# Distributed Environment for Critical Infrastructure Decision-Making Exercises

Understanding the Complexities of Our Financial Networks

A critical focus area for the Department of Homeland Security, Science and Technology Directorate (S&T) is the development and deployment of technologies used to protect the nation's cyber infrastructure, including the Internet, that depend on computer systems to support their missions. Critical infrastructures, including financial services, energy and transportation sectors, operate in an environment of high-volume transactions. Because of increasing complexities and poorly understood interdependencies among their networks, a large number of unknown vulnerabilities exist. Recognizing this problem, the financial sector identified a need for exercises to stress the massive complexity and interdependencies of our critical infrastructures.

Advancing state-of-the-art of critical infrastructure protection exercises

In 2008, based on the need of the Financial Services Sector, S&T began funding the Distributed Environment for Critical Infrastructure Decision-making Exercises (DECIDE) project. DECIDE is a software suite that significantly advances state-of-the-art critical infrastructure protection exercises. The software offers the capacity for a new caliber of exercise that will guide participants in preparing for low probability, high consequence events in the complex and interdependent financial sector.
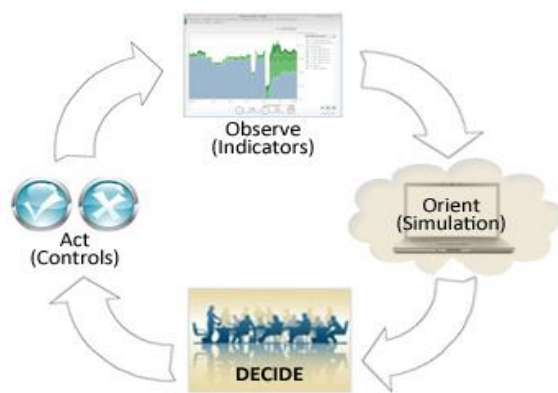
DECIDE enables exercise participants to simulate scenarios using a closed-loop format so the consequences of each participant's actions feed back into the exercise. These exercises are designed to help participants understand the systemic results of their actions and those of their industry peers—specifically scenarios that may prompt cascading failures, resource contention, systemic instability and other unintended consequences. DECIDE allows critical infrastructure operators to identify scenarios where industry-wide coordinated response tactics are beneficial and offers the capacity to exercise these scenarios to demonstrate potential benefits.

DECIDE significantly reduces barriers to exercise participation by providing maximum benefits for minimal time and monetary investment in a reusable exercise setup and planning process. DECIDE exercises insulate each participant's proprietary information, allowing competitive institutions to participate with confidence.

The goal of DECIDE is to allow enterprise decision makers to evaluate responses to operational disruptions of market-based transactions across networks, provide a dedicated exercise capability for several critical infrastructures in the United States, and foster an effective business continuity effort to deal with increasingly sophisticated cyber threats.

Making an Impact

The project will enable private sector entities located within critical infrastructures to conduct collaborative, realistic, fully immersive, scenario-based exercises with response decisions made by enterprise risk managers. These exercises will be based on realistic impacts to individual business models. DECIDE will reduce the time and cost of building large-scale distributed exercises, ensure business return on investment for participating in exercises, and address the issue of sharing business-sensitive information with competitors and regulators. Ultimately, the project will allow more businesses to realistically exercise contingency plans.

DECIDE was originally conceived by the financial services sector and is currently being designed for that sector; however, exercises in all transaction-oriented critical infrastructures could be supported in the future. DECIDE will be of greatest value to operational managers and their immediate leadership. Aware of varying levels of interest and enthusiasm among exercise participants, DECIDE designers strive to allow users to get started quickly and to provide tools for deeply engaged participants to drill into operational details and participate at a very high level.

To learn more about the DECIDE Project, contact sandt cyber liaison@hq.dhs.gov.

2014 11 03