**AOS** **Asymmetric Operations** | Communications Systems

*Wireless Cyber Capabilities Group (QKW)*

# Cyber-Enabled Spectrum Superiority

## WHO WE ARE

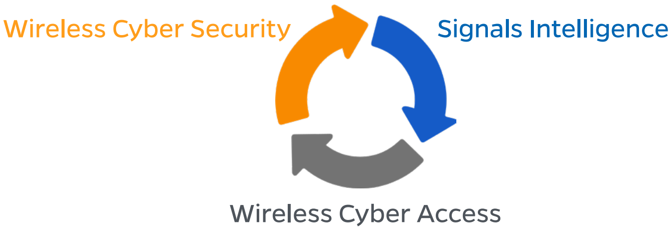
Wireless Cyber Capabilities (QKW) is a group of wireless communications experts dedicated to helping our nation achieve electromagnetic spectrum (EMS) superiority at home and abroad. Our scientists and engineers devise novel solutions to both offensive and defensive wireless-cyber challenges across a myriad of technologies and infrastructure. These include, but are not limited to, Internet of Things (IoT), tactical radio, cellular, and satellite communications. Our fielded solutions include elements of advanced signal processing, wireless reverse engineering, cognitive radio, and artificial intelligence (AI). We continually strive to redefine the "art of possible" in the rapidly evolving landscape of wireless technology.

APL JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

## WHAT WE DO

We provide U.S. military and intelligence communities a significant operational advantage by exploiting adversary wireless communications protocols, devices, and systems, while securing our own against technical surveillance, wireless intrusion, and electronic attack.

### FOCUS AREAS



## OUR RESEARCH

### SIGNALS INTELLIGENCE

As an operating domain, the EMS is dense with complex signal activity. These are indeed the "footprints" that implicitly reveal adversary location, activities, and operational intent. Drawing on our extensive knowledge of signals and systems, we begin by developing persistent, automated detection and characterization techniques. We then expand to technical surveillance on known wireless infrastructure and wireless reverse engineering of waveforms and protocols of interest. The resulting intelligence illuminates the operating area for further blue-force action.

25-00083 1-28-25

## WIRELESS CYBER ACCESS

Wireless devices and systems now present a sizable attack surface to degrade adversary readiness and inhibit their projection of power. We thus utilize our extensive knowledge of wireless protocols to develop novel methods of projecting cyber effects in adversary networks. These include disruption of command and control, influencing red perception, and obfuscating blue-force activities. We focus particularly on targeted, nonattributable techniques which provide flexibility in both scope and scale of engagement.

## WIRELESS CYBERSECURITY

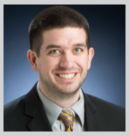
U.S. forces operate in increasingly challenging environments. As we pivot from counterterrorism threats to near-peer competition, we must protect our wireless networks from cyber actors with capabilities on par with ours. This necessitates resilience to ubiquitous surveillance, wireless intrusion, and electronic attack. We therefore draw upon our extensive knowledge of waveform design and wireless networking to secure our devices and systems against a range of cyber threats and electronic warfare devices.

## OUR FACILITIES

Our Wireless Communications Laboratory (WCL) is a highly advanced, collaborative space designed to support our development of innovative solutions to EMS superiority challenges. This state-of-art facility houses computing resources and specialized test equipment for modeling and simulation, rapid prototyping, and assessment of wireless network intelligence and maneuverability under various topologies and operating environments. Additionally, the WCL houses multiple reconfigurable 4G and 5G cellular networks, including an outdoor multicell CBRS (Citizens Broadband Radio Service) network and two operationally relevant commercial satellite communications networks. Also available are two large radio frequency (RF) shield rooms, a 100 GHz anechoic chamber, and a restricted-access area for sensitive equipment.

### QKW CONTACTS

**Andrew Adams**
*Group Supervisor*
*Andrew.Adams@jhuapl.edu*
**240-228-6637**



**Jason Harper**
*Assistant Group Supervisor*
*Jason.Harper@jhuapl.edu*
**240-228-9139**

**Scan to view**
**QKW Publications**
**www.jhuapl.edu/wireless-cyber-capabilities**

**WWW.JHUAPL.EDU**