September
2025

THE RISKS OF QUANTUM COMPUTING TO COUNTERINTELLIGENCE

JOB AID

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

CDSE Center for Development
of Security Excellence

Quantum computing represents a paradigm shift in data processing that promises exponential advances in speed and power. It also poses possible risks to our national security and to our nation's counterintelligence operations. The goal of this Job Aid is to show some of the risks, the needs for awareness, and ultimately some type of effective countermeasures.

IMPLICATIONS FOR COUNTERINTELLIGENCE

Leaked communications, agent identities, diplomatic cables, and intercepted transmissions are four real concerns. Entire troves of classified data once considered secure, could possibly become compromised.

For example, quantum machine learning may allow our adversaries to identify patterns in covert operations. Patterns like recruitment, travel, or even the behavior of our undercover agents. Quantum computing could also be used in predicting intelligence operations which could increase the risk of an agent being exposed. Facility access, agent ID verification, and document authentication systems could also be circumvented or fooled.

One positive aspect of quantum computing has to do with the "Know Your Customer (KYC) Threat". Organizations, especially in the financial sector will use quantum computing to verify the identity of their clients. It's a foundational component of Anti-Money Laundering regulations and is used to prevent financial crimes like fraud, money laundering, and terrorist financing.

BIOMETRICS AND ADVANCED AI TOOLS

Biometrics (fingerprints, facial recognition, and iris scans) are becoming more widely used in intelligence and government security systems. Quantum-assisted Ai can now model and replicate biometric data with a far greater degree of accuracy than before. Deepfakes, voice synthesis, and image manipulation can all be enhanced to defeat biometric and visual security checks.

RESOURCES

- National Institute of Standards and Technology (NIST): Post-Quantum Cryptography Standardization Project
- National Security Agency (NSA): Quantum Computing and Cryptography
- Center for Strategic & International Studies (CSIS): Quantum Computing and National Security
  https://www.csis.org/analysis/unleashing-quantums-potential
- U.S. National Counterintelligence and Security Center (NCSC): Annual Threat Assessments
  https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2025/4058-2025-annual-threat-assessment
- World Economic Forum: Why Quantum Computing is a Threat to Cybersecurity
  https://www.weforum.org/stories/2024/04/quantum-computing-cybersecurity-risks/
- MIT Technology Review: The Race to Develop Post-Quantum Cryptography
  https://www.technologyreview.com/2019/07/12/134211/explainer-what-is-post-quantum-cryptography/