# Overview of
# Quantum-Safe VPN Techniques

Presented by Mark Pecen, ETSI WG QSC, COO ISARA Corp.

ETSI Security Week – 19 June 2019

# Agenda

1. The migration to quantum-safe cryptography and crypto-agility
2. Virtual Private Network (VPN) basics
3. Underlying security protocols, vulnerabilities and solutions
4. Conclusion and summary

# The Quantum Revolution is Here

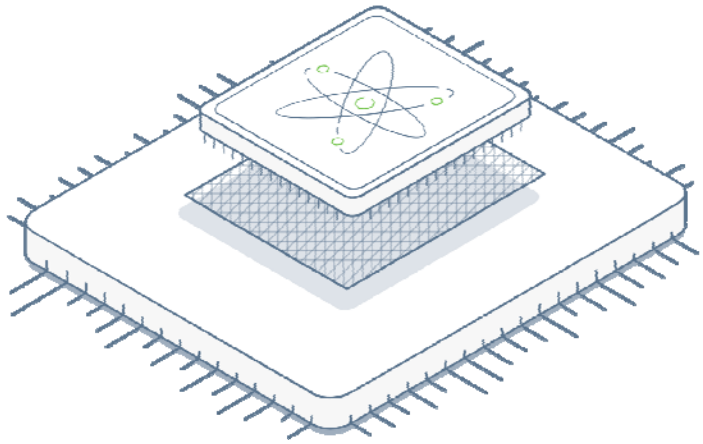
Performance of a quantum computer is **problem-class dependent**

- Certain problems are easy to solve, some are no faster than classic computers

**Solvable problems for quantum computers:**

- Integer factorization problem (used in RSA)
- Discrete logs problem (used in ECC, typically wireless security)

**Real threat** to the current state-of-the-art of protecting information, public key cryptography



# Quantum's threat to secure communications

Secure Communication Protocol

Shor's Algorithm **breaks** current public-key algorithms

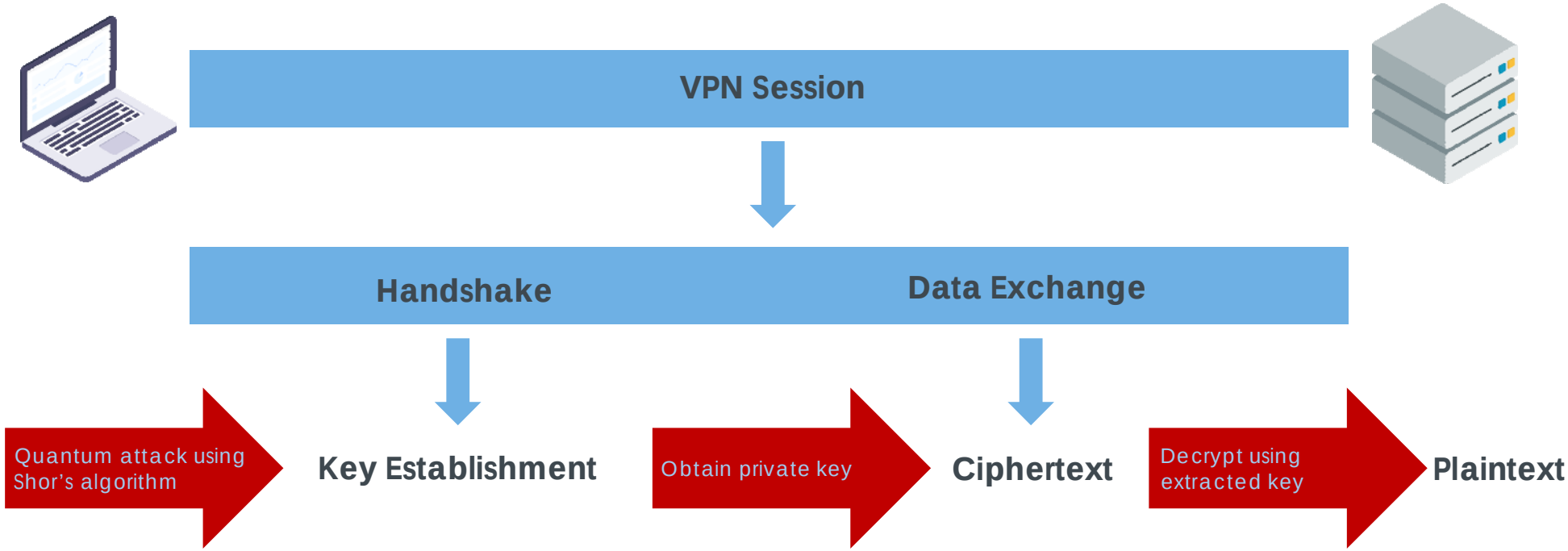
Key Establishment

Authentication

Grover's Algorithm **weakens** symmetric encryption (square root)

Encrypted Transmissions

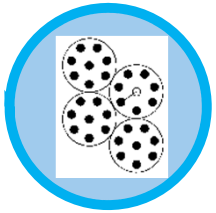
# Harvest & Decrypt Attack on VPN



# 5 classes of math problems

that cannot be solved using a quantum computer

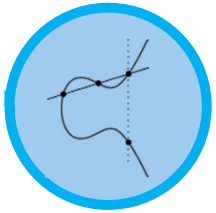
**Hash-based**



**Code-based**

**Lattice-based**

**Multivariate-based**



**Isogeny-based**

# What is Crypto-Agility?

The ability to react to cryptographic threats quickly, at a systems level it **bridges the gap** between current and quantum-safe security methods. It addresses the need to protect against quantum-enabled attacks now or the failure of a crypto algorithm for any reason whatsoever.

# The Virtual Private Network (VPN)


Provides a **secure communication connection** between two end-points

Creates a private network over a public network (Internet)

Many different technologies are used, but goals are basically the same

Two types:

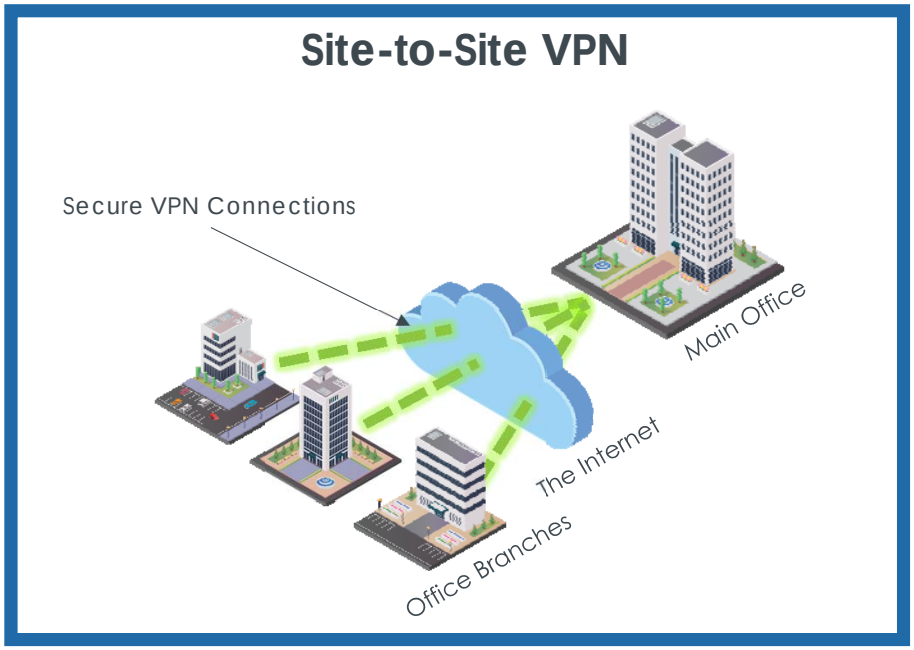
- Remote access
- Site-to-Site

# Site-to-site VPN

Creates a secure tunnel between **two locations**, using insecure network as transport mechanism

Provides secure communications, using encryption

Also provides authentication – ensures that users are connected to intended end-points and not attackers



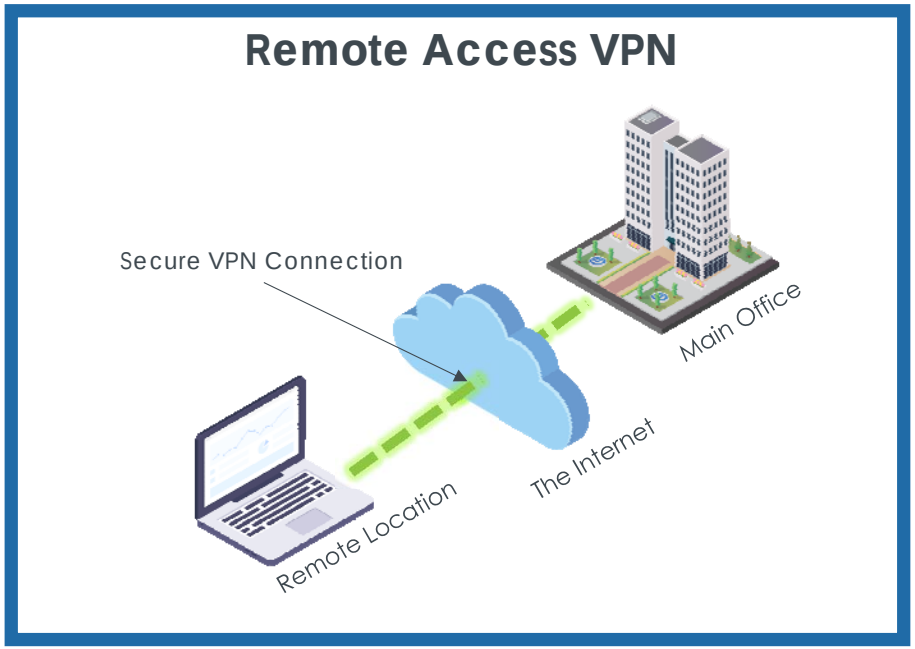
# Remote access VPN

Allows **a personal device** (computer, smartphone, etc.) to connect into an organization's private network over insecure channels

Outsiders can see encrypted data moving between the user's device and the organization's gateway, but cannot identify the organization's internal hosts to which the data are addressed

In contrast to the site-to-site VPN, the remote access VPN establishes tunnels fairly frequently

- Authentication is frequent
- Key management is required to securely share the secrets between gateway and devices



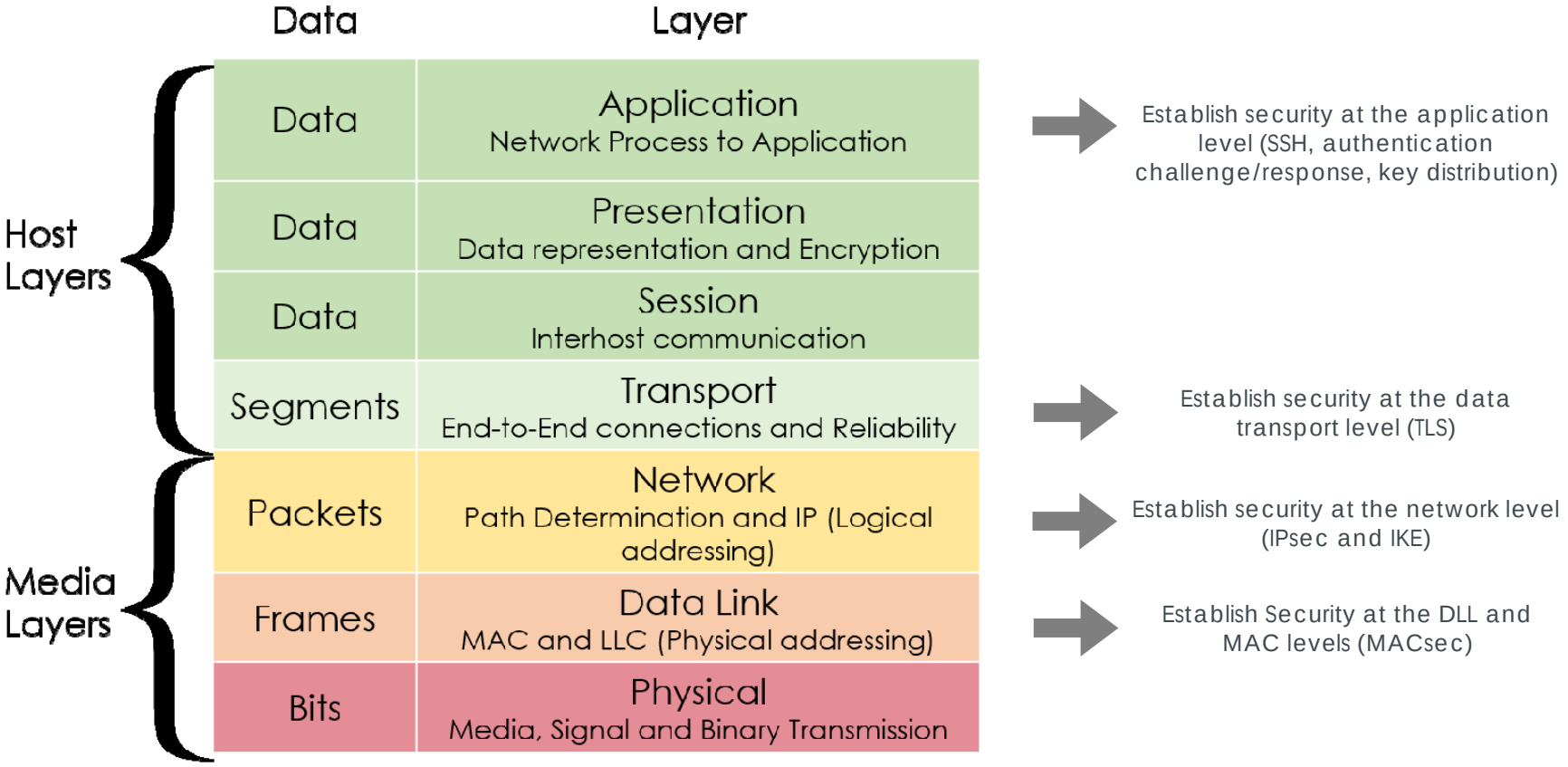
# Security provided by underlying protocols

1. Internet Protocol Security (IPsec)
2. Internet Key Exchange (IKE)
3. Transport Layer Security (TLS)
4. Medium Access Control Security (MACsec)
5. Secure Shell (SSH)
6. … and others

All of them must ensure **Authentication** and **Key Establishment**

are **Quantum-Safe**

# OSI Model

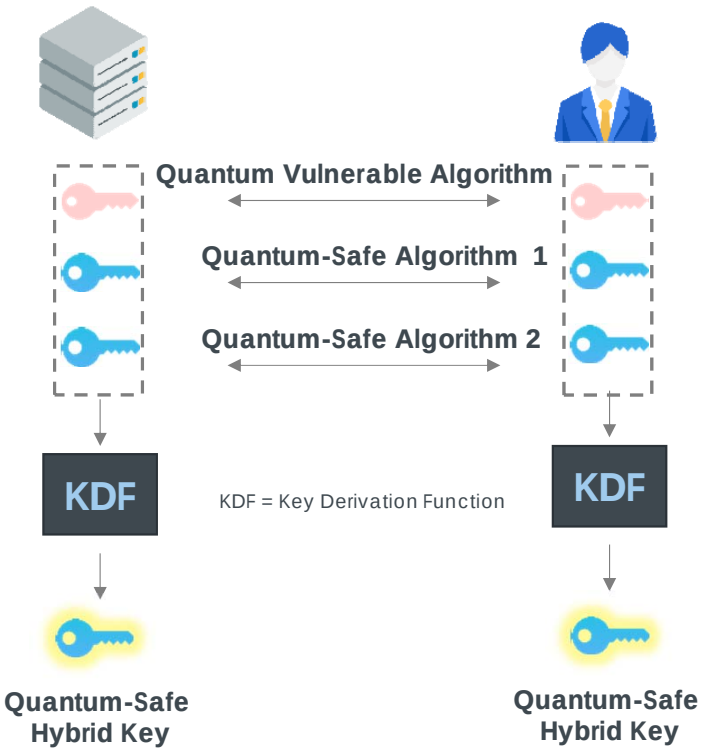

Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data representation and Encryption
Data
Session
Interhost communication
Segments
Transport
End-to-End connections and Reliability
Packets
Network
Path Determination and IP (Logical addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal and Binary Transmission
Establish security at the application level (SSH, authentication challenge/response, key distribution)
Establish security at the data transport level (TLS)
Establish security at the network level (IPsec and IKE)
Establish Security at the DLL and MAC levels (MACsec)

# Hybrid security environments

Hybrid schemes help ease the transition from conventional key establishment and authentication to crypto-agile

This is achieved by **combing legacy and upgraded security**

May include RSA or ECC with one or more quantum-safe algorithms such as lattice-based cryptography



# Public Key Infrastructure (PKI)

Sending a public key and signature proves the sender owns a private key

This is insufficient for authentication – doesn't tell us who the sender is

PKI is the system that **authenticates the sender**

This proves that the public key indeed belongs to a legitimate entity

# Hybrid requirements

**Heterogeneous Environment**

Support for future and legacy technology

**Backward Compatibility**

If a legacy component shows up in a network, no damage will be done

**FIPS Compliance**

Quantum-safe algorithms are not yet FIPS compliant, but the legacy component must still be FIPS compliant

**Cryptographic Agility**

If any crypto technique is broken (by quantum computers or otherwise) there's the ability to rapidly change algorithms, protocols, etc.

**Limit Amount of Exchanged Data**

Implementers must be cognizant of data fragment size limitations, record size limits, processing requirements, etc.

# Additional hybrid requirements

Use of at least **two algorithms** and a security handshake negotiated over a combination of at least one legacy handshake and one quantum-safe handshake

**Minimum** user experience impact

**Localize and limit** changes to protocols

**Focus on confidentiality** – a passive attacker can eavesdrop on encrypted data today and save it until they have access to powerful quantum computers

**Efficient negotiation** of hybrid algorithms

# Direct drop-in approach

A contrast to the hybrid approach, **directly drop in** a quantum-safe encryption or authentication algorithm

The new algorithms can be **used directly in the particular key exchange** or negotiated in the startup process inherent to the VPN

The direct drop-in approach would be by definition **less flexible than hybrid**, but the requirements generally remain the same

# Many challenges, but solvable

Several challenges were identified, but these are largely solvable

**Fragment size issues** have impact on available processing processing power and bandwidth allocations

In some cases, directly introducing hybrid solutions to legacy systems may be **impractical** – direct drop-in solution must be used

**Care must be taken** that the migration to quantum-safety and crypto-agility are robust and avoid breaking the system by introducing opportunities for side-channel attacks

# Summary

**A number of issues** for implementing a quantum-safe VPN have been presented

**Many requirements** have been identified that are common to both

- Hybrid mechanisms
- Direct drop-in replacement methods

**Requirements include**

- focus on backwards compatibility,
- limiting data exchanges when appropriate, and
- limiting complexity when possible

**We've limited** our discussion to the major IPsec, IKE and TLS issues

**There are substantially more issues** relevant to MACsec and SSH

# Conclusions

**1**

The transition to quantum-safe VPN implementation is **extremely complex**

**2**

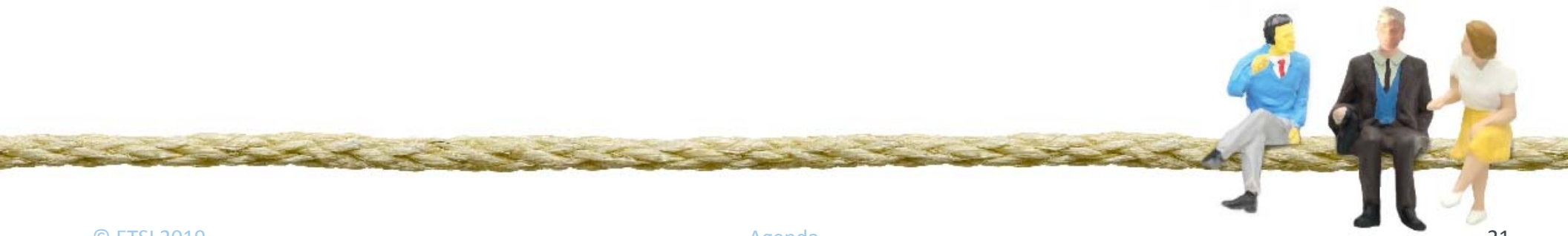
Organisations should **start migration planning early** to ease this transition, and minimize costs of disruption to their business

**3**

For a rigorous treatment of the implementation of quantum-safe VPNs, please refer to **ETSI TR 103 617**

Questions, comments ?

Contact me at mpecen@approachinfinity.ca



# Mark Pecen

- **Chairman of the European Telecommunication Standards Institute (ETSI) TC Cyber Working Group for Quantum Safe Cryptography (QSC), in Sophia Antipolis, FRANCE**
- **Mark Pecen, Chief Operating Officer of ISARA Corporation, which develops security libraries for next-generation networks and computing platforms**
- Former senior executive for BlackBerry, Ltd. where he founded the Advanced Technology Research Centre and helped to develop a significant portion of BlackBerry's wireless and networking patent portfolio

- Awarded the title of Motorola Distinguished Innovator and Science Advisory Board member for developing valuable intellectual property for cellular wireless communication – also managed professional services for clients in Europe and North America
- Inventor on over 100 patents of technologies adopted globally and used in everyday wireless services, including for the Global System for Mobile Telecommunication (GSM), Universal Mobile Telecommunication System (UMTS), High-Speed Packet Access (HSPA+), Long-Term Evolution (LTE) for 4G wireless and others
- Serves on boards of Mobiquity, Safeguard Scientifics, Rocket Wagon, Swift Labs, Ontario Centres of Excellence, University of Waterloo Institute for Quantum Computing, Wilfred Laurier University School of Business, Canadian government advisory council on GDPR
- Graduate of the University of Pennsylvania, Wharton School of Business and School of Engineering and Applied Sciences