This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2018-11623C

Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper

Vincent E. Urias, William M.S. Stout, Brian Van Leeuwen, and Han Lin

PRESENTED BY

Will Stout

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.

BACKGROUND

Cyber networks are extremely non-deterministic, complex systems.

To address this, we must develop foundational research protocols to enable reproducible cyber experiments that can systematically uncover deep understanding of a cyber system's security posture

BACKGROUND

Cyber ranges are quite valuable to not only understand the effects of cyber attacks, but also to provide fertile ground to train future cyber defenders; however, further areas in the experiment life-cycle should be considered.

Impetus for this position was based on multi-year studies, which culminated in:

- Gaps
- Challenges
- Feasibilities

THE PATH TO CYBER EXPERIMENTATION

Security practitioners require training systems that adequately reflect the environments they will work in.

- Realistic security systems
- Flexible architectures
- Testing/analysis platforms

Operational systems (disruptions)

Testbeds (expensive)

Simulations (low-fidelity)

THE PATH TO CYBER EXPERIMENTATION

How capable is the platform in configuration and deployment of new cyber experiments?

How quickly can experiments be designed and implemented (i.e., machine speed vs. human speed)?

How faithful is the capability and platform in representing and evaluating cyber security technologies?

What is the process for effective training and equipping of the cyber analysts with new approaches, tactics, techniques, and solutions?

Does the capability include methods or algorithms for scoring and measuring the effectiveness of the approaches, tactics, techniques, and solutions under evaluation?

What is the scalability of the system-under-study through deployments on the platform? Can the capability and platform replicate systems at desired scales?

Can multiple information system applications be deployed and have faithful interoperability with other systems and applications?

Will the capability and platform accurately represent the operation of mission critical applications and the impacts to it from the approaches, tactics, techniques, and solutions under evaluation?

THE PATH TO CYBER EXPERIMENTATION

Cyber Ranges are "interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment."

- Virtual
- Emulated,
- Hardware-in-the-loop (HITL)

Standalone ranges in a single organization, to multiple ranges emulating the Internet, remotely accessible from anywhere.

THE PATH TO CYBER EXPERIMENTATION

Ranges environments should provide:

- RT feedback and with-fidelity simulation
- facility for teams to engage/support the experiment
- hypothesis testing mechanisms with various players
- performance-based assessment metrics and data

Academia

Private Industry

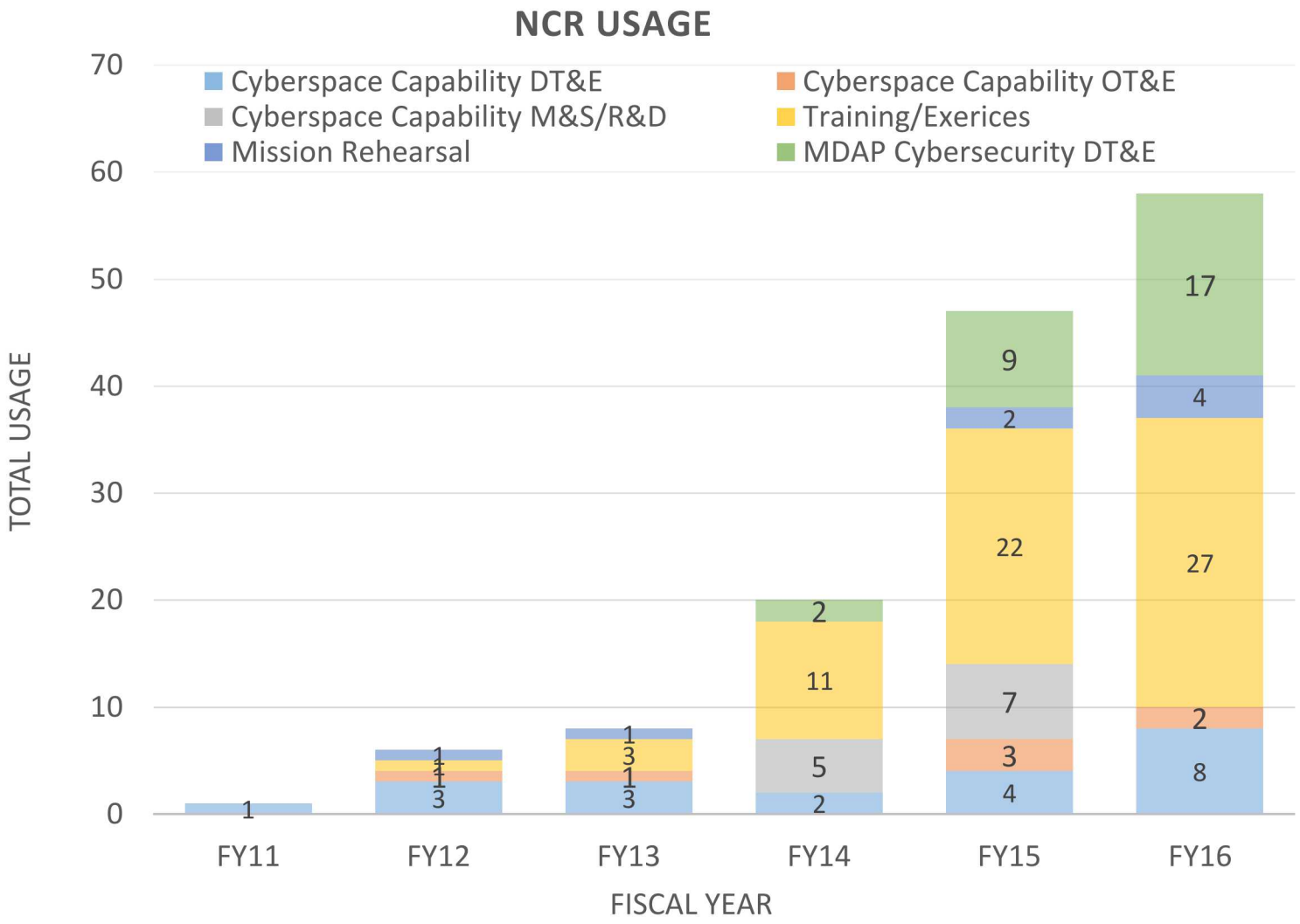
Government

A BLUEPRINT FOR CYBER RANGES

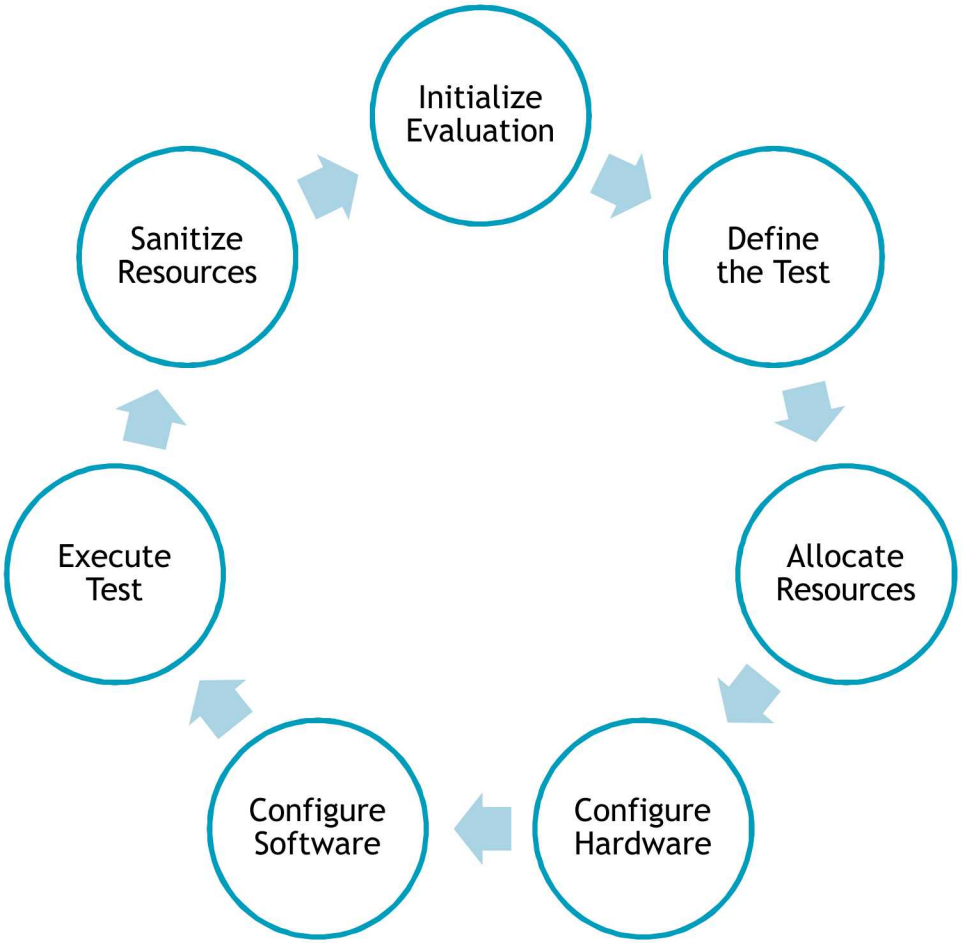
National Cyber Range (NCR) - DoD resource

- DARPA → Test Resource Management Center (TRMC)
- Corporate Operations (T&E Range Oversight), Test Capabilities Development, Interoperability, and Technologies Development
- Accredited by DIA; multiple classifications
- Key components include:
  - Secure facilities
  - Unique security architectures
  - Integrated tools for cyber testing
  - Multidisciplinary staff

A BLUEPRINT FOR CYBER RANGES



NCR Life-Cycle



LIMITATIONS AND THE NEEDS OF TOMORROW

Integration conferences
Licensing
Remote Access Management
Credential Management
Configuration Management
Documentation
Automation and Pre-configuration Templates
Build-in Debugging Processes
Periodic Hardware Testing and Refresh
Architectural Integration Testing
Experiment Integration

LIMITATIONS AND THE NEEDS OF TOMORROW

Integration Conferences

"Significant delays occurred in distributed provisioning information from many agencies. The delays impacted the execution of task items on the critical path and did not allow sufficient time for the integration of dependent environments into a functioning base environment."

Licensing Management

"Licensed firmware for a device could not support required features. An extremely slow, out-of-band connection was required to download the new licensed firmware - which set back deployment by several hours.""

LIMITATIONS AND THE NEEDS OF TOMORROW

Remote Access Management

".. a single Windows machine was setup as a remote log-in server. The user had to routinely log-off disconnected users in order to have enough free memory for the desktop (20-some people should not be logged into the same host at the same time."

Credential Management

"During one particular buildout of the event environment, multiple different organizations provided sections of the network infrastructure. Frequently, the necessary credentials to access and troubleshoot system components in the environment were not handed off or made available (e.g., router and user-workstation passwords)."

LIMITATIONS AND THE NEEDS OF TOMORROW

Documentation

"the results of poor communication and documentation from parties, resulting in uncertainty in responsibilities, when things needed to be done, and who could provide help when needed. Or, delays caused by naming issues of devices on network maps vs. device names on VMs. Often, responses are very slow, as email is not a good means to convey an issue."

Automation and Pre-configuration Templates

"instances where networking devices were not configured ahead of time, resulting in field engineers entering configurations line-by-line, where a copy and paste operation in a terminal would have save a considerable amount of time."

LIMITATIONS AND THE NEEDS OF TOMORROW

Build-in Debugging Processes

"the process should include written points of contact for specific systems and a tiered support chain as needed for the experiment. This should also include the system designers and deployment team. This should attempt to prevent disruption of previous known configurations that then become suspect."

Periodic Hardware Testing and Refresh

"One observation noted the simple process of burning a disc in a room and trying to get a file onto the higher network. The effort turned out to be disastrous due to DVD burners and readers failing, resulting in many man hours wasted."

LIMITATIONS AND THE NEEDS OF TOMORROW

Architectural Integration Testing

" deployment setting up virtual machines (VMs), incorrect operation of system was identified; numerous devices were isolated and not showing expected connectivity. After moving the virtual devices on to a single compute blade, the deployed VMs operated as expected. It was determined that the infrastructure switching was not completely functional or reliable."

Experiment Integration

"single integrator for the various architectures and technical requirements; created a bottleneck in the dissemination of technical information to others for interfacing requirements. In another exercise, multiple organizations providing systems for use in the environment had different levels of knowledge for the proper functioning of their systems, yet no one organization had cross-system knowledge - making it difficult to compile the data necessary to perform proper function checks on the environment.

LIMITATIONS AND THE NEEDS OF TOMORROW

Configuration Management

"During one build-out of an environment, multiple organizations provided sections of the network to a single party, who would work with the subject matter experts from each of the organizations and then package and send captures of the environment to the range provider for integration. The environment would be reconfigured without logging changes, leaving differences between the actual environment and what the organizations sent to the range provider; as a consequence, images needed to be reloaded multiple times to fix misconfigurations."

CONCLUSION

Discussed need and constructs of a cyber range.

- Every experiment carried out in a cyber range will have various nuances.
- Nuances should be captured and addressed in the life-cycle of the experiment.

Our position: the basic structure of experiment life-cycles is not enough, flexibility should address the many challenges and shortcomings that arise out of cyber range testing.

Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper

PRESENTED BY

Will Stout

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.