Opportunity Title: Investigating 5G: Security Community Threats and Identifying Countermeasure Opportunities
Opportunity Reference Code: ICPD-2020-38

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2020-38

How to Apply **Create and release your Profile on Zintellect** – Postdoctoral applicants must create an account and complete a profile in the on-line application system. **Please note: your resume/CV may not exceed 2 pages.**

Complete your application – Enter the rest of the information required for the IC Postdoc Program Research Opportunity. The application itself contains detailed instructions for each one of these components: availability, citizenship, transcripts, dissertation abstract, publication and presentation plan, and information about your Research Advisor co-applicant.

Additional information about the IC Postdoctoral Research Fellowship Program is available on the program website located at: https://orise.orau.gov/icpostdoc/index.html.

If you have questions, send an email to ICPostdoc@orau.org. Please include the reference code for this opportunity in your email.

Application Deadline 2/28/2020 6:00:00 PM Eastern Time Zone

Description **Research Topic Description, including Problem Statement:**

Modern and future wireless technologies, such as fifth generation (5G), are utilizing increasingly higher frequencies extending into the millimetre wave and beyond with their associated ability to support higher information bandwidths. The commercialization of this technology is leading to the availability of low cost RF sub systems and components at these higher frequencies. This is likely, to increase technical threats operating at these higher frequencies, which will be produced at a significantly lower cost with easy deployment. This will mean that the public, businesses, and infrastructure would be vulnerable to cyber-attacks. There is also a user case within airport security and screening techniques used at border checkpoints. This research would investigate what these threats are so that the security forces can a) detect their presence and b) put effective counter measures in place to protect the public, businesses, and national infrastructure.

The aim of the research is to:

- Explore how these frequencies and waveforms interact with electronic systems at a fundamental level.
- Adapt 5G technology sub systems to demonstrate:
  - The technical surveillance vulnerabilities posed by these.
  - Their application to detective countermeasures.
  - Provide advice and guidance to protect the public, businesses and national infrastructure and enhance security screening at airports/border checkpoints.

Example Approaches:

There is a growing area of research that examines security and privacy concerns, identifying attack methods and countermeasures to offer greater protection from such attacks. For example, there has been research to discover how audio from loudspeakers can be recovered from soundproof buildings due to the subtle disturbances they cause to RF transmitters such as widely available such as Wi-Fi[1]. The research identifies the risk and then describes how to protect against this potential attack method.

Relevance to the Intelligence Community:

Opportunity Title: Investigating 5G: Security Community Threats and Identifying Countermeasure Opportunities
Opportunity Reference Code: ICPD-2020-38

The security community needs to fully understand the potential threats posed to the public, businesses, and infrastructure associated with Common-Off-The-Shelf technology that operates at the higher frequency range on 5G. Detection and early mitigation is essential to address this threat. There is also the implication of improving screening technologies at airports or borders by increasing our techniques for detection of hidden devices. Portable screening devices is a research challenge that remains unresolved.

References:

Wei, T., Wang, S., Zhou, A., & Zhang, X. (2015). Acoustic Eavesdropping through Wireless Vibrometry. Proceedings of the 21st Annual International Conference on Mobile Computing and Networking - MobiCom '15, 130-141. doi:10.1145/2789168.2790119

Key Words: 5G, Millimetre Wave, Radio Physics, Technical Security, Wireless Sensing, Pattern Recognition, Countermeasures

Qualifications

Postdoc Eligibility

- U.S. citizens only
- Ph.D. in a relevant field must be completed before beginning the appointment and within five years of the application deadline
- Proposal must be associated with an accredited U.S. university, college, or U.S. government laboratory
- Eligible candidates may only receive one award from the IC Postdoctoral Research Fellowship Program

Research Advisor Eligibility

- Must be an employee of an accredited U.S. university, college or U.S. government laboratory
- Are not required to be U.S. citizens

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **Chemistry and Materials Sciences** (12)
  - **Communications and Graphics Design** (2)
  - **Computer, Information, and Data Sciences** (16)
  - **Earth and Geosciences** (21)
  - **Engineering** (27)
  - **Environmental and Marine Sciences** (14)
  - **Life Health and Medical Sciences** (45)
  - **Mathematics and Statistics** (10)
  - **Other Non-Science & Engineering** (2)
  - **Physics** (16)
  - **Science & Engineering-related** (1)
  - **Social and Behavioral Sciences** (27)