Network Security in a Quantum Future

SIF Discovery Show and Tell Presentation
5th June 2024

NGESO, Cambridge Consultants, University of Edinburgh & University of Warwick

ESO

Meet the team!

Network Security in a Quantum Future: Presentation Team

Sarah Hadfield (ESO)

James Cruise (Cambridge Consultants)

Bob Oates (Cambridge Consultants)

ESO	National Grid ESO
cambridge consultants Part of Capgemini Invent	Cambridge Consultants
THE UNIVERSITY of EDINBURGH	The University of Edinburgh
WARWICK THE UNIVERSITY OF WARWICK	The University of Warwick

Outline of the problem

When will quantum computers pose a credible threat to the resilience of the grid?

What can be done to manage that risk in a cost-effective, proportionate way?

What is the innovation aspect of this work, and what are the benefits?

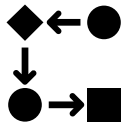
Innovation challenge focus theme:

Leveraging disruptive computing technologies for improving system visibility, performance and cybersecurity
(Theme 2)

Innovations

Novel framework to evaluate the quantum threat to cybersecurity

Methodology for quantum timescale estimates + readiness indicators



Clear risk assessment + mitigation process for quantum threat

Specific to the energy sector

Benefits

- ✓ Enables timely, cost-effective and appropriate quantum threat mitigation strategies for energy networks
- ✓ Supports resilience across the energy industry

The Discovery project encompassed two key workstreams

Work Package 1

Quantum threat assessment

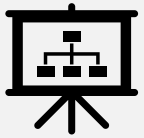
Work Package 2

Information model design

(Quantum-Aware Risk Management process)

Literature review

Interviews and collaboration



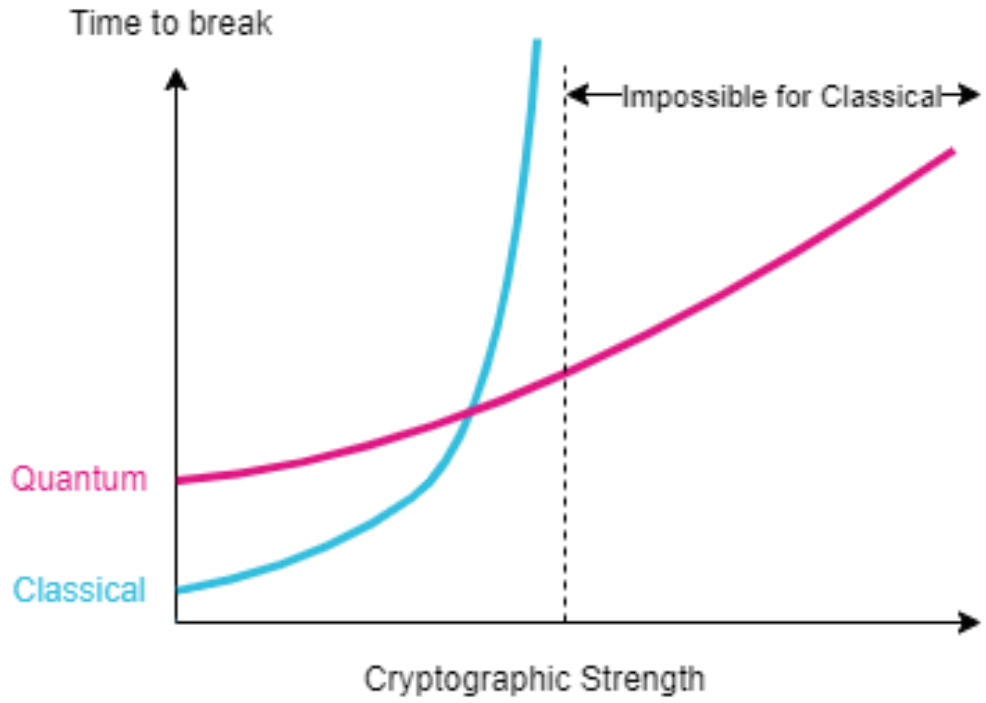
Interactive workshops

Feedback and review

What is quantum computing, and why does it matter for the energy sector?

- Quantum computing will bring both benefits and threats to the energy sector
- Security technology used to protect information **will be broken by quantum computers -** likely in the **next 10-20 years**
- But **quantum development is accelerating** and could reduce this time (time-to-threat)
- Current computers would take millions of years to break current schemes – future quantum computers could break it in **as little as 8 hours**
- Energy networks are a **prime target** for cyberattacks
- Understand what are **appropriate and proportionate response now** - to prevent problems in the future

Quantum capabilities vs classical computing



*Quantum computing delivers dramatically faster processing power than classical computing, by **exploiting quantum physics***

***Dramatic acceleration** for problems requiring highly complex calculations, e.g., chemical simulation, climate system modelling, high-energy physics, as well as attacking encryption algorithms*

Quantum threat assessment – Understanding what, when, how and who

1

Which security controls used by the energy sector are at risk from quantum computers?

Several commonly used security controls are threatened by quantum computers which could undermine our ability to manage cybersecurity risks in the future

Impact:
Energy system providers need to ***evaluate and catalogue all cryptographic schemes*** *in use*

2

What is the likely timescale for quantum attacks to become a concern for the energy sector?

Experts estimate **10-20 years until relevant quantum computers are available,** but **developments are accelerating this.** Attacks may take **only hours.**

Impact:
Greater refinement *of estimates is needed to* ***understand specific threats*** *and* ***identify highest risk assets***

3

When does industry need to react against future threat?

Current quantum threat risk frameworks **provide basic insight** for specific security scenarios

Impact:
A quantum-aware ***Risk Management process*** *is required to* ***fully characterise threat timelines and uncertainty,*** *and to* ***evaluate mitigations***

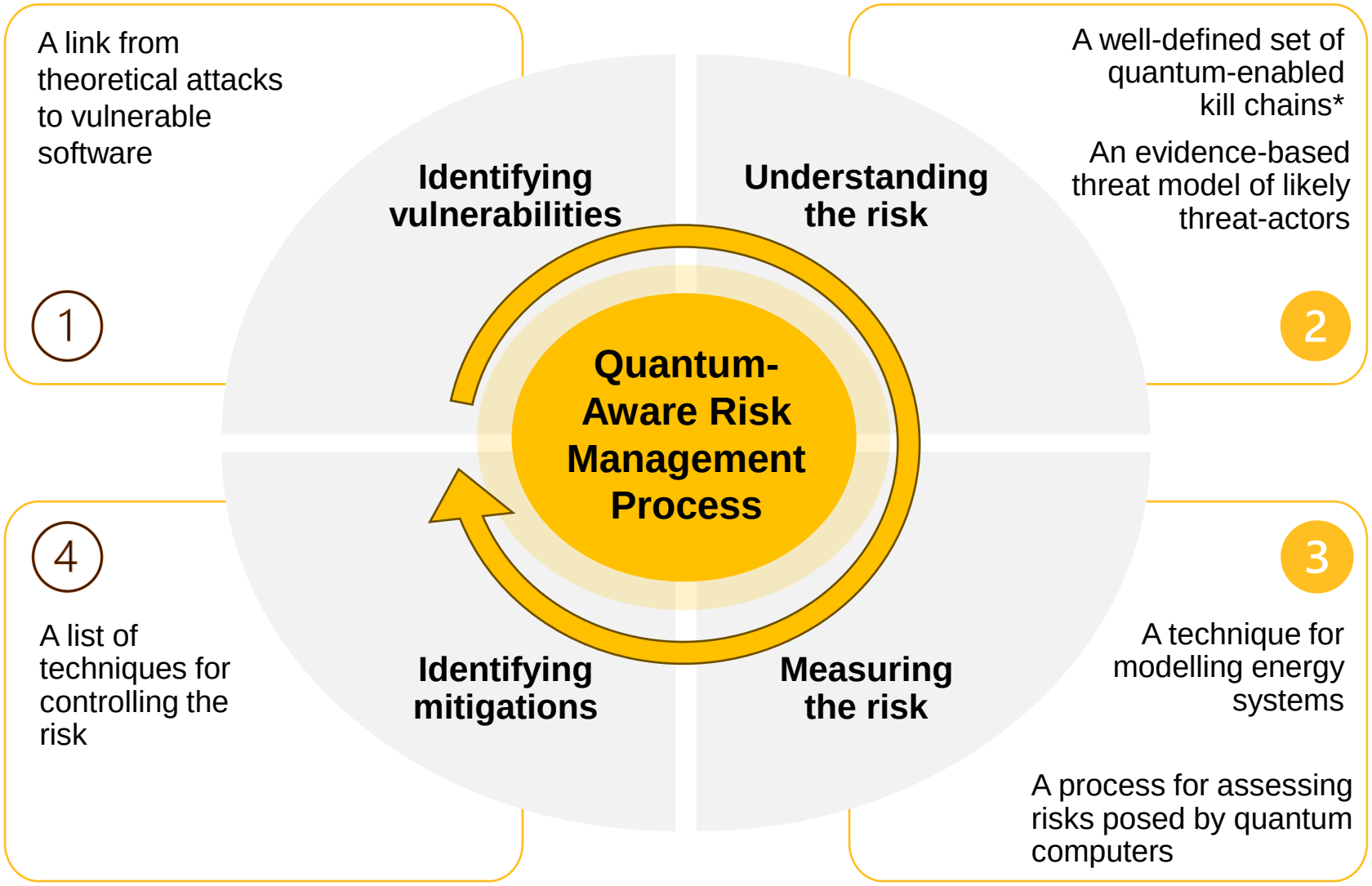
4

Who is likely to have access to suitable technology?

Countries and governments are most likely to have access to suitable quantum computers

Impact:
Organised crime and hacktivist groups have been discounted in the short-term due to expected lack of access to resources

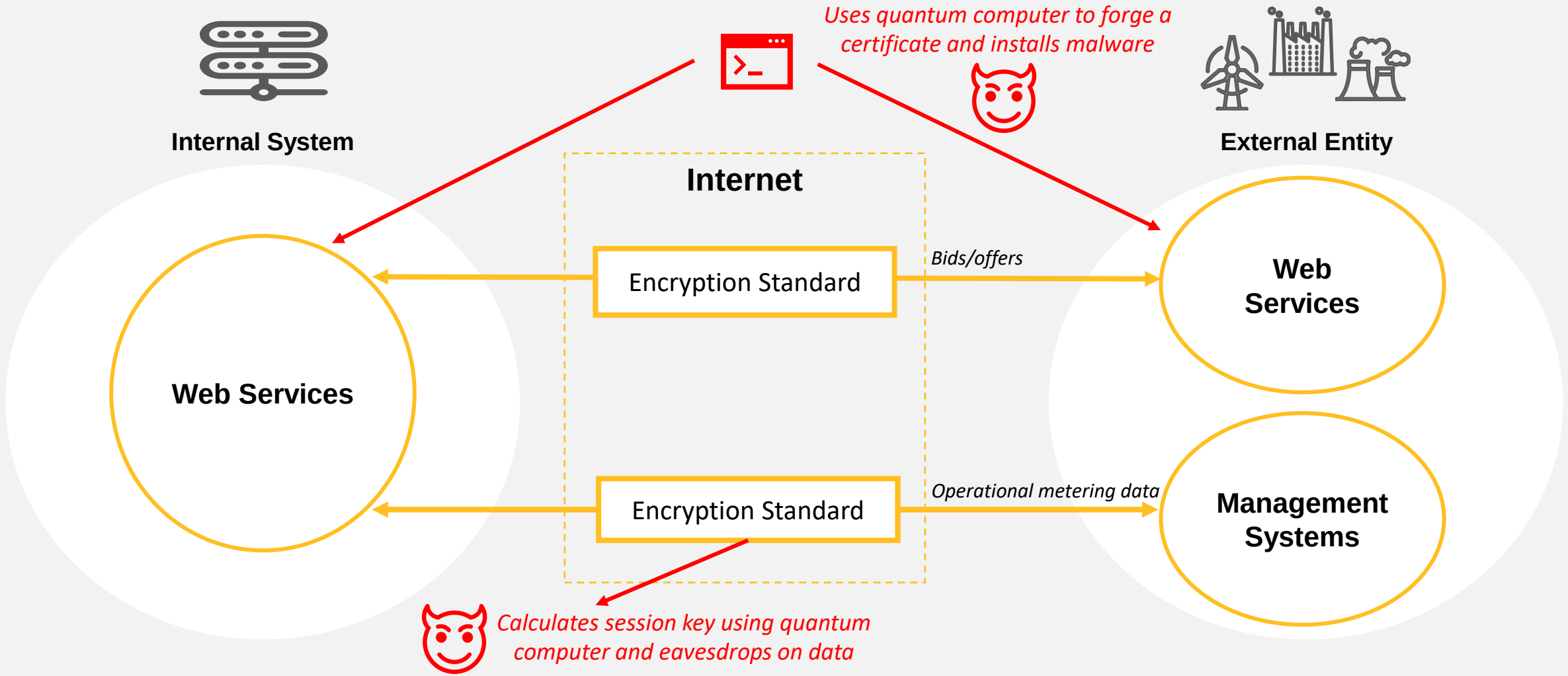
How can security professionals make informed choices about how to secure energy infrastructure against quantum computers?



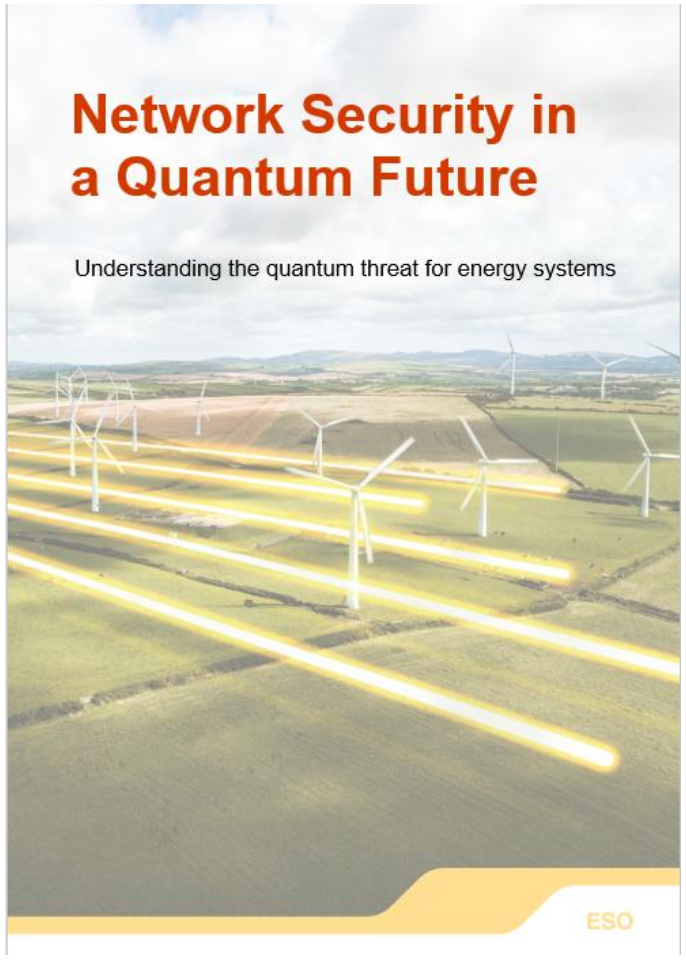
** Kill chain = description of the structure of a specific type of cyberattack*

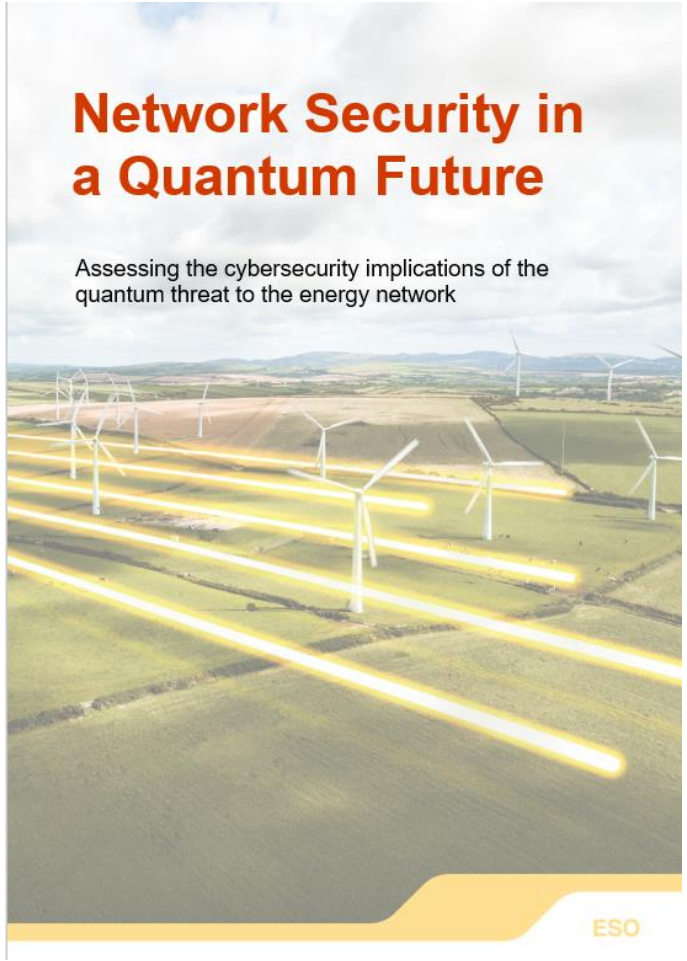
Testing the process by working through an energy system case study

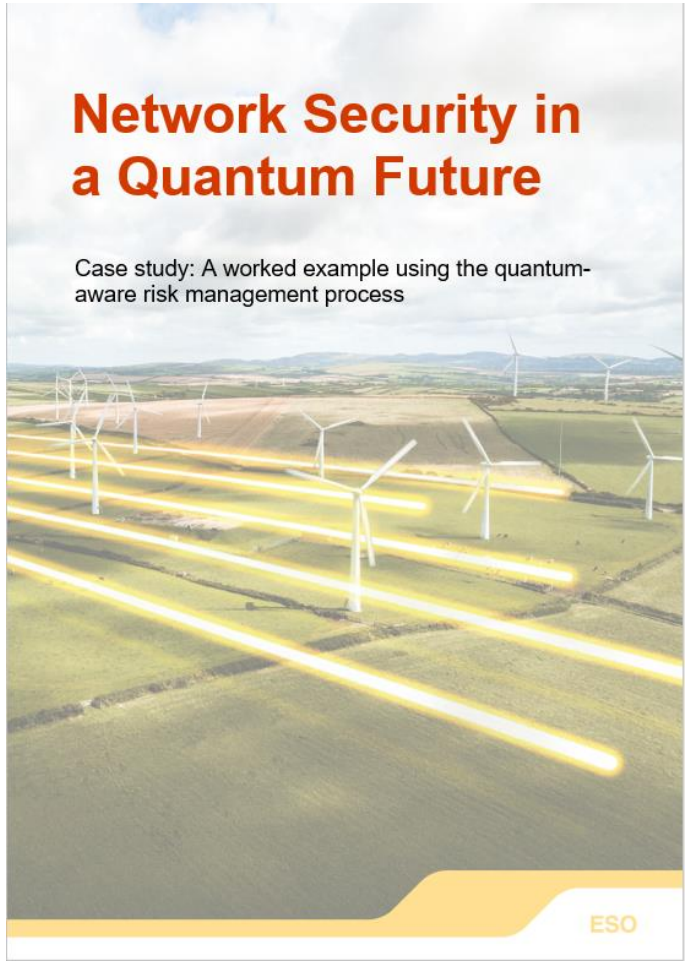
Exemplar test case: Quantum threat to energy network balancing system



Project deliverables are three reports on quantum threat, information model/risk management processes, and test case study







Reports can be accessed at: https://smarter.energynetworks.org/projects/10103996-2/

The Discovery phase has delivered clear benefits for the energy sector and consumers, but some gaps remain

Discovery Phase benefits

- ✓ Important **insight into how to characterise, quantify and mitigate the risk** posed by quantum computers to the energy sector
- ✓ **Quantum-Aware Risk Management process** can be used as-is for initial exploration of energy network vulnerabilities and mitigations
- ✓ Process can also form **basis for a future software tool** for energy sector security professionals
- ✓ Discovery reports provide policy makers and energy sector professionals with enhanced understanding of quantum impact and mitigations, to **support effective planning**
- ✓ **Energy-sector-specific** analysis and process

Gaps to address in order to realise value

- ❑ **Impact of quantum evolution (hardware and algorithms) over time is not captured** in the process - need for better capture of the impact on threat timelines
- ❑ **Uncertainty is not captured,** which limits the ability of the process to support decisions about mitigation strategies for the energy sector
- ❑ Model is not comprehensive, and **does not yet cover all risks** that have been identified
- ❑ Process itself is lengthy, and requires **significant manual work as well as training/subject matter expertise** for users

Next steps for Alpha: *Develop Quantum-Aware Risk Management software tool for the energy sector*

1) **Quantum-Aware Risk Management tool:** decision support software (minimum viable product/demo version)

   Benefit: Automates process of identifying, prioritising + mitigating quantum risks to energy network

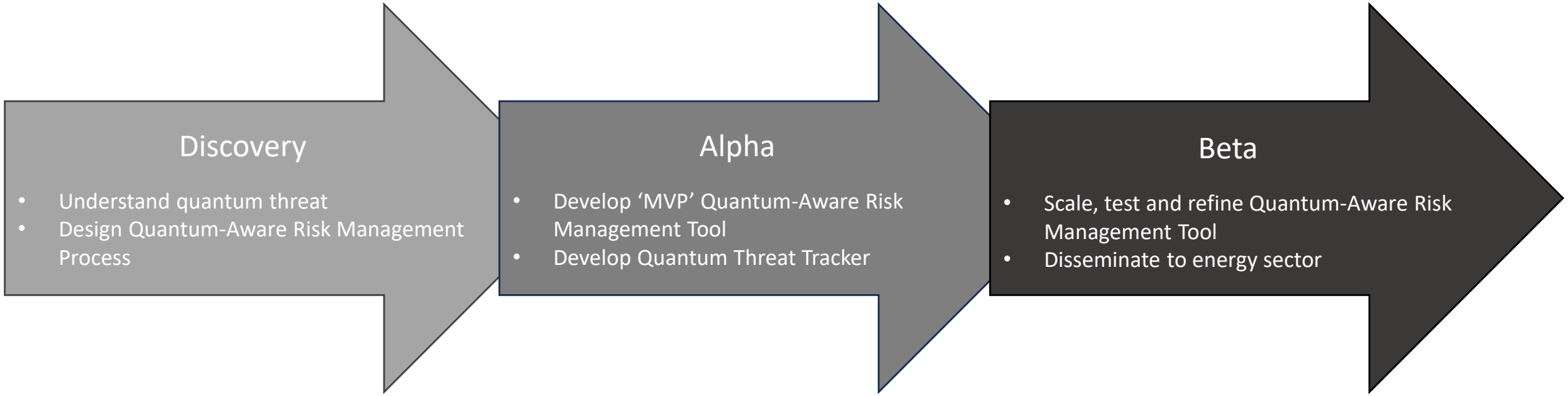
2) **Quantum Threat Tracker:** supporting analysis module capturing expert inputs

   Benefit: Enables rapid, repeatable, updatable assessment of quantum impact on energy-specific security scenarios; quantifies uncertainties + proposes key technology indicators as warning signs

Turns complexity into actionable intelligence for Energy sector

Supports resilience

Benefits realised will flow across all stakeholder groups



Thank you!

For more information, please contact:

ESO Innovation team
innovation@nationalgrideso.com

James Cruise (Cambridge Consultants)
James.cruise@cambridgeconsultants.com

Bob Oates (Cambridge Consultants)
Bob.oates@cambridgeconsultants.com