Cybersecurity in the Quantum Era

NQCIS weden

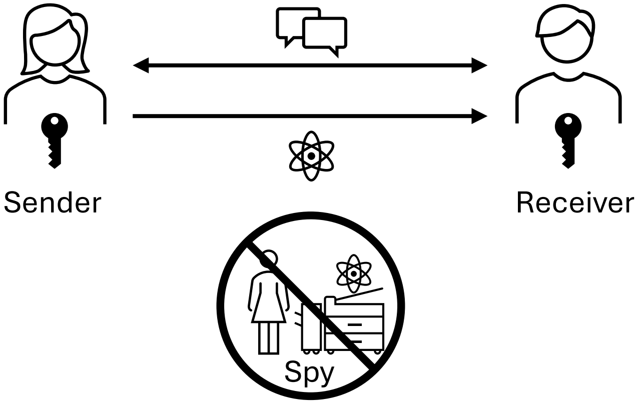
National Quantum Communication
Infrastructure in Sweden

The Quantum Threat

Cybersecurity is at risk since quantum computers will be able to crack the cryptographic algorithms that are currently being used to secure digital communication. This means that secret data, which is shared digitally today, is vulnerable to “harvest now, decrypt later”-attacks, where encrypted information is stolen and stored until a quantum computer is fully developed. Modern cryptographic algorithms are generally based on difficult mathematical problems and are designed in response to specific attacks. A cryptographic scheme that instead breaks this pattern is quantum key distribution (QKD), which theoretically represents an unconditionally secure protocol.

What is QKD?

Quantum key distribution (QKD) is a cryptographic procedure based on the laws of quantum mechanics, where cryptographic keys are exchanged between two parties using an untrusted quantum channel and an authenticated classical channel. Its security is guaranteed by the fact that quantum states cannot be copied. If a spy listens in on the communication, this will alter the quantum mechanical properties of the states, allowing the two parties to immediately detect the disturbance and discard the key.



Securing Digital Communication

All data transfer through digital communication is susceptible to the quantum threat. So, in the quantum era, QKD implementations will be beneficial for the protection of sensitive data, especially for institutions that are interested in keeping information confidential for a long time. Examples of community sectors which may benefit from an additional layer of security enabled by the laws of quantum mechanics are described below.

Business. Without an added quantum security level, business calls requiring audio and video communication over the internet will be vulnerable to eavesdropping and attacks.

Industry. Storage sites with online access may become an open door for trespassers to break in and read the content of documents containing trade secrets or private data concerning industry operations.

Secure Critical Infrastructure. Sensitive data related to the critical services of for instance governmental operations, health, banking, energy and defense will be open to eavesdropping and attacks involving falsified data, faulty bank transfers, and manipulation of electric grids and powerplants etc.

Research. Research data and personal data from research participants may be accessed by attackers if a QKD operational system is not in place.

The European Quantum Communication Agenda

To kick-start the readjustment to a future where the quantum threat becomes reality, the European Commission established the EuroQCI project, an initiative within the Digital Europe Program. EuroQCI is part of the EC strategic autonomy agenda with the aim to create a secure quantum communication infrastructure across the 27 European Union (EU) member states. Together with the European Space Agency (ESA), the EU nations will form a QKD operational system composing of both a terrestrial segment based on fiber communication networks and a space segment linked to satellites. This quantum-based system will be integrated into existing communication infrastructures, providing additional security. The project is coordinated by Petrus, a consortium of experts from both the academic and industrial quantum communities.

EuroQCI

The Swedish Initiative - NQCIS

As part of EuroQCI, the National Quantum Communication Infrastructure in Sweden (NQCIS) team aims to deploy and test QKD systems tailored to the geographical needs of Sweden. The NQCIS consortium brings together expertise from the classical communication industry and the emerging quantum communication field. The collaborating partners comprise of several of the leading universities in Sweden, including KTH Royal Institute of Technology, Stockholm University, Chalmers University of Technology and Linköping University, the start-up companies Quantum Scopes AB and quCertify AB, as well as the global telecommunication provider Ericsson AB.

The QKD Operational System in Sweden

To achieve quantum connectivity across Sweden, the NQCIS project involves validating short- and long-distance QKD solutions, utilizing terrestrial, submarine and satellite links between strategic nodes. In developing the operational system, the team will work along the following four axes.

OT

Open QKD Testbed

Set up a QKD testbed with fiber and free-space systems, with a central hub that is open to research organizations and industry, at the AlbaNova University Center in Stockholm

MN

Metropolitan Network

Develop a many-node network within Metropolitan Stockholm, with the purpose of serving both government and industrial facilities

LN

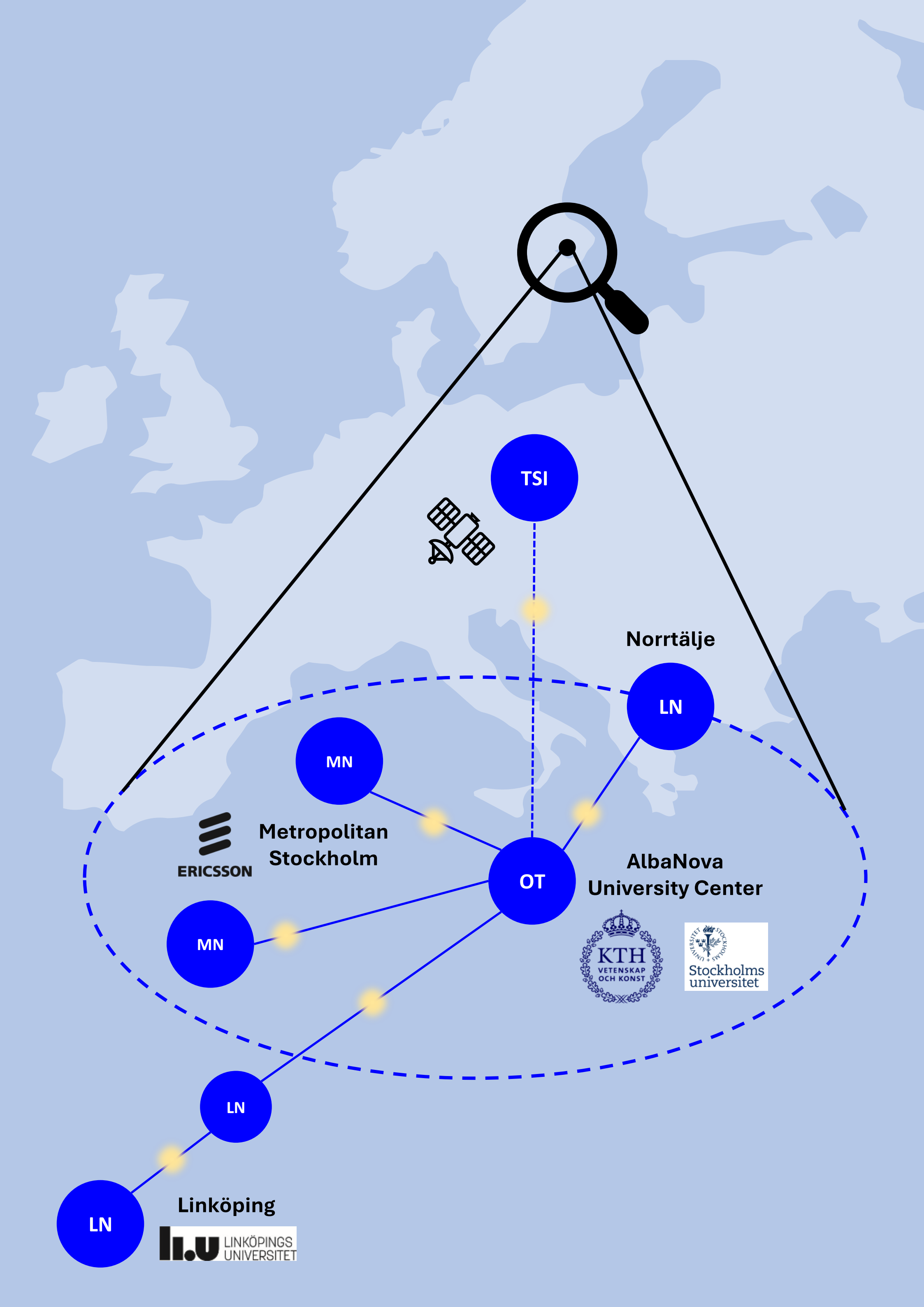
Long-distance Network

Deploy a long-distance network with trusted nodes through terrestrial links towards Linköping and Norrtälje, preparing for cross-border connections

TSI

Terrestrial to Space Interface

Interface the terrestrial segments of the operational system with a satellite link, enabled by the European Space Agency (ESA)


TSI
Norrtälje
LN
MN
Metropolitan Stockholm
ERICSSON
OT
AlbaNova University Center
KTH VETENSKAP OCH KONST
Stockholms universitet
MN
LN
Linköping
LN
LINKÖPINGS UNIVERSITET

Interested in Learning More?

For more information about the need for a quantum communication infrastructure in the quantum era, we recommend looking at the webpages listed below.

Unravelling Quantum Cryptography
www.infographics.icfo.eu/quantum_cryptography

How Does Quantum Cryptography Work?
www.bit.ly/icfo_quantum

The EuroQCI Project, Coordinated by Petrus
www.petrus-euroqci.eu

EU Launches Nostradamus – Prepares Europe for a Quantum World
www.bit.ly/eu_nostradamus

Quantum-related Cybersecurity in Denmark
www.bit.ly/quantum_cybersecurity

Read About Nordic Initiatives

www.nqcis.eu

www.naqci.fi

www.qci.dk

Contact Information

Project Leader
Katia Gallo, Professor
gallo@kth.se

Deputy Leader
Vaishali Adya, Assistant Professor
adya@kth.se

Project Manager
Daniel Vare, PhD
vare@kth.se

www.nqcis.eu

NQCIS is co-funded by the European Union, Vinnova and Wallenberg Centre for Quantum Technology (WACQT) through DIGITAL-2022-QCI-02-DEPLOY-NATIONAL, with project number 101113375-NQCIS.

Co-funded by the European Union

VINNOVA

WACQT | Wallenberg Centre for Quantum Technology

KTH VETENSKAP OCH KONST

Stockholms universitet

CHALMERS

LiU LINKÖPINGS UNIVERSITET

ERICSSON

QUANTUM SCOPES

quCertify