DETER Project Components:

- Developer of research in experimental methodologies (the crucial recipes, tools, and interfaces) to increase understanding of how to carry out science-based experimentation. This is often referred to as "research on research."

- Designer and operator of a laboratory platform, DeterLab, that readily allows researchers to put into practice their "future thinking" ideas – through testing and experimentation – to advance solutions to hard problems in cyber space. This is critical, especially as more and more systems become Internet-integrated.

- Provider of essential educational exercises in cybersecurity to academic institutions. The use of DeterLab enables hands-on learning to significantly bolster the capabilities of the next generation of cyber architects and guardians.

USCViterbi
School of Engineering
Information Sciences Institute

Berkeley
UNIVERSITY OF CALIFORNIA

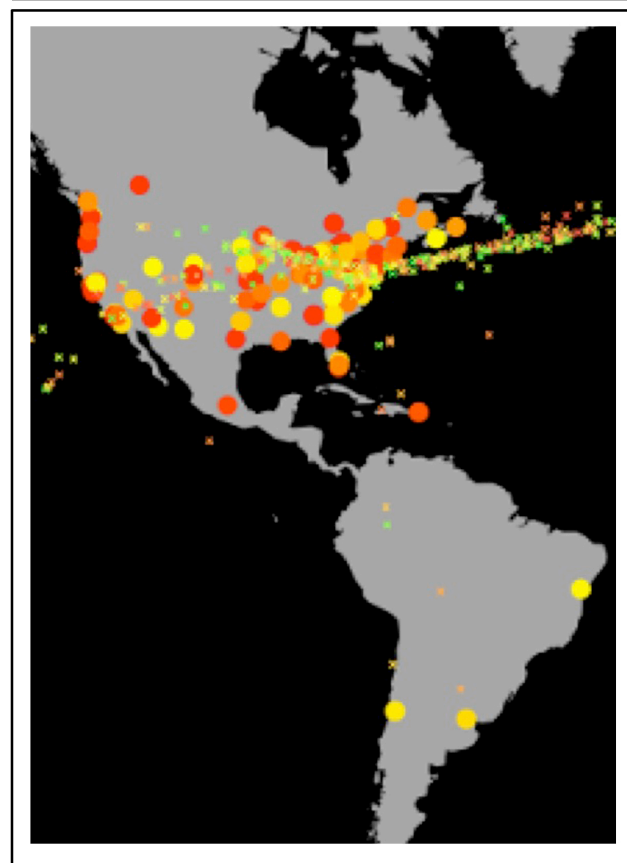SPARTA, Inc.
a **PARSONS** Company

"DETER is aimed at being the environment that will help researchers innovate faster, produce defensive solutions that we can then transition and commercialize and make (widely) available…"

Dr. Douglas Maughan
Department of Homeland Security

deter-project.org

The **DETER** Project

DETER: research project and operator of DeterLab, an advanced testbed facility, where leading researchers conduct critical cybersecurity experimentation and educators teach using hands-on exercises. DeterLab emulates real-world complexity and scale necessary to evolve next-generation solutions to help protect against sophisticated cyber attacks and network design vulnerabilities. As devices become Internet-integrated, the need for resilient design is apparent. This is where it begins.

DETER Background

Originating in 2003 and funded by DHS, DOD, and NSF, the DETER Project was formed to create experimental methodologies to enable innovations in cybersecurity research.

The need for infrastructure to implement these methodologies gave rise to DeterLab in 2004 – a state-of-the-art testbed – to experiment and test defense solutions for network technologies.

For over a decade, DETER has supported thousands of researchers in academia, industry and government.

Accessible, Scalable Virtual Lab

DeterLab supports large-scale experimentation necessary to emulate real-world complexity.

It is a publicly shared scientific laboratory and proving ground for researcher innovations.

- Web-based application, review and approval process
- Authenticated remote access through a web-based portal
- Usage is free
- Ability to create virtual hosts and networks from DeterLab's hardware.
- Integrated tools for data and traffic generation
- Open usage policy encourages collaboration


Worm / Botnet / DDoS Scenario
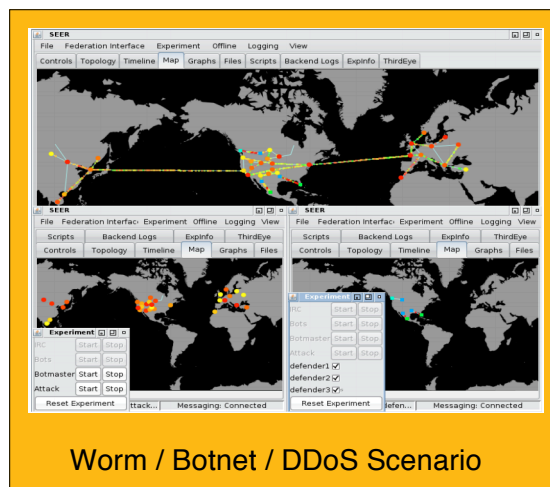
DeterLab Capabilities:

- **Multi-resolution virtualization** of experiment resources
- **Federation** to connect heterogeneous resources from different owners with varying usage and access policies
- **Multi-party experiments** technology that provides controlled but co-joined experiments, creating different views within one unified experiment
- **Experiment orchestration**, providing deterministic control over the various components in an experiment
- **Predictive modeling of human behavior** supporting definition of mental models, reactive goal-driven behavior, and combinations of deliberative/instinctive behaviors
- **Risky experiment management** to allow controlled experiment interaction with the real Internet

Support for Cyber Physical Systems (CPS):

- Extensions for CPS, simulation and visualization
- Modeling tools for CPS
- Support for multiple collaborators
- Federation and experiment orchestration capabilities for distributed experiments and experimental control

Power Grid cyber-attack scenario running in real-time in DeterLab
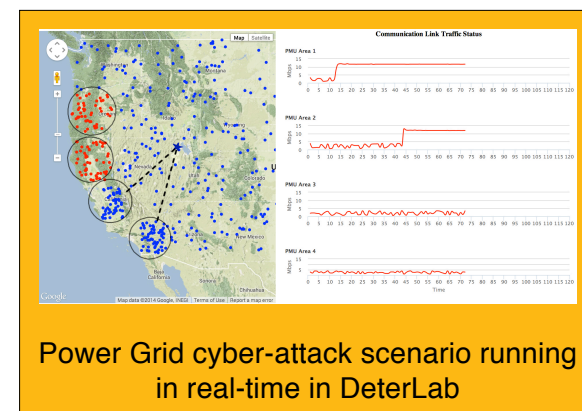
Education and Training

DeterLab is also offered as a hands-on teaching lab (*education.deterlab.net*) used by cybersecurity educators and students at a wide range of universities.

- Teaches how to perform scientifically correct experiments
- Over a dozen packaged practical lab experiments and exercises available for frequently-taught topics in cybersecurity
- Community-contributed class modules
- Students gain valuable experience with realistic security challenges and solutions