place, SEER will allow users of widely varying sophistication to carry out activities ranging from structured undergraduate education to research experiments with order-of-magnitude increases in complexity over those possible today.

Complementing our research plan is an integrated outreach and education program explicitly designed both to catalyze significant advances in cybersecurity R&E and to provide in-depth feedback to the technical research and development program. The integration of this program and our technical work plays a central role in the structure of our project.

The **intellectual merit** of the work lies in a) the concept and capabilities of our proposed model for risky experiment management; b) in the design of our experiment health monitoring system, its ability to ensure that experiments of significant complexity can be relied on to proceed correctly and produce accurate results, and the contributions of the research to the larger problem of management in highly decentralized networks; and c) in our approach to dynamic federation, which has been shown in early form to support large experiments across multiple Emulab-style testbeds, and will in fully developed form do so while supporting a rich set of user and testbed technical and policy requirements, including those of risky experiment management and experiment health monitoring. Further intellectual merit lies in the integration of these capabilities and in improved understanding of how such capabilities can most effectively be made available to the researcher.

The **broader impact** of the proposed effort is, in the first instance, to significantly alter the nature of experimental academic research throughout cybersecurity and networking, by enabling order-of-magnitude or more increases in experiment scale, complexity, and scope. A further impact is the potential to advance the *methodology* of cyber-security education, by enabling a curriculum based on large-scale sharable facilities and increasingly sophisticated and realistic structured exercises. Beyond the cyber-security R&E community, the broadest impact of the work lies in its potential to alter the landscape of security in real-world cybersystems, now some of the most critical infrastructures of modern society.