As a founding member of the Cyber Conflict Research Consortium, the Space Dynamics Laboratory (SDL) works in collaboration with leading universities and policy research institutions nationwide to support the Department of Homeland Security and military customers with cyber security exercise planning tools and expertise.

SDL and consortium team members recently developed CyberSMART, the Cyber Scenario Modeling and Reporting Tool. This web-based application allows a widely dispersed team of scenario developers to efficiently collaborate and capture the information necessary to plan complex cyber incident preparedness exercises. These exercises help to examine an organization’s capability to prepare for, protect from, and respond to potential cyber-attacks, thereby strengthening their security, readiness, and incident response capabilities.

The CyberSMART™ Exercise Execution Engine is used to carry out cyber exercises to provide participants with exercise injects from the Master Scenario Events List (MSEL) generated in the planning phase. It enables an Exercise Controller to manage the MSEL and the exercise by controlling scenario time and dynamically changing the MSEL injects as necessary. By design, when an MSEL inject is ready for execution, it is delivered to the specified target organizations. These injects arrive in player dashboards via an intuitive, email-like interface where players may view the observable effects of the inject and respond accordingly. The inject delivery system supports multiple media types to allow for an engaging atmosphere. Players use this email-like system to respond to the injected event for after-action review and to communicate with other participants.

A system-wide instant chat window is also available to allow for communication between participants. CyberSMART™ is an easily scalable tool, allowing for the planning and execution of both small and large exercises. SDL is continuing research and development of CyberSMART and expanding its capabilities to support full scale exercises.

SDL helps develop tools used during scenario-based cyber security exercises that determine an organization’s capability to respond to potential cyber-attacks.
SDL is also working with the consortium to develop a multi-user simulation tool to assess the impact of cyber-attacks on organizations and enterprises within critical infrastructure sectors. DECIDE-FS™ (Distributed Environment for Critical Infrastructure Decision-making Exercises-Financial Sector™) is a highly flexible, user-friendly product that enables enterprise risk managers and business professionals to collaboratively (through multi-party exercises) and individually (through internal use) assess the impact of potentially catastrophic disruptions to large portions of their value chain or sector-wide events.

DECIDE allows users to simulate critical electronic transactions across systems, routes, and organizations that can mirror their real life counterparts. Large time spans of data are simulated over a short time to allow decision makers to quickly see the effects of their decisions over time. Their decisions and performance, like in the real world, affect the decisions and performance of their peers in the simulation. DECIDE allows decision and policy makers to unite to make decisions that mitigate losses.

DECIDE makes available a large array of scenario injects, or attacks, to the scenario development team. This allows participants to develop and experience a wide range of unique scenarios resulting in varying levels of critical response knowledge relative to their sector.

The DECIDE tool is currently being used in a series of exercises to assess and improve operational risk management, crisis planning, and recovery planning in the banking and finance sector.