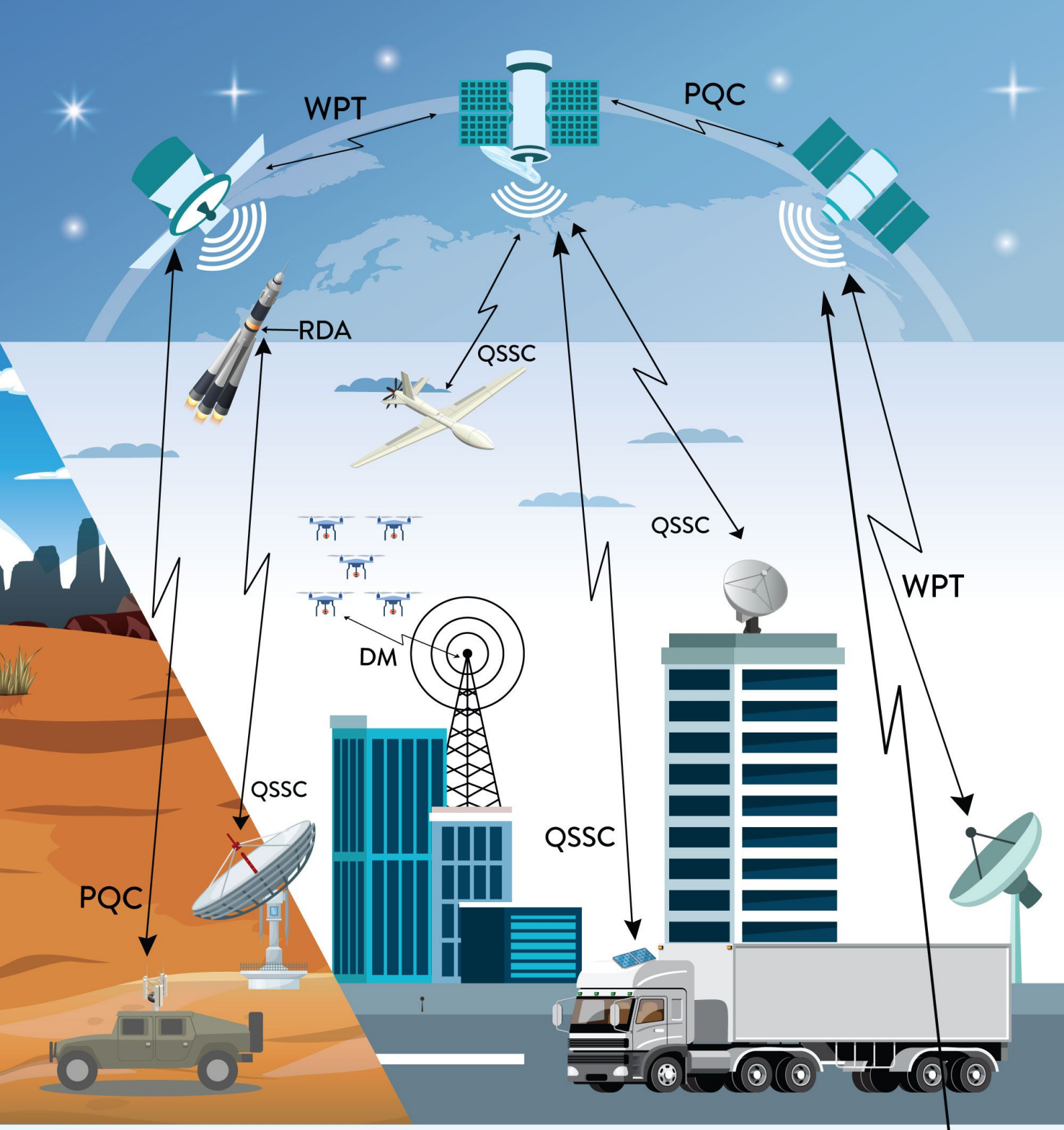
QUEEN'S UNIVERSITY BELFAST

SCHOOL OF ELECTRONICS, ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES | CWI CENTRE FOR WIRELESS INNOVATION

PIONEERING CYBERSECURITY AND CONNECTIVITY TECHNOLOGIES FOR SPACE



At QUB we research and develop cybersecurity and wireless comms technologies applicable to future needs in space:

Security:

- Post Quantum Cryptography (PQC)
- Trustworthy AI for Future Open Networks
- AI-Assisted Physical Layer Security
- Trusted Hardware for Future Comms Infrastructure
- Quantum Safe Secure Communication (QSSC)
- Integrated Quantum-resilient Cryptography (hybrid PQC/QKD activity)

Wireless Comms:

- Directional Modulation (DM)
- Retrodirective Antenna array (RDA)
- Wireless Power Transfer (WPT)

www.qub.ac.uk/ecit

Space exploration requires significant technological innovation, including advancements in launch technologies and electronics systems, to facilitate, among many, EO, robotics, and human life support systems in space exploration missions.

These advancements are necessary to make space exploration more efficient, cost-effective, and sustainable. Queen's University Belfast (QUB) offers deep tech knowledge to Space innovators, from post-quantum cryptography to advanced wireless connectivity.

SECURITY AND AI

While space systems rely on similar infrastructure to terrestrial digital infrastructure, they face unique cyber security challenges in relation to scale, distance and criticality. The cost of a security breach to a satellite involves not only its high capital value but also the potential impact of such a breach, for example shut down affecting global access to services or causing it to crash into other satellites.

Radio links between ground stations and satellites also need to be protected from unauthorised access, corruption or spoofing. Next generation space missions will operate as a 'network of space-based entities' formed with links between the different, heterogeneous nodes, both in space and on the ground, and with the distinction between commercial and military space becoming blurred, the attack surface is increasing.

It is therefore imperative that next-generation space systems are resilient to emerging cybersecurity threats to space equipment, software and communications. With CSIT's research expertise we are ideally placed to address space security challenges. We investigate hybrid quantum/post-quantum systems for securing next-generation space communication systems, AI-enabled security capabilities, such as intrusion detection for satellite networks, and how Digital Twins can be used in security monitoring of satellite systems.

POST-QUANTUM CRYPTOGRAPHY

Our advanced capabilities in big data analysis tools, HPC computing, AI/ML and quantum technologies like post-quantum cryptography (PQC) and Integrated Quantum-resilient Cryptography (hybrid PQC/QKD), can help EO service providers, military & security agencies or interplanetary explorers with the information security needed to succeed in complex space missions.

ANTENNA DESIGN

We have researched and developed (funded by ESA) specialised antennas for the harsh demands of space for over 20 years, for rocket launchers and EO satellites to stay connected to ground stations at all times. Our know-how can be applied to satellite constellations and space settlements and their vehicles.

WIRELESS POWER TRANSFER

Our team of experts in power amplification, antenna design, and beamforming have researched since 2018 the fundamental requirements to develop a practical demonstration of a system that can transfer power to an object whose position relative to the wireless power source is unknown, and that can lie in either the near or the far-field of each other, with arbitrary orientation in both line of sight and beyond visual line of sight (BVLOS) situations. We have produced two major innovations for BVLOS WPT: beyond near/far field auto-focusing antenna array technology, and orientation agnostic rectifying antenna (rectenna) systems. Our know-how can be applied to bring energy remotely to satellites in constellations and HAPS, from space-based solar power farms to Earth, or to electric vehicles in space settlements.

For more details contact: Norbert Sagnard: **n.sagnard@qub.ac.uk**