



OAK RIDGE NATIONAL LABORATORY

Cyber Resilience and Intelligence

The more technologically advanced and connected our world gets, the more we introduce cyber vulnerabilities into our national critical infrastructures. Sophisticated nation-state actors are leveraging those vulnerabilities to steal valuable information, disrupt our way of life, and destroy systems critical to our survival.

Staff within the Cyber Resilience and Intelligence Division's research sections—Adversary Intelligence Systems and Resilient Complex Systems—are identifying and characterizing our nation's adversaries, enabling resilient operation of critical systems in the face of cyber attacks, and helping analysts process multi-modal data streams to more efficiently understand threats and inform mission-driven response actions.

RESEARCH FOCUS AREAS

We leverage ORNL's resources and expertise in cybersecurity, mathematics, high-performance computing, artificial intelligence, and complex systems to provide national security and intelligence community partners with novel solutions focused on:

Cybersecurity Science

Developing innovative R&D capabilities that allow scientific contributions to advance cybersecurity, including cutting-edge, data-driven defensive cybersecurity architectures, technologies, and evaluation methods

Critical Infrastructure Resilience

Researching cyber-physical systems security and resilience to address risks to critical national infrastructure, including industrial control systems and networks for energy, transportation, weapons, and manufacturing systems

Machine-Augmented Intelligence

Building data science and visualization tools to improve analysts' ability to make national security decisions; identify and characterize insider threats; and exploit intelligence, surveillance, and reconnaissance analytics

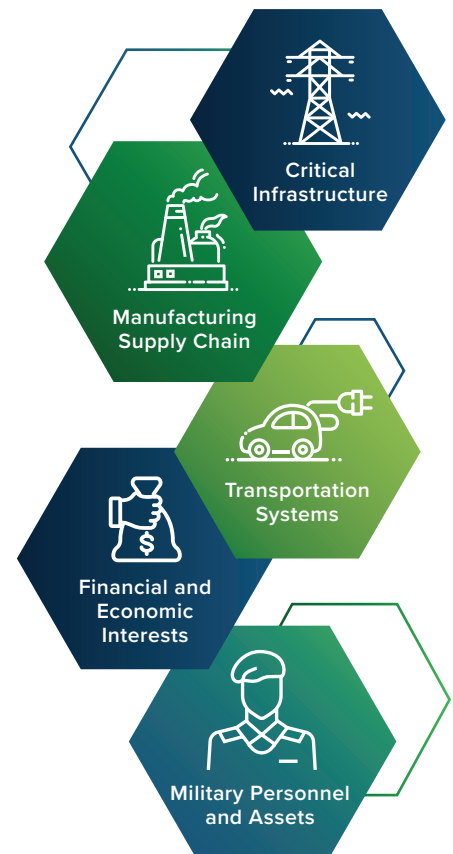
Identity Science

Developing tools and technologies to unveil the identity of our nation's adversaries while protecting the privacy of our citizens

Systems Vulnerability Science

Developing tools to identify software, hardware, and complex system vulnerabilities to support national security interests

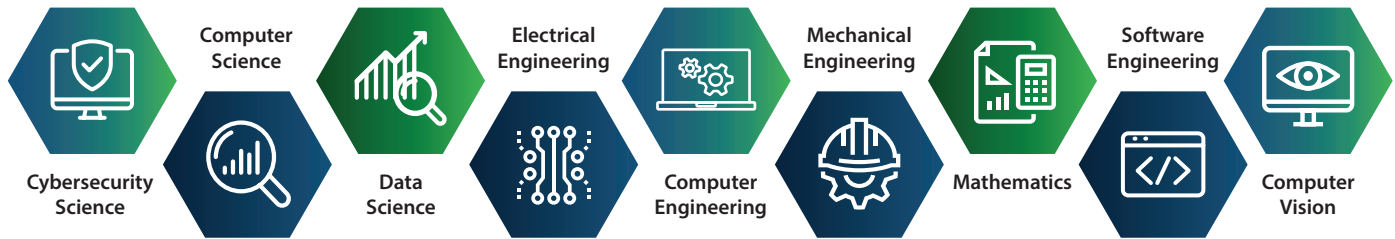
SECURING OUR NATION'S CRITICAL ASSETS



Every day, we're performing scientific research to ensure our nation's most critical assets remain secure and resilient against dynamic adversaries.

SCIENTIFIC DISCIPLINES

Our scientists and technical staff are highly skilled in the disciplines most needed to solve pressing cyber and cyber-physical security challenges.



FACILITIES

- **Cyber Science Research Facility**—Consolidated, dedicated laboratory space for engaging in open cybersecurity science, including vulnerability science, cyber-physical systems, and energy and control systems security
- **Grid Research Integration and Deployment Center**—A unique, multipurpose research environment that combines multiple electrification and systems security research activities across the utility, buildings, and vehicle space
- **Vehicle Security Laboratory**—A component of the National Transportation Research Center, dedicated to assessing cyber vulnerabilities while vehicles are in operation, including onboard computer signal interrogation and interception
- **Embedded Systems Lab**—A security R&D laboratory for embedded hardware and software that includes tools for hardware/software forensics, supply chain analysis, and system vulnerability evaluation
- **Identity Science Laboratory**—ORNL's living scientific platform for research, development, testing and evaluation of identity-related discoveries, technologies, data, and environments

IMPACT



Critical Infrastructure Resilience: Through the 5-Lab WestWorld project, we're developing an intelligence-driven platform for the creation of advanced cyber defense capabilities for the electric grid.

Transportation: We've developed an algorithmic pipeline that can decode vehicle CAN signals, helping identify malware threats in the networks that communicate everything from accelerator pedal angle and brake position to wheel speed and engine temperature.

Cybersecurity Science: Our HPC-enabled, AI-driven Cyber Operations Research Range is optimizing cyber defense architecture and human analyst performance—reducing analysis time from months to hours.

Intelligence: We're bringing the power of data science and HPC to the intelligence analyst. Our research has developed programs to fuse and analyze multi-modal data—including aerial imagery—in real time, helping analysts perform their mission more quickly and completely.

CONTACT

Shaun Gleason | Division Director | gleasonss@ornl.gov | 865-341-1849

Oak Ridge National Laboratory is managed by UT-Battelle LLC for the US Department of Energy

2022-G00224