5th Meeting of the IoT Advisory Board
Speaker: Christopher Autry, CEO, Iothic
1115-1145am **EST Tuesday 18, July, 2023**

Short Bio:
Chris Autry is part of the Department of Computer Science at The University of Oxford, and holds an MSc in Software Engineering and Security from Oxford. He is also the CEO and founder of Iothic (www.iothic.io), a company focused on post-quantum safe network technology.

Where we are today with IoT and IIoT?
Three technological hurdles in IoT/IIoT systems: Existing Infrastructure, Interoperability and Security; Think about IoT/IIOT networks on a spectrum: One end = single owner, static network, defined connections that never change. Other end = highly dynamic networks that themselves change over time that interact with other highly dynamic networks, each with different administrator/owners. IoT and IIoT require the dynamic end of the networking structure. One of main obstacles is that most IoT solutions are designed with the the wrong end of the network spectrum in mind (ie, static, single owner, highly centralised and predefined connections) but reality is modern IoT networks are dynamic, ever changing and involve multiple owner/ administrators.

Hope and promise of IoT/why is it important?
An idealised IoT landscape is one in which everything can securely communicate and connect with anything else that relevant in realtime. The complex real-time networks of things could provide functionality that we can only begin to envisage. In this scenario all sorts of intelligent automation and functionality become possible.

Connecting between IoT, AI and Quantum

AI and Machine learning are all dependant on network functionality, understanding the connections and functionality between the nodes in the network and then optimising in realtime the best possible combination of functionality to adapt to a particular real world problems. What would take a classical computing model 100 years to solve can be theoretically accomplished by Quantum computing in a matter of seconds. Calculating the probability of all possibilities at once. Near-term quantum computers are already being coupled with AI train models on network functionality to much success.

The power of quantum computing further has the potential to seriously disrupt all current security standards deployed in IoT/ IIoT networks. This includes all static security certificates, RSA, SSL/TSL and more. While there is a conscious attempt to define post-quantum cryptographic algorithms, much of this work is based on the client-sever model of computing rather than decentralised computing, designing harder to solve algorithms that quantum computer cannot easily disrupt. One issue here is running these quantum safe algorithms on current infrastructure including but not limited to the operating technology (OT) on which most infrastructure including infrastructure in military and defence runs.

It is the option of this author, that the power of quantum computing poses just as much if not more of an existentialist threat to humanity if not addressed appropriately than AI alone. Of course as previously mentioned, combining the two is another level of complexity and in fact Quantum AI is a term currently deployed. The entirety of technology can be turned on its head in ways we can only begin to imagine with easy accessibility of quantum computing. This affects IoT and IIoT directly as both are ideally intelligent networks that provide realtime functionality. If these networks are driven by Quantum AI, possibilities currently unknown become possible.

Direct Recommendations

1. Invest **in integrating (quantum-safe) security solutions directly into network itself;** Do not add another software layer that needs to be managed. Future-proof existing networks on existing infrastructure.

   IMPACT ON IOT/IIOT: *Future proofs current and future systems architectures using current networking and NIST standards*

2. **Invest in relatively autonomous and intelligent networking capabilities that require minimal or little human involvement once the technology is deployed.**

   IMPACT ON IOT/IIOT: *De-risks the human element of security, decreases cost by decreasing systems management, creates more intelligent dynamic networks.*

3. **Invest in decentralised and dynamic networks that can adapt in realtime; Move away from static, highly defined, centralised network structures.**

   IMPACT ON IOT/IIOT: *Allows for current and future highly dynamic fluid IoT, and IIoT networks and interoperability between disparate networks.*