In recent years, the possible emergence of a cryptographically-relevant quantum computer (CRQC), a device that exploits quantum-mechanical phenomena to break cryptographic systems, has become more of a reality. A substantial amount of research has gone into the construction of such machines, resulting in increasingly larger and more capable quantum computers. In fully realized, a CRQC would be capable of undermining the security of digital communications on the Internet and elsewhere.

Moreover, this is not a far-off threat. A sophisticated “harvest now, decrypt later” adversary can store encrypted communications sent over many years (including those being sent today!), waiting for the point in time that a CRQC emerges so that they can break into them all.

In this talk, I will survey efforts by the international cryptographic and cybersecurity community to develop, analyze, standardize, and deploy Post-Quantum Cryptography (PQC) to the global communications backbone to resist such threats. This is a very active area of modern research and engineering, with PQC algorithm standards being driven and championed by the U.S. National Institute of Standards and Technology, standards for protocols using PQC being developed within the Internet Engineering Task Force (IETF) and elsewhere, and most (if not all) large tech companies actively working these solutions into their products.