AOS **Asymmetric Operations** | Cyber-Physical Systems

Critical Infrastructure Protection Group (QNI)

Protecting U.S. Infrastructure From Persistent Threats

WHO WE ARE

The Critical Infrastructure Protection Group (QNI) is a close-knit community of computer, system, and security engineers creating game-changing capabilities that enable U.S. infrastructure to be robust in the face of complex and persistent threats. We design, build, hack, destroy, and invent to advance the state of the art in industrial control system (ICS) cyber defense and vulnerability research. We champion creativity and boldness, empowering our staff to win many funded independent research and development projects.

APL JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

WHAT WE DO

QNI members develop novel methods to protect, and perform vulnerability research on, cyber-physical systems and ICS in critical infrastructure and military applications, ensuring U.S. systems are hardened while designing novel ways to defeat cyber-defense technologies and exploit targeted systems. QNI also protects the national airspace, developing and evaluating systems ranging from high-altitude, internationally mandated collision avoidance systems to low-altitude traffic management and counter-drone solutions.

FOCUS AREAS

- **Cyber-Physical Systems/ICS:** Fortifying operational technology (OT) networks and the critical systems they control
- **All-Hazards Protection and Understanding:** Safeguarding essential systems and assets against a wide range of threats
- **Decision-Making Under Uncertainty:** Developing strategies and artificial intelligence/machine learning (AI/ML) tools to make informed, robust choices based on incomplete information
- **Modeling, Simulation, and Analysis:** Building advanced modeling and simulation engines to analyze and forecast complex, dynamic environments
- **Operational Technology Reverse Engineering:** Performing vulnerability analysis of critical systems supporting Government and Intelligence Community missions

OUR RESEARCH

CYBER RESILIENCE AND CAPABILITY DEVELOPMENT FOR INDUSTRIAL SYSTEMS AND TECHNOLOGIES

Infrastructure services such as power, water, transportation, and communications are vital parts of our daily lives. QNI understands

the risks in these systems, allowing us to (1) make U.S. systems resilient to cyber threats and all-hazards failures, and (2) leverage found cyber vulnerabilities to develop software and hardware capabilities based on government requirements. Our team works with military, civilian, and government sponsors to conduct vulnerability assessments and develop strategic concepts that ensure U.S. advantage in the OT systems essential to infrastructure services. Recent work includes developing advanced architectures and technologies for improved OT situational awareness, as well as orchestrated/automated response and recovery of OT systems from cyberattacks.

VIGILANT INTEGRATION FOR SECURE AND TRUSTED AUTONOMY

QNI's focus is to strengthen and protect the homeland by creating the robust and resilient future for the transportation sector of critical infrastructure. We build upon 25 years of expertise in civil aviation to help the government address key mission challenges, including (1) certifying and measuring trust in AI/ML/large language model (LLM) systems, (2) protecting domestic targets against drone threats, and (3) adapting the national airspace to allow innovation and increasing levels of autonomy.

KEY PROJECTS

- **More Situational Awareness for ICS (MOSAICS):** DoD-backed, first-ever comprehensive integrated and automated cyber defense capability for ICS, allowing users to efficiently detect, characterize, respond to, and recover from cyberattacks in real time
- **Airborne Collision Avoidance System X (ACAS):** FAA-funded family of systems based on the current congressionally mandated technology to avoid midair collisions between a variety of crewed and uncrewed platforms in current and future air traffic environments
- **Sea Change:** NAVSEA-supported effort to design, develop, and deploy cybersecurity capabilities for shipboard and ashore combat and control systems
- **Deckard:** Development of AI/ML anomalous track detection models to help USMC identify suspicious open-water behavior
- **Nightjar:** A software decision support layer provided to TSA that enables consistent threat and risk determinations of small drones
- **Critical Infrastructure and Operational Resilience:** Development and execution of a technical strategy to ensure U.S. strategic assets remain mission-capable against nation-state cyberattacks before and beyond 2027
- **Cyber Resilient Platforms and Infrastructure:** Research portfolio ensuring critical national systems remains mission-capable in the face of nation-state cyberattacks before and beyond 2027

OUR FACILITIES

QNI's Cyber-Physical Resilient Systems Solutions (CYPRESS) Lab is a design, build, and test facility providing 3,000 gross square feet for:

- Infrastructure resilience research and development
- Environmental modeling and simulation
- Control system fabrication and construction

QNI CONTACTS

Josh Silbermann
Group Supervisor
Josh.Silbermann@jhuapl.edu
240-228-0142

Ed Lorenzo
Assistant Group Supervisor
Edwin.Lorenzo@jhuapl.edu
240-228-0739

Ben Zintak
Assistant Group Supervisor
Benjamin.Zintak@jhuapl.edu
240-228-4518

WWW.JHUAPL.EDU