Argonne NATIONAL LABORATORY

A POWERFUL TOOL FOR **MANAGING INFRASTRUCTURE RISKS**

DISrupt (Decision and Infrastructure Sciences) helps identify disruptions that result in significant cascading failures within and across critical infrastructure systems, providing essential information for managing risks

DISrupt uses advanced modelng and algorithms and information about the shifting global threat landscape—powered by Argonne's high-performance computing resources

WHAT IS IT?

DISrupt is a family of models and analytical tools that helps identify and prioritize high-consequence failure points within critical infrastructure systems. Developed through multiple Laboratory-Directed Research and Development (LDRD) investments and more than 3 years of project applications, pioneering results generated by these tools in the Energy, Transportation, and Emergency Services sectors have allowed Argonne researchers to identify infrastructure assets that, when disrupted, cause significant cascading failures. The ability to identify these failure points within and across critical infrastructure systems provides essential information for managing associated risks.

DISrupt is also informed by the knowledge that our adversaries can conduct reconnaissance operations to assess the environments in which infrastructure systems are situated and execute highly synchronized, multisite attacks against them.[1] This ability to attack specific components of a system, causing cascading impacts in a targeted region or city, makes it imperative for infrastructure protection programs to prepare accordingly.

CONTACT

Duane R. Verner, AICP
Manager
Resilience Assessment Group
Decision and Infrastructure Sciences
Argonne National Laboratory
Email: dverner@anl.gov

U.S. DEPARTMENT OF ENERGY
Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.

February 2019

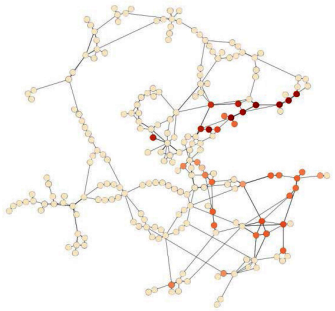
INFRASTRUCTURE IMPACT

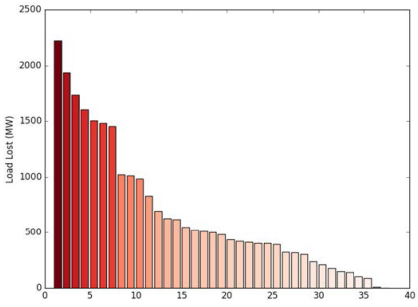
DISrupt allows infrastructure owners and operators and government officials to understand system disruptions and dependencies, ultimately reducing risks to critical functions.

HOW DOES IT WORK?

Advanced modeling, algorithms, proprietary systems data, and dependency data analytics — powered by high-performance computing and informed by the shifting global threat landscape — are integral to the DISrupt prioritization approach. Without prioritization, infrastructure security programs are typically guided by intuition or expert judgement, and they often fail to consider system-level resilience. System-level understanding is critical because very few infrastructure disruptions actually result in cascading failures. For example, results from Argonne's test of a major U.S. electrical system (below) showed that only 36 of 225 transmission substations resulted in load loss during an N-1 contingency.[2]

Understanding how to identify high-consequence failure points is essential, but the complexity of infrastructure systems can quickly become overwhelming. For example, in a notional region with 1,000 electric power assets, nearly 1 billion failure scenarios are associated with an N-3 contingency. It is simply not technically or financially feasible for system operators and government agencies to assess and prepare for all possible failures. By identifying the most critical failures affecting infrastructure systems, DISrupt is a powerful tool to help manage risk for national critical functions.[3]





IMPLICATION

DISrupt helps protect critical U.S. infrastructure against global threats and natural hazards, strengthening the security and resilience of the nation's critical infrastructure systems.

Our adversaries have the ability to execute cyber attacks in the United States that generate disruptive effects on critical infrastructure — such as disrupting an electrical distribution network — similar to those demonstrated in Ukraine in 2015 and 2016.

Worldwide Threat Assessment of the U.S. Intelligence Community, January 2019

[1] "Analysis of the Cyber Attack on the Ukrainian Power Grid," https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, accessed December 5, 2018.

[2] D. Verner, D., F. Petit, and K. Kim. "Incorporating Prioritization in Critical Infrastructure Security and Resilience Programs." Homeland Security Affairs 13, Article 7 (October 2017). https://www.hsaj.org/articles/14091

[3] Ibid.