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 team 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. We champion creativity and boldness, empowering our staff to win many funded Independent Research and Development projects. QNI is a caring and fun community.

APL JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

WHAT WE DO

QNI members develop novel methods to protect cyber-physical and industrial control systems in the national infrastructure and military, hardening them against malicious activity. QNI also protects the national airspace, designing collision avoidance systems for manned and unmanned aircraft of all sizes and working to ensure that their integration into everyday life is efficient and safe.

FOCUS AREAS:

» **Assured Autonomy**
» **Decision Science**
» **Collision Avoidance Systems**
» **Industrial Control Systems**
» **Cyber-Physical Systems**
» **Cybersecurity**
» **Reverse Engineering**
» **Systems Engineering**

OUR RESEARCH

DECISION SCIENCE

AI brings new possibilities to infrastructure systems like self-driving vehicles and urban air mobility. QNI's collision avoidance work uses decision theory to help aircraft choose optimal responses from innumerable future states, protecting over 4 billion passengers annually. Beyond aircraft collision avoidance, QNI is mitigating disruptive adversary tactics that threaten advanced system design and autonomous integration

efforts. Securing infrastructure systems requires decision science that scales to scenarios like armed conflict, counterterrorism, and gray zone deterrence.

ASSURED AUTONOMY

Autonomous urban and aviation ecosystems promise high-speed commerce, transportation, and public safety operations, but participants share resources to complete missions. Safely building these systems requires robust interactions between independently developed algorithms and systems as decision-making logics maximize efficiency and safety. Traffic signal, collision avoidance, power grid control, and drone dispatch algorithms can fail in new ways as they become increasingly autonomous. QNI is building runtime white- and black-box monitors, stress-testing mechanisms and simulations, and the policies required to permit a safe, autonomous future.

NAVAL CYBER RESILIENCE

Cyber-physical systems on naval platforms control or enable critical operations such as weapons, navigation, and power generation. A holistic approach to securing these systems for continuous operations is vital. QNI provides novel security solutions for tailored intrusion and anomaly detection systems, undetectable response mechanisms, and autonomic recovery capabilities to ensure constant combat readiness. Recent work includes out-of-band communication analysis for superior situational awareness and virtualizing programmable logic controllers for redundancy and real-time recovery.

CRITICAL INFRASTRUCTURE PROTECTION AND ANALYSIS

Infrastructure services such as power, water, transportation, and communications are vital parts of citizens' daily lives. QNI works with civilian and military government sponsors to conduct vulnerability assessments and develop strategic concepts to increase the security and resilience of the operational technology 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 recover of OT systems from cyberattacks.

QNI CONTACTS

Tao Jen
Group Supervisor
Tao.Jen@jhuapl.edu
240-228-5231

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

WWW.JHUAPL.EDU