

# Network Security in a Quantum Future

May 2024

Assessing the cybersecurity implications of the quantum threat to the energy network



## Ofgem Strategic Innovation Fund Contributing Partners

	National Grid ESO
 <p>Part of Capgemini Invent</p>	Cambridge Consultants
 <p>THE UNIVERSITY <i>of</i> EDINBURGH</p>	University of Edinburgh
 <p>WARWICK THE UNIVERSITY OF WARWICK</p>	University of Warwick

## Executive Summary

The SIF Discovery project “Network Security in a Quantum Future” is the first step in providing much-needed insight into the scale and timing of the quantum threat for energy systems, and developing mitigations tailored to the technologies deployed in the UK energy system. This work has been undertaken by a consortium of National Grid ESO, Cambridge Consultants, the University of Edinburgh, and the University of Warwick.

The field of quantum computing opens up many new opportunities. The topic is extremely technically challenging, and its potential benefits and threats have attracted a great deal of academic research. One significant area of exploration has been the potential for quantum computers to undermine traditional cryptographic techniques, and consequently undermine the confidentiality, integrity and provenance of data protected by those techniques. However, the feasibility and implications of these threats for a real-world system that supports the critical national infrastructure of the UK, such as the energy network, is less well understood.

This cybersecurity analysis report, in conjunction with its sister report, “Understanding the quantum threat for energy systems” summarises the outputs of an investigation into the practical implications of the quantum threat to the energy sector and addresses the following questions:

1. How can we cut through the hype and understand the feasible threats that quantum computers pose to the security of energy systems?
2. How can security professionals make informed choices about how to secure energy infrastructure against quantum computers?
3. What does this mean in practical terms to the energy sector?

Key findings of the work are:

- Quantum computers are likely to represent a realistic threat to the energy sector and could do so as early as 2035.
  - In this timeframe, quantum-enabled attacks are likely to compromise the integrity, confidentiality, and provenance of data, through the ability to derive private shared secrets and keys from publicly shared data during key exchanges and certification publications.
  - These shared secrets will allow attackers to eavesdrop on encrypted communications, insert new commands into secure command and control lines, and fake the signatures of legitimate software publishers.
  - The time required to execute these attacks is likely to be an important factor when considering the feasibility of attack against a specific system. However, the advent of store-now, decrypt-later attacks (where an attacker harvests confidential encrypted data in the hope that they will be able to decrypt it when technology reaches a position to do so) demonstrates that this is not always the case.
  - The most likely threat actors are nation states, due to the high costs associated with creating and maintaining a quantum computer, and the skills required to meaningfully operate them. Initially these are likely to be Russia and China, but others will follow as the technology becomes more established.
- To make informed choices about how to secure energy sector infrastructure against quantum computers, it will be essential for energy network security stakeholders to make use of structured processes, tools, and frameworks, to ensure a comprehensive and effective approach. The initial Quantum Aware Risk Assessment process outlined in this report is a first step toward developing a usable approach for the energy sector. Key activities for security professionals are:
  - First, security stakeholders must understand where vulnerable software is employed within the system. The work undertaken in this project makes identifying vulnerable systems easier, by linking weaknesses in algorithms to higher-level software libraries and cryptographic frameworks that will be affected.
  - Then, stakeholders must assess the risk – understanding it and measuring it. As part of this work, we have designed a high-level methodology to perform quantum-aware risk assessments.

- Finally, stakeholders must select an appropriate mitigation to reduce that risk where appropriate. We have developed a taxonomy of mitigations, together with their characteristics, to support the selection of appropriate techniques.

The practical ramifications of the findings of this report for the energy sector are that:

- For many enterprise systems used within the sector, such as cloud computing and office networks, the transition to post-quantum computing will largely happen “under the hood” as large software companies such as Microsoft, Google, and Amazon move their systems to more secure implementations.
- However, systems within the energy network that lack crypto-agility and have severe computational constraints are likely to require special attention to ensure the security of critical systems.
- In addition, it will be important to characterise systems within the energy network where the change to post-quantum computing is not feasible.

The objective of this work is ultimately to build a robust and usable process for identifying what systems should be prioritised for upgrade in the short-term to avoid exposure to the quantum-threat, and identifying the most effective mitigations. Looking ahead, we have identified a number of next steps to progress towards development of an effective and usable Quantum Aware Risk Management process for the energy sector:

- **Embedding quantum timelines into risk management approach:**
  - *Challenge:* Existing techniques for estimating the risk posed by quantum computers do not provide a full picture, because they focus only on the timeline till the emergence of cryptographically relevant quantum computers, and not on the properties of subsequent quantum-enabled attacks. The full picture needs to combine the two, to enable organisations within the energy sector to identify what systems need attention when.
  - *Next step:* The proposed Quantum-Aware Risk Management process in this report attempts to resolve this by focussing on practical quantum-enabled attacks, but at present lacks the higher-level view of comparing the lifetime of systems against the probable date for the emergence of a cryptographically relevant quantum computer. Work needs to be done to merge the two approaches so that an energy organisation can develop a clear understanding of which systems require attention, and which systems are either low risk or will be managed by third-parties.
- **Improving scalability and usability of approach:**
  - *Challenge:* The risk management approach (Quantum Aware Risk Management process) must be simple and scalable enough to enable energy sector organisations such as NG ESO to set up best practices for managing the quantum threat, that ensure common principles are applied throughout the organisation. The approach as currently outlined is complex and likely too time-consuming to be easily scalable.
  - *Next steps:* To enable this, steps would include developing a simpler asset model that can be deployed at scale across the entire energy sector, in order to enable easier mapping of vulnerabilities to post-quantum cryptographic attacks. To identify all potentially vulnerable systems, a systematic discovery of systems that are reliant on public-key cryptography is required. This may require the employment of third-party crypto-finding tools and interrogation of the software bill of materials (SBOMS) of critical systems.
- **Developing a better heuristic to determine which mitigation to apply where:**
  - *Challenge:* In order to understand exactly which mitigations are feasible in different scenarios, more work needs to be done on characterising the mitigations and their implications. Examples of unknowns include an incomplete specification of what sort of system/device/communication channel can handle PQC. In addition, where key rotation frequency needs to be increased, there will be a commensurate increase in bandwidth consumption and latency, which is not yet characterised.
  - *Next steps:* It will be key to better characterise the practical implications of implementing PQC on embedded systems and how the protocols will be handled by networking middleware and security devices. We must also characterise the bandwidth and latency implications of

increasing key rotation frequency. The heuristic needs to evolve to take into account the challenges of incorporating crypto-agility into large-scale deployments. More work is required to systematically identify vulnerable systems within the energy sector and to address the wider issue of making sensible decisions in the presence of uncertainty that cannot be trivially resolved.

To ensure the proposed Quantum-Aware Risk Management process meets the desired objectives, it is not sufficient to address the next steps outlined above. It will also be critical to establish ongoing consultation and collaboration with energy security professionals (in the first instance, NG ESO), on priorities, costs and timelines; user interfaces, and the best way to ensure outputs are compatible with practical operational and IT processes.

---

Key supporting tools and analyses we have developed as part of this work (mapped to the key risk tasks above) include:

- **Identifying vulnerabilities:** A mapping from theoretical algorithmic attacks to vulnerable software libraries to aid understanding of the scale of the challenge (Section 2.3.1).
- **Understanding the risk:** A well-defined set of kill chains that explain how threat actors can launch attacks using quantum computers, and an assessment of their practicality (Section 2.3.3).
- **Understanding the risk:** An evidence-based threat model of likely quantum-enabled threat-actors produced from knowledge about quantum investment and the capability of nation states and historical and emerging attack trends (Section 2.4).
- **Measuring the risk:** A minimal asset model for characterising energy systems so their risk from quantum computers can be evaluated (Section 3.3).
- **Identifying mitigations:** A taxonomy of mitigations that can be used to manage the threat posed by quantum-enabled kill chains (Section 3.4).
- **Identifying mitigations:** A process for identifying risks posed by quantum-enabled threats and mapping them to the mitigation taxonomy (Section 3.6).
- A worked example, applying the process to an indicative energy sector system (Appendix 1).

# Contents

Executive Summary.....	3
Contents .....	6
<b>1 Introduction.....</b>	<b>8</b>
<b>2 Understanding the quantum threat to the energy sector.....</b>	<b>9</b>
2.1 Section Summary .....	9
2.2 The risk of cyber-attacks against the energy sector .....	9
2.2.1 Cybersecurity-relevant trends within the energy sector .....	10
2.3 Moving from theory to real-world vulnerabilities .....	11
2.3.1 Vulnerable software libraries .....	11
2.3.2 Other cryptographic vulnerabilities .....	12
2.3.3 Quantum-enabled kill chains .....	13
2.3.4 Attack timings .....	15
2.4 A quantum threat actor model for the energy sector .....	16
2.4.1 Approach.....	16
2.4.2 Cost considerations .....	16
2.4.3 Capability considerations.....	17
2.4.4 Threat actors: Nation States.....	18
2.4.5 Threat actors: Organised crime .....	20
2.4.6 Threat actors: Hacktivists .....	21
2.5 Quantum threat timeline .....	22
2.6 Conclusions .....	22
<b>3 Methodology for performing quantum-aware risk management.....</b>	<b>24</b>
3.1 Section summary .....	24
3.2 Quantum risk estimation in the literature .....	24
3.3 Asset model .....	25
3.3.1 Functional assets .....	26
3.3.2 Computational assets .....	26
3.3.3 Operational information assets .....	27
3.3.4 Communication channel assets.....	27
3.3.5 Public-key cryptography assets.....	28
3.4 Mitigation taxonomy.....	28
3.4.1 Post-quantum cryptographic algorithm selection .....	30
3.5 Process Derivation.....	34
3.5.1 Prepare .....	34
3.5.2 Categorise.....	35
3.5.3 Select.....	35
3.6 Quantum Aware Risk Management Process Summary .....	36
3.6.1 Prepare .....	36

3.6.2	Categorise.....	36
3.6.3	Select.....	36
3.6.4	Applying the process to an indicative energy system.....	36
<b>4</b>	<b>Conclusions .....</b>	<b>37</b>
4.1	Key outputs from this work .....	37
4.2	Future work.....	37
<b>5</b>	<b>References .....</b>	<b>39</b>
<b>1</b>	<b>System of interest.....</b>	<b>43</b>
<b>2</b>	<b>Model analysis.....</b>	<b>43</b>
2.1	Prepare .....	43
2.1.1	Performing a system risk assessment.....	43
2.1.2	Common controls identified .....	48
2.2	Categorise .....	49
2.3	Select.....	49
<b>3</b>	<b>Conclusions .....</b>	<b>56</b>

# 1 Introduction

Quantum computers represent more than a simple computational speedup over traditional computing techniques; instead they represent a significant paradigm shift in how algorithms and data are represented and processed.

The SIF Discovery project “Network Security in a Quantum Future” is the first step in providing insight into the scale and timing of the threat for energy systems, and developing mitigation tailored to the particular technologies deployed in the UK energy system. This work has been undertaken by a consortium including National Grid ESO, Cambridge Consultants, the University of Edinburgh, and the University of Warwick.

In the sister report “Understanding the quantum threat for energy systems” the current state of quantum computing research is explored, and a number of cryptographically relevant algorithms are identified. These algorithms threaten to undermine assumptions contained within modern cryptography about the amount of time it would take for a motivated attacker to compromise the confidentiality and integrity of secured data.

However, the complexity of quantum computers and the fear, uncertainty and doubt that frequently pollutes the cybersecurity sector, means that a lot of hype has been generated about these threats. As a result, this report, in conjunction with its sister report, aims to answer the following questions:

- How can we cut through the hype and understand the feasible threats that quantum computers pose to the security of systems?
- How does a security professional make informed choices about how to secure their infrastructure against quantum computers?
- What does this mean in practical terms to the energy sector?

The report begins in Section 2 by characterising the quantum threat to the UK energy sector. It does so by forming an understanding of the current threat landscape for the UK energy sector and by looking ahead using the 10-20 year horizon suggested by the sister report “Understanding the quantum threat for energy systems” as the likely period in which quantum computers will become cryptographically relevant.

Section 2.3.3 goes on to identify how theorised quantum attacks on specific algorithms can be translated into practical kill chains on software libraries used by the energy sector.

In Section 3 the groundwork is performed for generating a repeatable, scalable process for assessing if a given system is vulnerable to the quantum threat. The analysis goes further than other approaches in the literature, by characterising scenarios when post-quantum cryptography is *not* the best solution, and by developing a formal asset model to capture the information required to perform such an analysis.

With these building blocks in place, the process is derived from classical risk assessments and presented in short form in Section 3.6.

In Appendix 1, a simple system, chosen to be indicative of energy sector applications, is analysed using the proposed methodology.

Finally in Section 4, conclusions are drawn about the work completed, and suggestions for future directions of the research are proposed.



## 2 Understanding the quantum threat to the energy sector

### 2.1 Section Summary

This section explores the current and future cybersecurity threat landscape for the UK energy sector and how quantum computers will change it.

It addresses the following questions:

1. Will quantum computers ever represent a realistic cyber threat to the energy sector and if so, when?
  - Quantum computers are likely to represent a realistic threat to the energy sector and could do so as early as 2035.
2. What are quantum-enabled attacks?
  - Quantum-enabled attacks are likely to compromise the integrity and confidentiality of data through the ability to derive private shared secrets and keys via publicly shared data during key exchanges and certification publications. These shared secrets will allow attackers to eavesdrop on encrypted communications, insert new commands into secure command and control lines and fake the signatures of legitimate software publishers. The time required to execute these attacks is likely to be an important factor in their practicality for many applications. However, the advent of store-now, decrypt-later attacks demonstrates that this is not always the case.
3. Who are the most likely threat actors?
  - The most likely threat actors are nation states due to the high costs associated with creating and maintaining a quantum computer, and the skills required to meaningfully operate them. Initially these are likely to be Russia and China, but others will follow as the technology becomes more established.

Section 2.2 characterises the current cybersecurity profile of the energy sector and looks ahead to how that might change given current technology trends.

The report goes on to identify how theorised quantum computer attacks against specific algorithms, can have meaningful impacts on real software being used within the energy sector, concluding by identifying four quantum-enabled attack kill chains (Section 2.3).

Combining the cybersecurity landscape identified in Section 2.2 with the quantum-enabled attacks characterised in Section 2.3 allows us to build a full adversarial threat model for quantum-enabled attacks against the energy sector in Section 2.4.

### 2.2 The risk of cyber-attacks against the energy sector

Globally, the energy sector is a consistent, high-priority target of cyber-attacks, with an average of around 10% (9.42% mean, 10.7% median) of all attacks annually targeting the sector according to [1]. Attackers, hostile to the UK, are highly motivated to target this sector as it is critical to national and economic security. The current UK national risk register determines that there is a 5-25% likelihood of a cyber-attack against infrastructure (including energy) within the next two years and a moderate impact (41-200 fatalities, 81-400 casualties, or hundreds of millions of pounds in economic cost) on the UK as a whole [2] though this is thought to be a conservative estimate.

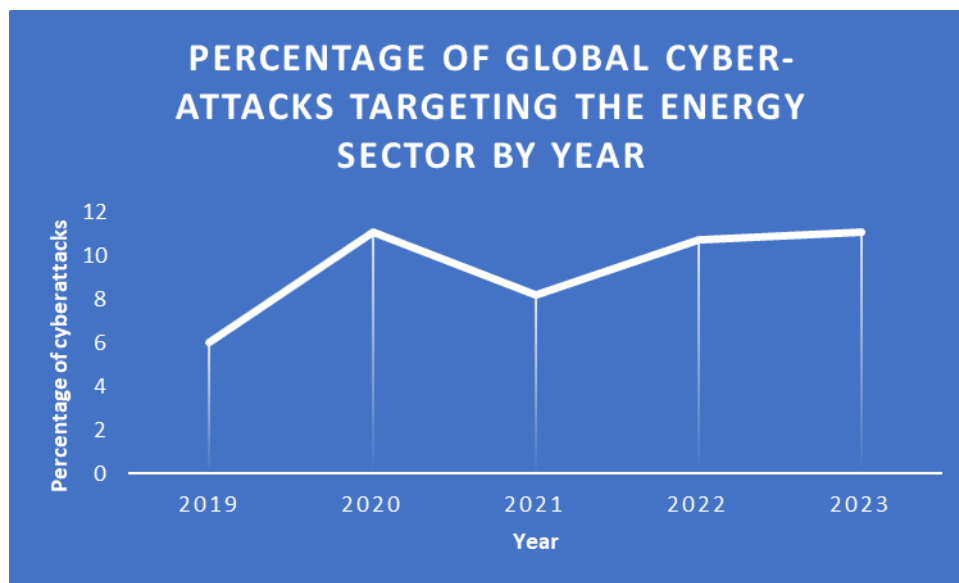


Figure 1 – The percentage of global cyber-attacks targeting the energy sector by year. Data taken from [1]

The impact of a well-coordinated cyber-attack on the energy sector is potentially wide-ranging. Not only would there be an immediate impact for domestic properties, industrial systems and civil buildings such as hospitals, there are a number of secondary impacts from other critical infrastructure being unable to operate in the absence of power.

The Colonial Pipeline [3] incident in the United States illustrates the immediate and far-reaching impacts of such cyber-attacks against energy resources, where a ransomware attack led to the suspension of operations, affecting the supply of over 2.5 million barrels of refined petrol daily. In terms of direct attacks against the electricity transmission sector, 2015's attack by Russian state actors disrupted the power to 225,000 customers [4].

Internationally Chinese state-sponsored actors have also shown an interest in disrupting energy systems via their 'Volt Typhoon' campaign within The United States, which, at the time of writing, is thought to be an ongoing campaign [5].

### 2.2.1 Cybersecurity-relevant trends within the energy sector

Given the expected 10-20 year timescales associated with the creation of a cryptographically-relevant quantum computer, it is important to not simply consider the energy sector as it is today, but the direction of travel for the future.

The UK electricity grid is aiming to run on 100% green energy by 2035 [6]. In order to achieve this there will be a growth in production and use of renewable energy, which in turn will drive a demand for energy storage (to compensate for periods of unfavourable weather conditions) and greater distribution of power generation across potentially multiple micro-grids.

Modern green energy systems (wind, solar, nuclear) are typically highly digitised, enabling high-value decisions to be made based on collected data about the environment and the status of the grid, sometimes with full autonomy. Energy storage systems, such as advanced battery energy storage, also rely heavily on digital systems to schedule their charging/discharging and, in some cases, maintain their physical safety. The rise of digitisation within the energy sector as a whole will make monitoring network infrastructure at scale a complex task.

Distributed systems represent a further shift in cyber risk, as their threat surface is much larger, with multiple network interfaces and remotely accessible digital systems. Highly distributed systems also tend to have more cost constraints for individual nodes which can, in turn, result in lower-performance computational systems at the edge that are unable to support computationally expensive security controls. Conversely, greater use of distributed systems could potentially reduce overall impact of attack compared to a scenario with a large single-source generator, if segregated correctly to prevent multiple, simultaneous attacks being launched.

The movement towards decentralised systems also suggests that there will need to be more local control of frequency and stability of systems, such as isolated microgrids. Organised decentralisation typically results in a much harder security problem due to the need to establish trust across multiple organisations. Standardisation is a possible solution to this challenge but can slow innovation and become cumbersome.

A further challenge is that the market-driven approach to energy generation used by the UK (and many other countries) means that distributed digital systems will increasingly need to be interoperable between organisations, communicating with each other using common, well-defined protocols. Without adequate security, this rise in interconnectedness could allow attackers to pivot between systems and cause widespread harm. For example, in [7] it is demonstrated that a coordinated attack on off-shore windfarms could have a destabilising impact on the entire grid.

Finally, increased geopolitical tensions are likely to increase the motivation of specific nation states to target the UK. As conflicts between nations become more explicit, the likelihood of disruptive cyber-attacks will continue to increase.

## 2.3 Moving from theory to real-world vulnerabilities

To understand if a given system is vulnerable to attacks that have been enabled by quantum computers, simply knowing which algorithms are vulnerable is insufficient.

It is important to a) understand what software libraries are vulnerable as a result of these vulnerable algorithms, b) understand the attacks that these vulnerabilities enable and, c) assess specific system(s) to evaluate if the attacks are feasible.

### 2.3.1 Vulnerable software libraries

In the sister report “Understanding the quantum threat for energy systems” it is explained that a number of key-exchange protocols and digital signature protocols, including some that are commonly used across the energy sector, are vulnerable to attacks based on quantum computers. These include:

#### Key exchange protocols:

- Rivest-Shamir-Adleman (RSA)
- Diffie-Hellman (DH)
- Elliptic Curve Diffie-Hellman (ECDH)
- Menezes-Qu-Vanstone (MQV)

#### Digital Signature protocols:

- Digital Signature Algorithm (DSA)
- Elliptic Curve Digital Signature Algorithm (ECDSA)
- Edwards Curve Digital Signature Algorithm (EdDSA)
- RSA

Software libraries and cryptographic frameworks have a complex relationship with cryptographic algorithms. Specific library versions can support multiple algorithms, with differing degrees of vulnerability. Table 1 is an indicative list of high-profile cryptographic frameworks used within energy sector assets that are made vulnerable by quantum computers.

<b>Cryptographic framework</b>	<b>Algorithms used</b>	<b>Example of applications in Energy</b>
<b>TLS 1.2</b>	<i>RSA &amp; Diffie-Hellman</i>	<i>Encrypting traffic between devices or organisations to support energy markets</i>
<b>TLS 1.3</b>	<i>Diffie-Hellman</i>	<i>Encrypting traffic between devices or organisations to support energy markets</i>
<b>X.509 Certificates</b>	<i>Typically use TLS for comms and various PKI algorithms for certificate keys</i>	<i>Signing software/firmware to be installed in sensitive areas such as power generation facilities or control rooms</i>
<b>https</b>	<i>TLS supported by the use of X.509 certificates</i>	<i>Encrypting client/server comms and authentication for portals that allow remote operators to view distributed energy assets</i>
<b>OpenSSL 3.X</b>	<i>Diffie-Hellman</i>	<i>Encrypting traffic between devices or organisations to support energy markets</i>
<b>SSH</b>	<i>Diffie-Hellman</i>	<i>Establishing remote connections to administer distributed energy resources, such as wind turbines</i>

Table 1 – Cryptographic frameworks affected by quantum vulnerable cryptographic algorithms

It is important to note that OpenSSL and the X.509 certificate already have post-quantum branches that use post-quantum cryptography to achieve their goals [8] so for many systems the process of upgrading may be trivial.

The list presented in Table 1 highlights some of the complexity associated with going from knowing what algorithms are vulnerable, to knowing what software systems are vulnerable. The process of cryptographic vulnerability discovery across a large organisation is a significant challenge in of itself, though tools do exist to support this activity.

### 2.3.2 Other cryptographic vulnerabilities

As discussed in the sister report “Understanding the quantum threat for energy systems”, quantum computing also threatens a number of other encryption methods such as symmetric encryption, hash functions and blockchain based methodologies.

The threat to symmetric encryption manifests as a modest speedup in the time it takes to use brute force to decrypt an encrypted message. This speedup is not currently considered a major threat and is trivially evaded with little overhead by increasing the key lengths used by the existing traditional algorithms.

The threat to hash functions is a similar, modest speedup in the time it takes to find hash collisions, which has the potential impacts of bypassing certain password mechanisms and allowing attackers to undermine the integrity of messages without detection. Again, this is trivially evaded with little overhead by increasing the key length.

Blockchain technologies use a wide variety of computational techniques to ensure their security. Quantum computers undermine these in two ways: 1) Increasing the computational power of the adversary, allowing them to prevent transactions from being completed and reverse transactions that were performed while they had control of the network (the so-called 51% attack [9]), 2) By allowing attackers to forge digital signatures for implementations that use traditional digital signature algorithms. Blockchain technology is not currently widely used in the energy sector. Future deployments of blockchain should be assessed in terms of their resilience to quantum-enabled attacks. This report will not elaborate further on blockchain vulnerabilities and risks beyond highlighting general PKI and digital signature risks.

### 2.3.3 Quantum-enabled kill chains

A “kill chain” is a stepwise description of a cyberattack that explains how the attacker will move from initial compromise to achieving their objectives. By mapping out these steps it is possible to identify all the opportunities that a defender has to stop the attack progressing.

The attacks that could be enabled by quantum computers are many and varied. However, four generalised kill chains are included below that support the analysis contained within this report:

1. Basic eavesdropping (K1)
2. Advanced eavesdropping (K2)
3. Issuing malicious commands over an encrypted connection (K3)
4. Installing signed malicious firmware/software (K4)

While there are other kill chains that are enabled by quantum computers, the vast majority are variations of the methods outlined in these four.

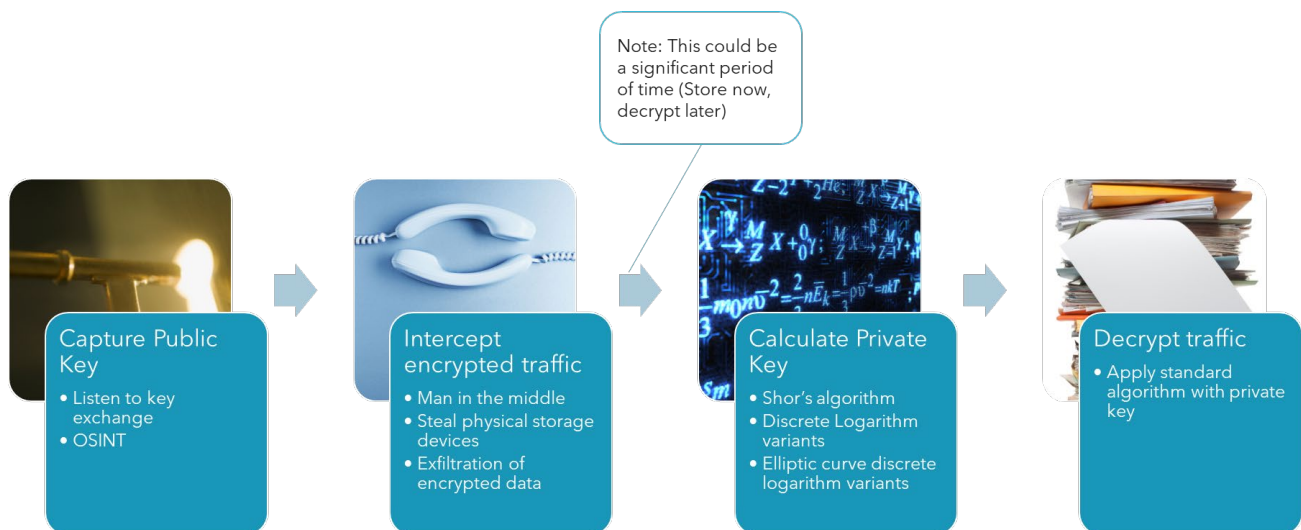


Figure 2 – Basic eavesdropping kill chain (K1)

The basic eavesdropping example is only included to illustrate how a quantum computer can access confidential data at a trivial level. The basic eavesdropping kill chain itself is not a realistic attack, but understanding how it works is essential to understanding how the more complex kill chains that could realistically be used in an attack work. For basic eavesdropping it is assumed that all the data of interest is encrypted via a quantum-vulnerable public-key encryption algorithm. This is the simplest illustrative example of how an attacker could use a quantum computer to access confidential information. However, in the real world this is highly unlikely as the computational cost of public-key cryptography means that it is typically only used to share the private key for a symmetric encryption algorithm. Note that the gap between steps 2 and 3 can be any length of time, facilitating “store now, decrypt later” attacks. The term “OSINT” in the diagram refers to “Open-Source Intelligence” – i.e. gathering publicly available information.

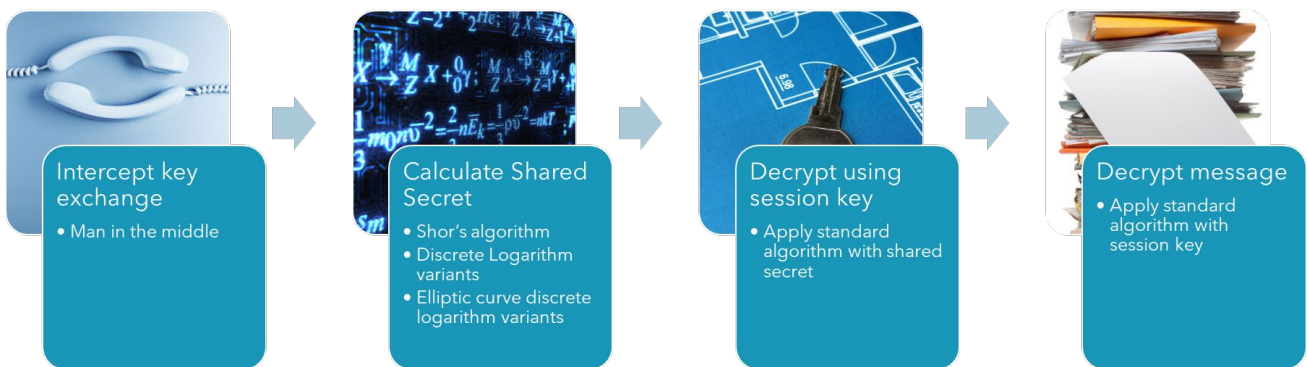


Figure 3 – Advanced eavesdropping kill chain (K2)

A more complex eavesdropping kill chain is presented in Figure 3, which represents a more realistic scenario. In this kill chain, the private key exchange used to establish a communications session is intercepted, as well as the encrypted traffic. The quantum computer is used to identify the shared secret, which is in turn used to decrypt that session's data using a classical algorithm. In a similar way to basic eavesdropping, once the key exchange and data exchange has been intercepted, the data can be decrypted much later, enabling store now, decrypt later attacks.

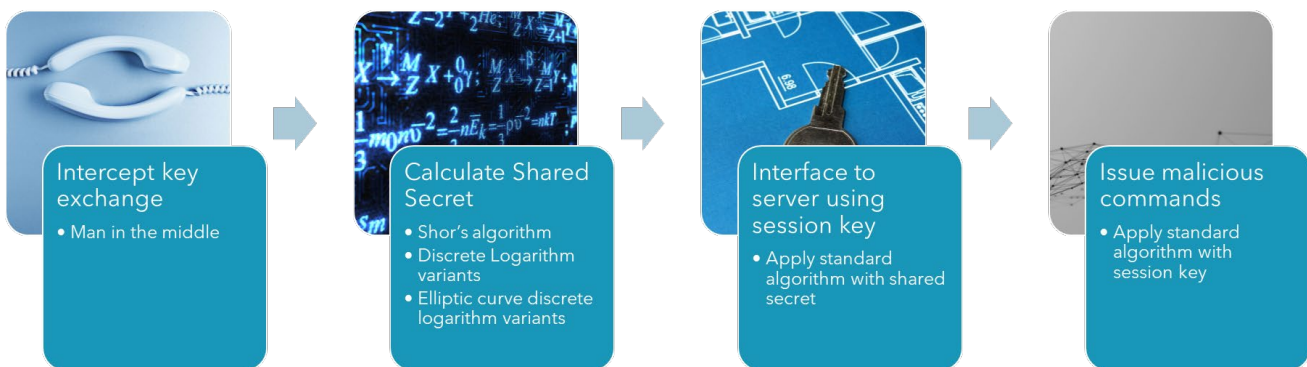


Figure 4 – Issuing malicious commands over an encrypted connection kill chain (K3)

The issuing of malicious commands requires a threat actor to pose as a legitimate system or actor, by breaking the assumption that if they have the private key, they must be a legitimate user. Again, this attack begins by intercepting the key exchange for the session and calculating the shared secret with a quantum computer. By using the session key, the malicious user can see all sent messages (as per “advanced eavesdropping” K2) and, via maintaining their man-in-the-middle position, send malicious commands by encrypting them with the session key and transmitting them to one of the parties communicating. This kill chain is time sensitive. If the session key rotates before the malicious user can calculate the shared secret, they cease to be able to communicate with the target system.

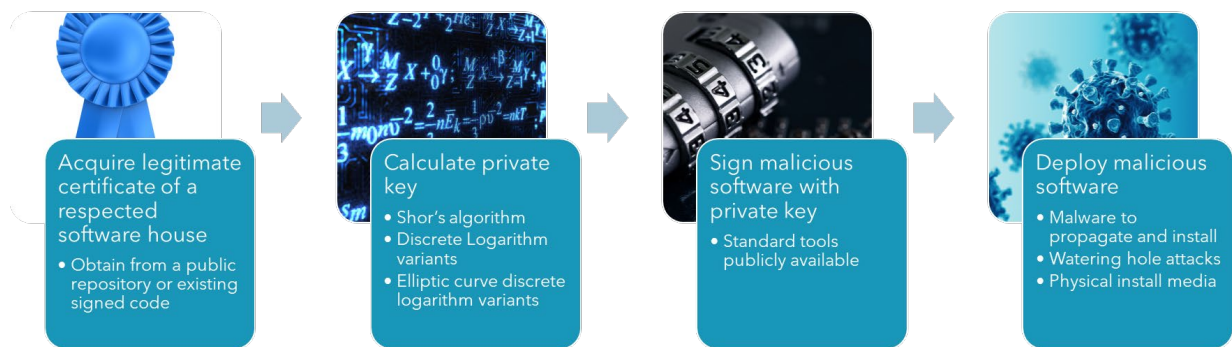


Figure 5 – Installing signed malicious firmware/software kill chain (K4)

In this example the attacker wishes to override a secure software installation process by signing malicious code to make it look like a trusted supplier has provided it. This would allow the distribution of such malicious code via auto-update systems, or via watering hole attacks (malicious control system software has been deployed via this vector before, though not with a false signature [10]). In this attack, the attacker has as long as the authentic certificate is valid to identify the private signing key and sign their software to make it appear to be authentic.

### 2.3.4 Attack timings

In the sister report “Understanding the quantum threat for energy systems” the approximate timings for calculating the private keys from the public keys are given for RSA and elliptic curve algorithms (reproduced in Table 2).

Security Strength (minimum)	RSA (Google / KTH Royal Institute of Technology / Swedish NCSA)			Elliptic curve (Korea University)		
	Key length	# Physical qubits	Runtime (rounded up)	Key length	# Physical qubits	Runtime (rounded up)
112	2048	20 million	8 hours	224	4.63 million	47 days
128	3072	38 million	14 hours	256	5.81 million	63 days
192	8192	140 million	4 days	384	8.32 million	261 days
256	16384	270 million	19 days	521	12.3 million	705 days

Table 2 – Time required to calculate the private key from the public key using quantum computers. Taken from the sister report “Understanding the quantum threat for energy systems”

This table implies that even for the least secure implementation of RSA considered (2048 bit), it would take an attacker with a quantum computer (using our current understanding of the technology) eight hours to calculate the private key. From that point, there would be additional, traditional computation required to decrypt or sign (depending on the kill chain) to launch the attack.

This eight-hour bound will be used throughout this analysis and is based on our current understanding of the technology and could be reduced as the technology advances. It should be kept up to date by continuing vigilance of developments in the quantum computer sector.

For the eavesdropping kill chains (K1, K2) this bound may or may not be a problem. For store now, decrypt later attacks, the attacker is assuming that the captured data will be useful in many years' time. However, in scenarios where confidentiality is only a priority for a limited window, this lower bound may be important when deciding whether a system is vulnerable to quantum-enabled attacks.

For the malicious command kill chain (K3), the attacker only has as long as the session key is active to insert spoofed messages. Such ephemeral keys have highly variable lifetimes (measurable in minutes, hours or even days depending on server configuration). Long-lived keys may provide an attacker with a limited opportunity to insert malicious commands.

For the installing malicious software/firmware kill chain (K4) a system is vulnerable for as long as the certificate of the organisation is not revoked either by placing it in a revocation list that can be checked during the installation process or by updating the trust anchors embedded within the device. Organisations rarely rotate their private keys unless they suspect they have been compromised, meaning that the window of opportunity for an attacker could be several years.

## 2.4 A quantum threat actor model for the energy sector

### 2.4.1 Approach

An adversarial threat model aims to define the type of attacker who is likely to launch an attack and what their motivations might be for doing so. This knowledge allows defenders to prioritise their resources in a way that mitigates the most likely, high-impact attacks first.

This threat model focusses on adversaries with the capabilities, resources, relationships, and behaviours to launch a quantum-enabled attack. This "attacker-centric" modelling method emphasizes understanding the adversaries' goals, their sophistication, and the methods they employ to achieve these goals.

### 2.4.2 Cost considerations

To effectively match threat actors to the quantum threat, it is necessary to identify the costs associated with using a quantum computer to target vulnerable systems. The primary costs of doing so largely break down into the following categories:

- Hardware costs
- Initial ramp-up costs
- Costs associated with running jobs

The hardware costs of quantum computers, especially those capable of running Shor's algorithm effectively (i.e., factoring large integers) are likely to be substantial, estimated as reaching millions of dollars. This includes not just the quantum processors but also the necessary cooling systems as many quantum computers operate at temperatures close to absolute zero utilising superconductors and phase change cooling. Furthermore, the cost of parity error correction systems and the classical computing infrastructure needed to control the quantum system and interpret its results must be included in any cost reckoning.

The initial ramp-up for a quantum computing system demands significant investments in both time and money. This phase involves:

- **Installation and Setup:** Physically setting up the quantum computer and integrating it with the necessary peripherals and classical computing resources.
- **Calibration and Testing:** Quantum systems require meticulous calibration to operate correctly, which can be a time-consuming and costly process.
- **Software Development:** Developing or adapting algorithms (like Shor's) to run on specific quantum hardware, including error correction and mitigation strategies.

This phase is also typically expensive because it requires specialized knowledge and equipment. However, once completed, the cost of running new jobs can decrease significantly, though ongoing maintenance and calibration will still incur costs.



Once a quantum computer is online and operational, the marginal cost of running additional jobs, such as executing Shor's algorithm for different numbers, can be relatively low compared to the initial setup. However, there are a few considerations:

- **Energy Consumption:** While individual quantum operations consume very little energy, the cooling systems and classical computers required to support quantum computing can be energy intensive.
- **Maintenance and Calibration:** Quantum computers need regular recalibration and maintenance to remain operational, which adds to the operational costs through the need for qualified technicians and access to equipment and consumables such as cooling chemicals.
- **Software and Algorithm Development:** Adapting or optimizing algorithms for specific problems or hardware changes can require significant effort and expertise.

Once the system is operational, the cost of running new jobs can be lower, but maintenance, calibration, and energy consumption will continue to contribute to ongoing expenses. It's also important to note that as quantum technology evolves, these costs and the efficiency of quantum operations will likely change.

The extremely high costs are likely to initially place quantum computers beyond the reach of many threat actors for the foreseeable future. As a result, we would expect cryptographically-relevant quantum computers to only be available to state-funded institutions or actors. However, quantum-compute-as-a-service platforms are already available based on the current level of technology. This implies that access to quantum computers could become available to a wider range of threat actors once the technology makes the shift from nation state to corporation.

### 2.4.3 Capability considerations

To scope the threat model, we have also considered which known nation states, with a history of targeting the energy sector, have also been investing in quantum technology.

This initial approach generates a base set of potential threat actors to consider. Additional threat actors have also been considered if we believe they may obtain secondary access to the technology, and/or may emerge as hostile nation state actors in the future. As capability is a difficult parameter to measure directly, we use financial investment into the technology as a proxy for capability. It should be noted that the figures presented in **Error! Reference source not found.** are based on the publicly announced investments and may be much larger for countries with less transparency into their funding allocations.

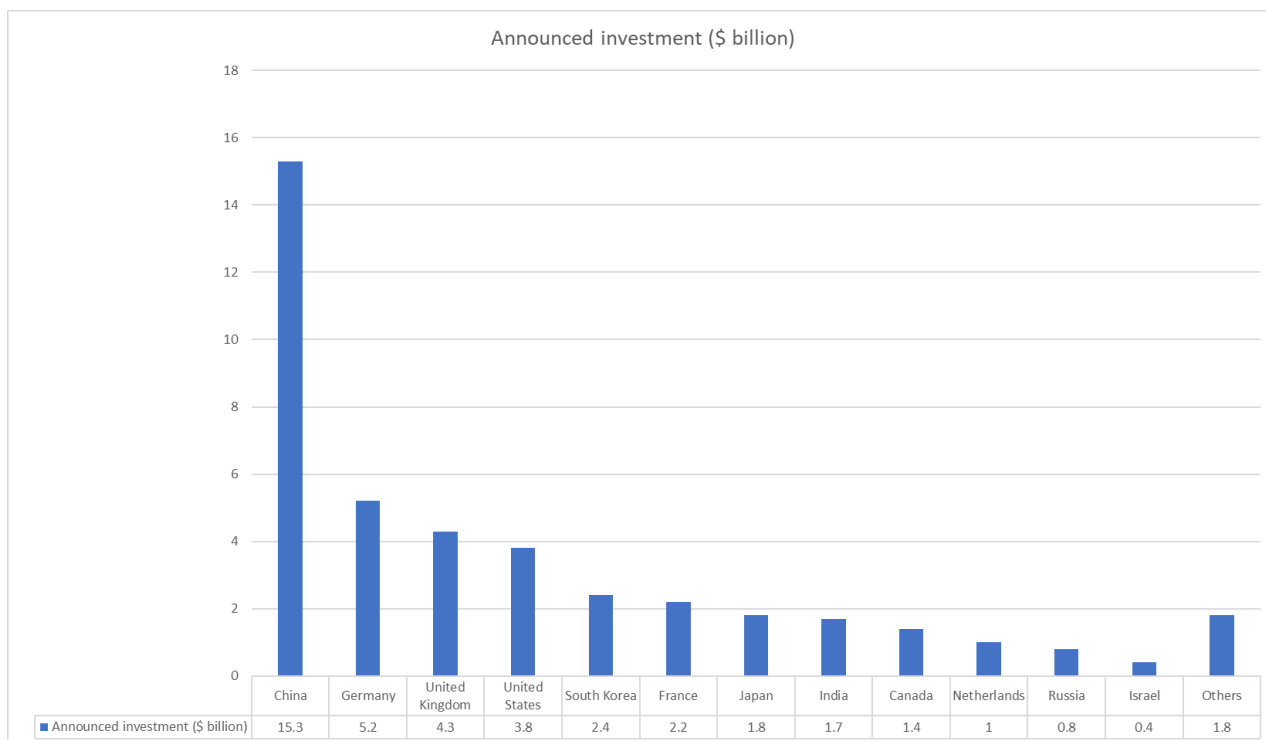


Figure 6 – Investment into quantum computing to date by nation. Data taken from [11]

Figure 6 outlines the key nation state investors in quantum computer technology, a good proxy for the level of capability the nation will have for developing and utilising such systems in the future. With this list in mind, we can move on to explore which nation states have previous form for targeting the energy sector.

#### 2.4.4 Threat actors: Nation States

A number of nation states have a reputation for targeting UK infrastructure. In the National Cyber Security Centre’s annual review of 2023 [12] China, Russia, Iran and The Democratic People’s Republic of Korea (DPRK) are explicitly listed as aggressive threat actors. This is reinforced by Microsoft’s threat actor naming taxonomy [13], which ascribes labels to threat actors from Russia, North Korea (also known as DPRK), China and Iran. Of these countries, China and Russia are in the list of quantum capable countries in **Error! Reference source not found.**

While Russia’s public investment in quantum technologies may appear modest [14], it has made significant progress in developing its own quantum capability, successfully developing, and deploying a 20-qubit quantum computer [15], four more qubits than its prior successful deployment only a year prior. This suggests that the total investment by Russia into quantum computing technology may be higher than publicly announced. The UK and its allies have directly attributed a series of cyber-attacks to the Russian military intelligence service [16]. These attacks reveal Moscow’s technical capability to disrupt critical national infrastructure.

Both Iran and DPRK are not likely to publicly announce quantum computing investment, but of the two countries Iran has made claims about advances in quantum technology, though those claims have been disparaged by most experts [17]. Iran is likely to continue expanding its cyber capabilities amidst ongoing geopolitical tensions and international sanctions. Iran’s active engagement in cyber operations provides a foundation for integrating quantum technologies into its cyber arsenal. The SNDL threat could be particularly relevant, as Iran might see value in collecting encrypted data that could later be decrypted with quantum advancements, offering insights into adversaries’ strategies or sensitive political and military communications.

Looking to the future, India, one of the countries investing into quantum computers, is emerging as a possible future cyber threat [18], so has been added to the list. India stands out with its vast IT and engineering talent. Despite its current modest investment in quantum technologies [14], India’s considerable production of IT and engineering expertise sets a foundation for significant growth in cyber capabilities. India’s targets for cyber-attacks could be aligned with Russia’s targets, due to their close military and economic relationship.

Brazil have begun a modest investment into quantum technologies [19], and are emerging as a realistic cyber threat [20]. However, there is no OSINT (open-source intelligence) evidence linking the cyber threat actors in Brazil to government activity. This lack of link between the nation state and the threat actors implies there is no short-term quantum threat from Brazilian hackers.

Finally, Pakistan has a long history of skilled cyber threat actors, such as the advanced persistent threat group APT-36 (also known as “Transparent Tribe”) [21]. In a similar manner to Brazil, Pakistan has also begun a modest investment into quantum computer technology, opening a dedicated research and education facility in 2023 [22]. While its current quantum investment is low [23], between 2025 and 2030, Pakistan could significantly enhance its cyber capabilities, influenced by its strategic security interests and alliances, notably with China. Pakistan's focus might lean towards developing defensive cyber capabilities to protect its critical infrastructure and military communications, considering its regional security dynamics, especially with India. However, the collaboration with China under the China-Pakistan Economic Corridor (CPEC), part of the Belt and Road Initiative, could provide Pakistan with access to advanced technologies, including quantum computing capability.

Table 3 outlines the typical goals and access levels to quantum computing for these nations, reflecting their strategic priorities and technological capabilities projected into the mid-2030s and beyond.

Threat Actor	Typical Goals	Access to Quantum Computers
China	Technological superiority, espionage, economic growth, and global influence.	High; significant national investment in quantum research and development.
Russia	Political influence, disrupting adversaries, maintaining regional dominance.	High; although Russia has a lower level of investment into the technology than other countries, they are typically highly active in cyber-attacks against the energy sector.
Iran	Regional dominance, evading sanctions, strengthening defence capabilities.	Low; growing capabilities, possibly with external assistance from allies.
India	Economic growth, national security, technological leadership.	Low; modest investments in technology sectors, including quantum computing.
Pakistan	National security, regional influence, military parity with India.	Low; limited resources but potential strategic investments in specific areas like security.
Brazil	Economic development, enhancing scientific capabilities, improving national security.	Low; emerging focus on leveraging quantum technology for various sectors.

Table 3 – Nation state threat actors, their goals and access to quantum computers


Nation states are highly varied in their motivations and it is considered that all of the kill chains discussed in Section 2.3.2 are potential use cases for these actors. Store-now, decrypt-later attacks are already being executed by nation state actors, who are harvesting encrypted, confidential documents now that may still be useful for intelligence when quantum computers enable them to be decrypted.

#### 2.4.5 Threat actors: Organised crime

Nation states are the most likely threat actors to achieve early access to quantum computers due to their high resource / high capability profile. However, in the longer term, quantum computer as a service and access to research prototypes may open access to a wider range of threat actors.

Organised crime has proven to be an adaptable and resourceful adversary. Financially motivated actors could see gains from intercepting confidential data (eavesdropping kill chains K1 and K2) or gaining access to vulnerable systems in order to hold them to ransom (either via issuing malicious remote commands or by installing signed ransomware using the appropriate kill chains, kill chains K3 and K4 respectively).

In Russia, in particular, there is evidence to suggest a symbiotic relationship between Russian state cyber efforts and organized cybercrime. Russia's state security services have been increasingly adopting tactics reminiscent of organized cybercrime groups. The Main Directorate of the General Staff of the Armed Forces of the Russian Federation (commonly known as the GRU) has been at the forefront of these activities and while



...THE LINES BETWEEN ORGANISED CRIMINALS AND STATE ACTORS ARE SOMETIMES BLURRED. STATE-LINKED ACTORS CAN USE SERIOUS AND ORGANISED CRIME AS A DESTABILISING FORCE, USING PROXIES TO OBSCURE THEIR ACTIVITY. THIS CAN MAKE IT HARDER FOR THE UK TO ACHIEVE ITS NATIONAL SECURITY OBJECTIVES AROUND THE WORLD. OUR RESPONSE TO SUCH STATE-LINKED ORGANISED CRIME GROUPS IS PART OF THE UK'S RESPONSE TO THE WIDER THREAT POSED BY SUCH STATES.

UK Serious and Organised Crime Strategy [44]

the GRU's physical actions on foreign territories have received significant media attention, their hostile cyber activities often fly under the radar. Notably, some of the malware infection methodologies used by the GRU mirror those commonly employed by cybercriminals [24].

There is little public evidence that organised criminal gangs are targeting the energy sector specifically. Instead, attacks are typically against targets of opportunity rather than driven by sector-specific interest.

The high costs associated with gaining access to quantum computers, along with the high degree of technical capability required to operate them, means that organised crime is unlikely to be an early adopter of quantum-enabled attacks. However, the lines between nation state actors and organised criminal gangs are blurring, with increased levels of cooperation between the two.

#### 2.4.6 Threat actors: Hacktivists

Recent activities have seen hacktivist groups targeting operational technology within the energy sector for disruptive purposes, indicating a shift towards more politically motivated cyber operations. These operations have targeted critical infrastructure in several countries, demonstrating the global nature of the threat. For instance, hacktivist campaigns have claimed successes in compromising the operational technologies of Russian energy companies and municipal electrical systems [25] (in Russian – translated using Google Translate service). However, given the high costs and capability demands of quantum-enabled attacks, such ideologically motivated attackers are not viewed as likely adopters of quantum computers.

## 2.5 Quantum threat timeline

Given the analysis in previous sections and data from the sister report “Understanding the quantum threat for energy systems”, it is possible to build a hypothetical timeline that brings together threat actor characteristics, and quantum technical capability. The following sections are speculative, and as they reach further into the future, their accuracy is likely to dwindle.



Figure 7 – A summary of key quantum threat events from 2025 to 2045 and beyond

## 2.6 Conclusions

This section investigated the following questions, based on our analysis of the cybersecurity landscape, the quantum computing landscape and identifying the practical implications of quantum-enabled attacks:

- :
1. Will quantum computers ever represent a realistic cyber threat to the energy sector?
    - Quantum computers are likely to represent a realistic threat to the energy sector and could do so as early as 2035.
  2. What are quantum-enabled attacks and are they likely to be practical?
    - Quantum-enabled attacks are likely to compromise the integrity and confidentiality of data through the ability to derive private shared secrets and keys via publicly shared data during key exchanges and certification publications. These shared secrets will allow attackers to eavesdrop on encrypted communications, insert new commands into secure command and control lines and fake the signatures of legitimate software publishers. The time required to execute these attacks is likely to be an important factor in their practicality for many applications. However, the advent of store-now, decrypt-later attacks demonstrates that this is not always the case.
  3. Who are the most likely threat actors?

- The most likely threat actors are nation states due to the high costs associated with creating and maintaining a quantum computer, and the skills required to meaningfully operate them. Initially these are likely to be Russia and China, but others will follow as the technology becomes more established.

Another important finding of this discussion is that there is a significant challenge associated with identifying where public-key cryptography is being utilised within an organisation. This challenge is made harder by the complex relationship between cryptographic algorithms and the software libraries and frameworks that implement them. Uses of public-key cryptography within the energy sector include VPN technologies, physical access control systems, wireless communications for distributed systems and the establishment of MFA authenticators. Future work should include an investigation to identify where the security of systems is predicated on the use of public-key cryptography.

## 3 Methodology for performing quantum-aware risk management

### 3.1 Section summary

This section of the report will:

- identify a clear process for identifying and characterising the risks associated with quantum computers for a given system of interest
- outline how to match those risks to practical mitigations that can control the risks, without jeopardising the operations of a critical system.

In Section 3.2 we examine existing techniques for assessing the risk posed by quantum computers to traditional systems, leaning heavily on analysis already conducted in the sister report “Understanding the quantum threat for energy systems”. The analysis concludes that there are still open issues that prevent the techniques being applied to real-world systems, especially the energy sector.

In Section 3.3 we present an asset model for characterising systems that are vulnerable to quantum computing technology. The model stores information that is required about a system in order to assess its level of risk to quantum-enabled attacks.

In Section 3.4 we discuss different approaches to mitigating the risks posed by quantum computers, resulting in a taxonomy of mitigations that can be selected from. We also draw conclusions about the types of system that will be trivially upgraded by third parties (typically web services and cloud technologies) and the type of system that will need special consideration (services with significant latency constraints and processing power limitations).

In Section 3.5 the analysis from the previous sections is brought together to derive a process for systematically identifying systems that are vulnerable to quantum-enabled attacks and characterising their risk. This section is largely informational and simply justifies the design decisions made to produce the process.

In Section 3.6 the resulting process is summarised. It is applied to an energy sector example in Appendix 1.

### 3.2 Quantum risk estimation in the literature

In the sister report “Understanding the quantum threat for energy systems” there is a detailed discussion of several critical tools for and approaches to evaluating quantum risk, including Mosca’s inequality [26], the extended framework based on Mosca’s inequality [27] and CARAF (the Crypto Agility Risk Assessment Framework) [28]. CARAF is not a quantum-specific technique, but a general crypto-agility framework that can be applied to post-quantum cryptographic methods. In [29] Mosca’s methodology, CARAF and a number of well-established risk management frameworks are compared. In addition, [30] applies the general threat modelling methodology PASTA (Process for Attack Simulation and Threat Analysis) to understanding the quantum-enabled threats to a cyber physical system.

While these tools and approaches are valuable, there are four common problems with existing quantum risk assessment methodologies, that need to be considered in the context of the current research:

1. Because they model systems asset-by-asset, the methodologies do not scale well for large organisations like the National Grid.
2. The primary focus is on the length of time it takes for a cryptographically relevant quantum computer to be developed; current approaches generally ignore the computational time for launching the attacks once such devices become available.
3. Standard risk assessment methodologies do not typically handle temporal properties (such as data lifetime) well and tend to assume confidentiality is a permanent property of data once required.
4. Post-quantum cryptography (PQC) and hybrid techniques involving PQC are typically the only mitigations considered for the risks.
5. There is a lot of uncertainty surrounding the nature of the quantum threat, in terms of when a cryptographically-relevant quantum computer will emerge, how it will impact specific systems, and at a



fundamental level, what systems will actually be vulnerable. Making good decisions in the presence of these sources of uncertainty is extremely challenging.

This work aims to address those problems in the following ways:

1. Problem 1 is addressed by developing an asset model that will capture the least amount of data required to make an informed assessment of the quantum threat, and that is rooted in functional groupings rather than individual assets.
2. Problem 2 is addressed by developing a threat assessment tool that is cognisant of the practical constraints around launching a quantum-enabled attack.
3. Problem 3 is addressed by ensuring that the amount of time that a data asset needs to remain confidential is factored into the threat assessment.
4. Problem 4 is addressed by developing a mitigation taxonomy that includes alternative techniques for addressing the quantum threat, including PQC.
5. Problem 5 is only partially addressed by work in this report and the sister report “Understanding the quantum threat for energy systems”. The uncertainty around the date of a cryptographically-relevant quantum computer emerging is managed, in part, by analysis performed in the sister report, which aims to identify the window in which the threat will manifest. The broader issue of identifying what systems are vulnerable is partially addressed in Section 2.3.1 through the linking of vulnerable cryptographic algorithms to higher level software libraries and frameworks. However, more work is required to systematically identify vulnerable systems within the energy sector and to address the wider issue of making sensible decisions in the presence of uncertainty that cannot be trivially resolved.

### **3.3 Asset model**

Performing a detailed risk assessment on every asset within the energy grid would be technically infeasible and resource intensive. By identifying the key properties required to make an informed, risk-based decision about the suitability of a given mitigation, it is possible to construct a minimum asset model that can be filled in to characterise a given system.

The asset model is outlined in subsequent sections, and a worked example can be found in Appendix 1.

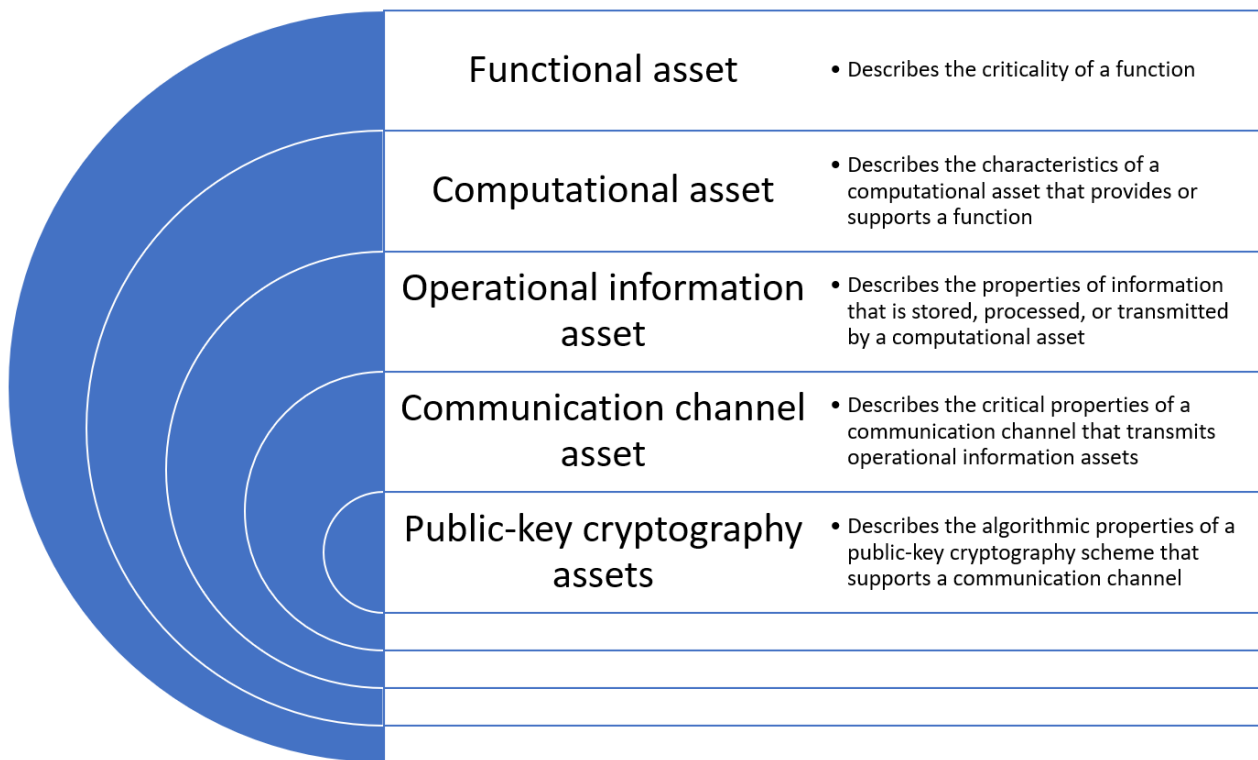


Figure 8 – Graphical representation of the asset model. Note that at each tier there could be a many-to-many relationship between the asset types e.g. a functional asset may be supported by multiple computational assets, each of which may support other functional assets.

### 3.3.1 Functional assets

The functional assets of a system are the functions that the system needs to perform. Each functional asset is assigned a criticality to inform prioritisation of action.

A system can perform many functions, and so can have multiple functional assets.

The criticality scale can be determined by the implementing organisation. For CNI systems, the Cabinet Office has a five-step process [31] for calculating the criticality of a system. However, the criticality levels and definitions are not publicly available. For the purposes of this report the criticality of a system shall be selected from the set {High, Medium, Low}, where “High” means that the functionality has a direct impact on the energy sector’s ability to supply energy to the country, “Medium” means that failing to provide the functionality carries financial penalties or produces inefficiencies that will cost the energy sector significant time or money, and “Low” means that losing the functionality is an inconvenience to energy sector participants.

This provides the following syntax for a functional asset:

- **Functional asset name (criticality: {High, Medium, Low})**

For example, “Generate Power(criticality: High)”, is a key functional asset of the national grid.

### 3.3.2 Computational assets

Computational assets are the computational elements that deliver the functions defined by functional assets.

Their primary uses in the context of this assessment are related to the performing of cryptographic functions and the execution of application software to deliver the functions defined by the functional assets.

A single functional asset may require multiple computational assets and a computational asset may support multiple functional assets simultaneously.

A computational asset has two properties of interest: its processing power and its memory capacity. Both properties will control the ability of the computational asset to perform cryptographic functions.

As the asset model evolves, and the properties of PQC are better characterised, it may be necessary to capture additional information to support decision-making about managing quantum threats.

The lack of characterisation for PQC mitigations in terms of their computational complexity and memory consumption makes creating a definitive scale for these properties difficult. Work has been done to benchmark the speed of some PQC algorithms in [32] via the use of reference implementations on known processors. In addition, the literature does include explorations of PQC complexity for specific scenarios, such as TLS [33], [34], [35]. However, to get a sound understanding of what these statistics mean for the practical deployment of PQC on traditional systems will require more analysis.

For the purposes of this report they will both be measured using the three-point profile {High, Medium, Low}.

This provides the following syntax for a computational asset:

- **Computational asset name(processing power: {High, Medium, Low}, memory capacity: {High, Medium, Low})**

For example, “Load Balancing Server(processing power: High, memory capacity: High)” and “Control System(processing power: Low, memory capacity: Low)” are energy sector-relevant computational assets.

### 3.3.3 Operational information assets

Operational information assets are collections of data that are used to inform decisions that drive the delivery of functional assets.

The term “operational” is used to distinguish between those information assets that deliver functions and “cryptographic” information assets, such as keys.

For each operational information asset, there are three properties of interest:

- Confidentiality impact: the impact of losing confidentiality for the operational information asset. Measured using a three-point {High, Medium, Low} scale.
- Confidentiality lifetime: the amount of time the information asset requires confidentiality. Measured in time.
- Integrity impact: the impact of losing integrity of the operational information asset. Measured using a three-point {High, Medium, Low} scale.

This provides the following syntax for an operational information asset:

- **Operational information asset name(confidentiality impact: {High, Medium, Low}, confidentiality lifetime: {time with units}, integrity impact: {High, Medium, Low})**

For example, if operational metering data is only used to make market decisions for a single iteration of the balancing market, it may only need to be kept secret for the duration of that decision-making process. However, the impact of losing confidentiality within that time frame may be significant if it allows a malicious user to undermine the independence of the market. Thus, “Operational Metering Data(confidentiality impact: High, confidentiality lifetime: 30 mins, integrity impact: High)” is a potential operational information asset for the energy sector.

### 3.3.4 Communication channel assets

Communication channel assets are used to transmit operational information assets from one computational asset to another, in order to achieve a function.

For this assessment, there are only two properties of interest for a communication channel:

- Latency demand: what is the maximum allowable latency for this communication channel to maintain the function it supports. Measured in time.
- Bandwidth demand: How much of the available bandwidth is currently used to achieve functions. A low value indicates that there is a large amount of overhead to accommodate additional information being transferred. For the purposes of this assessment a three-point {High, Medium, Low} scale is used.

This provides the following syntax for a communications channel asset:

- **Communication channel name(latency demand: {time in units}, bandwidth demand: {High, Medium, Low})**

For example, “Power Plant to Balancing System Comms(latency demand: 1 second, bandwidth demand: Low)” is a possible communication channel asset for the energy sector.

### 3.3.5 Public-key cryptography assets

Public key cryptography assets are the techniques used to protect the confidentiality and integrity of operational information assets.

For this assessment there are only two properties that are of interest:

- The key rotation period i.e. how often is the shared secret re-established between the communicating parties. This is measured in time.
- Underlying algorithm: a description of the underlying algorithm used, from the set listed in Section 2.3.1. This provides the following syntax for a public-key cryptographic asset:
- **Public-key cryptographic asset name(key rotation period: {time in units}, underlying algorithm: {algorithm name})**

For example “TLS 1.3 operating on power plant to balancing system comms(key rotation period: 30 mins, underlying algorithm: Diffie-Hellman)” is a public-key cryptography asset for the energy sector.

## 3.4 Mitigation taxonomy

The final analysis required before specifying a quantum-enabled attack risk assessment methodology is to understand what mitigations are available to compensate for quantum-enabled threats.

In Table 4 the mitigations are presented along with a commentary about their applicability. Note that the applicability discussion is a purely technical one. Other parameters, such as human factors arising from complexity or system performance, should also be taken into account when introducing new controls.

Mitigation Type	Description	Applicability
<b>Post Quantum Cryptography (PQC)</b>	Replace broken cryptography with an algorithm specifically designed to be resistant to quantum computers	<ul style="list-style-type: none"> <li>• Systems where software update can be performed with low cost/effort.</li> <li>• Systems that match the computational requirements of PQC</li> </ul>
<b>Hybrid approaches</b>	Replace broken cryptography with a hybrid of a standard cryptographic approach and a PQC approach	<ul style="list-style-type: none"> <li>• As PQC.</li> <li>• Key advantage of this approach is that it mitigates uncertainty about PQC algorithm security.</li> <li>• Key disadvantage is that it requires even more computational complexity and bandwidth. However, this may be an acceptable overhead as it only applies during key exchange and signature checking.</li> </ul>
<b>Key lengthening</b>	Increase the key length for a standard cryptographic approach	<ul style="list-style-type: none"> <li>• Situations where either the confidentiality of the data is time-limited,</li> </ul>

Mitigation Type	Description	Applicability
		<ul style="list-style-type: none"> <li>• or the window of opportunity for the attacker is heavily influenced by the computational time required to launch the attack (see Table 2 for timing benefits).</li> </ul>
<b>Increase key exchange frequency</b>	Rotate private session keys more often to limit the useful lifetime of quantum-calculated credentials (K3) or update the private keys used for signing software more frequently (K4).	<ul style="list-style-type: none"> <li>• Appropriate for K3 when preventing an attacker from inserting malicious commands over an encrypted channel, as it reduces the window of opportunity for the attacker to calculate and use the private key for the session.</li> <li>• Also applicable when considering digital signatures in situations where it is trivial to access the most up-to-date public key of the signatory. However, this is likely to be extremely difficult in practice, as it involves reissuing signatures on a large scale, and having a mechanism to revoke signatures on devices with limited external communications.</li> </ul>
<b>Architectural changes</b>	Restructure the system in a way that limits the man-in-the-middle opportunities for the attacker	<ul style="list-style-type: none"> <li>• Applicable in situations where the communications channel can be physically secured to prevent eavesdropping on the key exchange or transmission of confidential data.</li> </ul>
<b>Alternative key exchange mechanics</b>	Continue to use symmetric cryptography, but find alternative channels to establish the shared secret	<ul style="list-style-type: none"> <li>• Applicable in situations where an alternative communications channel security mitigates man-in-the-middle. For example, manual transfer of keys via physical media.</li> <li>• It is of note that the characteristics of the alternative medium properties will have an impact on the frequency of key updates, and introduce new risks based on interception of that alternative communications channel.</li> </ul>
<b>Phase out asset</b>	Accelerate the removal of the asset with an intent to either a) discontinue the service being supported by the asset function, or b) replace the	<ul style="list-style-type: none"> <li>• Applicable when the service being supported or the asset itself is reaching the end of its life.</li> </ul>

Mitigation Type	Description	Applicability
	asset with an asset that can support one of the above mitigations	

Table 4 – Mitigations for controlling quantum-enabled risks

Note that there may be situations where the risk does not require mitigation and can simply be accepted. For example, there may be scenarios where the impact of losing confidentiality of an information asset is very low, and the costs associated with protecting that asset are significant.

An important trend in quantum-enabled attack mitigation is the application of hybrid and PQC cryptography to cloud computing services. Google, Amazon, and Microsoft are researching PQC and contributing to open—source software libraries that will make the transition to PQC significantly easier for the average consumer. In fact, for many consumers and businesses, the shift from traditional encryption to PQC will happen largely “under the hood”, as many the services they use today are cloud-based and will seamlessly transition to more secure algorithms.

However, for the energy sector this is unlikely to be the case. Within energy networks, legacy systems, systems with low computational power, or systems with tight memory requirements at the edge will struggle to adopt PQC approaches without incurring significant costs to upgrade their systems. For this reason, alternative approaches should be explored that can manage the risk in the period between the emergence of the quantum threat and the widespread adoption of PQC in low-power systems.

Early adopters of PQC, both in the energy sector and beyond, should ensure that they prioritise approaches that can be cryptographically agile, i.e. systems where the underlying cryptographic algorithms are easily changeable. This is because PQC algorithms are relatively unproven in practice compared with traditional algorithms, and may yet still be vulnerable to new attacks (which they then need to employ new computational approaches to counter), quantum or otherwise.

### 3.4.1 Post-quantum cryptographic algorithm selection

A number of post-quantum cryptographic algorithms have been developed. However, all such algorithms, despite the rigour with which they have been theoretically tested, have had limited hours of operation in the field.

The most prominent assessment of such algorithms has been performed by NIST (National Institute of Standards and Technology – US). The NIST algorithm selection process is currently in its fourth round and has selected four PQC algorithms for standardisation.

PQC Algorithm Name	Algorithm Type
<b>CRYSTALS-Kyber</b>	ML-KEM (Module-Lattice-based key encapsulation mechanism) used primarily for key exchange.
<b>CRYSTALS-Dilithium</b>	Digital signature
<b>Falcon</b>	Digital signature
<b>SPHINCS+</b>	Digital signature

Table 5 – NIST selected algorithms [36]

Whilst the NIST down-selection process has yielded a best practice list of algorithms, there are two challenges associated with the selection presented.

Firstly, there is only one key encapsulation algorithm. When large numbers of organisations rely heavily on a single implementation of a single algorithm, vulnerabilities in that algorithm can have far-reaching consequences. For example, the Heartbleed vulnerability discovered in 2014, in the OpenSSL implementation of transport layer security, was estimated to make 66% of the world’s internet servers vulnerable to attack

[37]. There are a number of ways a cryptographic system can become vulnerable. A shortlist can be found in [38] and is presented in Table 6 alongside a discussion about how that weakness translates to PQC.

<b>CWE Category</b>	<b>CWE ID</b>	<b>Description</b>	<b>Applicability to PQC</b>
<b>Weak encoding for password</b>	261	Failing to encrypt a password or storing it in plaintext.	Not relevant to this discussion.
<b>Use of a key past its expiration date</b>	324	Using a key beyond its intended usage period.	This lengthens the window of opportunity for a quantum-enabled cryptographic attack.
<b>Missing cryptographic step</b>	325	Implementation-specific vulnerability arising from a poor design decision to omit a seemingly unimportant aspect of the algorithm.	Specific implementations of PQC could introduce this error.
<b>Use of weak hash</b>	328	Employing a hashing algorithm that is not adequately secure.	There are currently no identified quantum-enabled attacks against hashing algorithms.
<b>Insufficient entropy</b>	331	The 'randomness' of the critical random steps, such as key generation, is inadequate and can be predicted or otherwise exploited by an attacker.	Regardless of the strength of the algorithm, if the attacker can predict the keys being generated, there is no real security benefit to applying the algorithm. This could be introduced by poor deployment of a PQC.
<b>Small space of random values</b>	334	The range of random numbers generated by a random number generator is too small, allowing brute force attacks.	If a key generation algorithm uses a small space of random values, then the attacker can trivially use brute force to recover the plaintext. This could be introduced by poor deployment of a PQC.
<b>Incorrect usage of seeds in pseudo-random number generator</b>	335	Failure to adequately initialise a pseudo-random number generator, produces a predictable sequence of numbers.	Similar to CWE-331's impact on PQC. Poor deployment could introduce this weakness.
<b>Use of cryptographically weak pseudo-random number generator</b>	338	A pseudo-random number generator that has not been designed with cryptographic applications in mind, may produce predictable outputs.	Similar to CWE-331's impact on PQC. Poor deployment could introduce this weakness.
<b>Improper verification of cryptographic signature</b>	347	The management process for handling cryptographic signatures fails to detect mismatches between the expect value and the actual value, or simply doesn't check at all.	Any new implementation of a digital signature checking service could introduce this error if quality is not managed.



CWE Category	CWE ID	Description	Applicability to PQC
<b>Use of password hash with insufficient computational effort</b>	916	Failure to use an adequate cryptographic hash to store passwords.	Similar to CWE-261 and CWE-328. Not relevant to this discussion.
<b>Generation of weak initialisation vector</b>	1204	Some cryptographic algorithms require an initial value to ensure that the initial state of the encryption process is not the same between operations. Failure to do this adequately can result in patterns within the plaintext becoming apparent in the ciphertext.	Where initialisation vectors are used in PQC, poor quality deployment could introduce this error.
<b>Use of a cryptographic primitive with a risky implementation</b>	1240	A specific implementation of a cryptographic function can introduce errors that make attacking them trivial.	As multiple implementations of the PQC algorithms are likely to be produced to meet specific needs (lower latency etc.) implementation errors are inevitably going to be introduced into some versions.

Table 6 – A taxonomy of cryptographic issues, defined by MITRE (taken from [38]). Descriptions are added for clarity

Secondly, while the selection process does consider computational complexity and memory requirements through the use of benchmarking, some of the selected algorithms do pose challenges for implementation on older infrastructure. This is particularly noticeable for the digital signature algorithms where traditional algorithms, such as the TLS handshake for https, use around 1248 bytes of signatures, vs PQC algorithms, such as CRYSTALS-Dilithium use around 14,724 bytes [39]. A nearly twelve times increase in the data required to transmit a digital signature may reduce the areas of applicability for such algorithms.

Other PQC algorithms, not currently part of NIST's selected algorithms (though many are under consideration) exist and have been implemented in the PQC branch of OpenSSL. These include:

- BIKE (Public key cryptography / key distribution)
- FrodoKEM (Public key cryptography / key distribution)
- HQC (Public key cryptography / key distribution)

This greater diversity of algorithms mitigates the risk that a flaw in a single algorithm results in widespread loss of security. However, they lack the scrutiny and cryptanalysis that has been applied to CRYSTALS-Kyber and, as a result, carry more risk.

In order to select the correct algorithm for a specific situation, more work is required to characterise the computational complexity, increased communication overhead, and memory requirements of the PQC algorithms. This not only applies at the computational level, but also the protocol level, as many networking middleware appliances and security devices (including firewalls) are not programmed to manage the increased handshake size associated with PQC-enabled TLS handshakes [40]. For the energy sector, where there are a large number of distributed devices at the edge, these constraints may make the adoption of PQC extremely challenging.

The risks associated with PQC have resulted in many early adopters choosing to use hybrid approaches (combining traditional encryption with new algorithms) to mitigate the risk that vulnerabilities are found in PQC algorithms[.

## 3.5 Process Derivation

This section outlines the way in which a methodology was derived to identify the risks associated with quantum-enabled attacks. Readers who are only interested in the methodology itself can jump to Section 3.6.

For simplicity, the NIST risk management framework (RMF) was selected as the template for moving from risk identification to the identification of controls [41]. In the NIST RMF the following steps are applied to an organisation's risk:

1. **Prepare:** Essential activities to prepare the organisation to manage security and privacy risks
2. **Categorise:** Categorize the system and information processed, stored, and transmitted based on an impact analysis
3. **Select:** Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
4. **Implement:** Implement the controls and document how controls are deployed
5. **Assess:** Assess to determine if the controls are in place, operating as intended, and producing the desired results
6. **Authorize:** Senior official makes a risk-based decision to authorize the system (to operate)
7. **Monitor:** Continuously monitor control implementation and risks to the system

For this activity we will focus on steps 1-3, as they should be applied to the UK energy sector and in the specific context of quantum-enabled attacks.

Thus, the process will be based on the steps: Prepare, Categorize, Select.

### 3.5.1 Prepare

The 'prepare' phase of the NIST RMF aims to achieve the following goals:

1. key risk management roles identified
2. organizational risk management strategy established, risk tolerance determined
3. organization-wide risk assessment
4. organization-wide strategy for continuous monitoring developed and implemented
5. common controls identified

Note that in step 1, the word "key" is used by NIST to refer to "pivotal" or "critical", not to be confused with the cryptographic sense of the word. In terms of goals that are impacted by the quantum computing context, the important activities are steps 3 and 5. Step 3, because the risk assessment in this case will focus on the risk posed by quantum-enabled attacks. Step 5, because the common set of controls to be considered by the assessment are specific to those controls that manage the quantum threat (see Section 3.4).

There are obviously a number of applicable cyber risk assessment standards. For this work, NIST SP 800-30 [42] was selected due to its large adoption rates and compatibility with NIST RMF.

The risk assessment steps are outlined below:

- a) Identify threat sources
- b) Identify potential threat events, relevance of the events, and the threat sources that could initiate the events
- c) Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts
- d) Determine the likelihood that threat events of concern result in adverse impacts, considering:
  - i. the characteristics of the threat sources that could initiate the events
  - ii. the vulnerabilities/predisposing conditions identified
  - iii. the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

- e) Determine the adverse impacts from threat events of concern considering:
  - i. the characteristics of the threat sources that could initiate the events
  - ii. the vulnerabilities/predisposing conditions identified
  - iii. the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.
- f) Determine the risk to the organization from threat events of concern considering:
  - i. the impact that would result from the events
  - ii. the likelihood of the events occurring

Applying these generic risk assessment steps to the quantum-enabled threat to the energy sector, provides the following:

- a) For threat sources in this context, see Section 2.4
- b) For threat events in this context, see Section 2.3.3. For the purposes of this report the application of a threat event to a specific system shall be referred to as an “attack scenario”
- c) For vulnerabilities, see Sections 2.3.1 and 2.3.3. Predisposing conditions have to be assessed on a case-by-case basis
- d) The likelihood of attack is based on the emergence of cryptographically relevant quantum computers (see the sister report “Understanding the quantum threat for energy systems”) and the quantum-enabled kill chain (see Section 2.3.3) applicability to a specific architecture
- e) The adverse impacts have to be assessed on a case-by-case basis
- f) The final risk score is a function of values to be calculated on a case-by-case basis

Step 5 of “Prepare” is to identify a common set of controls. This set is listed in Table 4.

### 3.5.2 Categorise

The categorize phase of the risk management framework aims to achieve the following goals:

1. system characteristics documented
2. security categorization of the system and information completed
3. categorization decision reviewed/approved by authorizing official

In terms of goals that are impacted by the specified context, the important activity is step 1. For information about classification of system characteristics see Section 3.3.

The categorize phase focusses on categorising assets within the system of interest and assigning them a level of criticality. However, as the prepare phase already mandates a risk assessment, there may be iteration between the two phases to gain a full understanding of the system and how the risks identified link to that system.

### 3.5.3 Select

The select phase of the risk management framework aims to achieve the following goals:

1. control baselines selected and tailored
2. controls designated as system-specific, hybrid, or common
3. controls allocated to specific system components
4. system-level continuous monitoring strategy developed security and privacy plans that reflect the control selection, designation, and allocation are reviewed and approved

In terms of goals that are impacted by the specified context, the important activity is step 1. In this step we assign a suitable mitigation to manage the risk posed by a quantum-enabled attack (see Section 3.4 for a taxonomy of mitigations).

## 3.6 Quantum Aware Risk Management Process Summary

The Quantum Aware Risk Management process is outlined below.

The process is divided into three phases: Prepare, Categorize, and Select.

### 3.6.1 Prepare

1. Identify the threat actors with the technical capability to launch quantum-enabled attacks and characterise their motivations (see Section 2.4 for a summary of threat actors based on current OSINT).
2. Identify the quantum-enabled attacks that could be launched by the threat actors (see Section 2.3.3 for a current list of quantum-enabled attacks).
3. Identify software components that are vulnerable to quantum-enabled attacks (see Section 2.3.1 for an incomplete list of software libraries that use cryptography that is vulnerable to quantum-enabled attacks). This step may be non-trivial. Cryptographic discovery is a known hard problem in cybersecurity. Best practice suggests taking multiple angles: What software/firmware is running where? What cryptography can be observed in network traffic? What services are exposed and what protocols are they operating? Each aspect might reveal another cryptographic component somewhere in a system. The discovery exercise is a key part of preparing, it can take significant effort and require specialist tools. During this step the sections of the information model in Section 3.3, that apply to public-key cryptography assets should be used to record the findings of the discovery process.
4. Evaluate the risk posed by these vulnerabilities
  - a. Identify attack scenarios based on steps 1-3 and the system architecture of interest
  - b. Evaluate the likelihood of attack scenarios
  - c. Evaluate the impact of attack scenarios
  - d. Evaluate the risk posed by attack scenarios
5. Identify a set of mitigations that can be applied to quantum-enabled attacks (see Section 3.4 for a preliminary list).

### 3.6.2 Categorise

Ensure that the asset model outlined in Section 3.3 is complete. As your understanding of the system grows, you may need to revisit the risk assessment from the prepare phase to update the impact of specific risks.

### 3.6.3 Select

Assign the controls identified in the Prepare phase to assets identified in the Categorize phase, assessing the impact on risk and complexity of implementing the mitigation for that system context.

### 3.6.4 Applying the process to an indicative energy system

A worked example of the process is presented in Appendix 1.

For the simple system in Appendix 1, a significant amount of analysis was required to generate the most impactful and least disruptive controls. More work is required to streamline and optimise this process.

## 4 Conclusions

This report has demonstrated that the emergence of quantum computers poses a cybersecurity threat to the energy sector.

Through evidence-based research, it has been possible to cut through the hype and focus on identifying and characterising practical attacks and mitigations against those attacks.

The report highlights the importance of monitoring quantum computing technologies and ensuring that the energy sector is ready when cryptographically relevant quantum computers emerge. It also lays out an initial Quantum Aware Risk Management process which has been notionally applied to a fictional test case for energy sector security (See Appendix 1).

### 4.1 Key outputs from this work

Key tools and analyses developed in this work, which can form the initial basis for developing a framework and set of processes for security stakeholders (**Quantum Aware Risk Management** process), include the following (mapped to the key tasks of *Identifying vulnerabilities, Understanding the risk, Measuring the risk, and Identifying mitigations*):

- **Identifying vulnerabilities:** A mapping from theoretical algorithmic attacks to vulnerable software libraries to aid understanding of the scale of the challenge (Section 2.3.1)
- **Understanding the risk:** A well-defined set of kill chains that explain how threat actors can launch attacks using quantum computers and an assessment of their practicality (Section 2.3.3)
- **Understanding the risk:** An evidence-based threat model of likely quantum-enabled threat-actors produced from knowledge about quantum investment and the capability of nation states and historical and emerging attack trends (Section 2.4).
- **Measuring the risk:** A minimal asset model for characterising systems so their risk from quantum computers can be evaluated (Section 3.3)
- **Identifying mitigations:** A taxonomy of mitigations that be used to manage the threat posed by those kill chains (Section 3.4)
- **Identifying mitigations:** A process for performing that risk assessment task (Section 3.6)
- A worked example, applying the **Quantum Aware Risk Management** process to a realistic energy sector system (Appendix 1)

However, in developing the above analyses, we have identified a number of outstanding challenges in progressing these to a more usable tool or framework for the industry. We would propose to address these in future work, as discussed below.

### 4.2 Future work

There are a number of open challenges that need to be addressed in order to enable creation of an effective and usable Quantum-Aware Risk Management process and roadmap for the energy industry. Below, we summarise these and suggest future work to address them.

- **Embed quantum timelines into risk management approach:** Existing techniques for estimating the risk posed by quantum computers do not provide a full picture, because they focus on the timeline till the emergence of cryptographically relevant quantum computers, and not on the properties of subsequent quantum-enabled attacks. But the full picture needs to combine the two, to build a strategic roadmap that will allow organisations within the energy sector to identify what systems need attention and what to do about them.
  - The proposed Quantum-Aware Risk Management process in this report attempts to resolve this by focussing on practical quantum-enabled attacks, but lacks the higher-level view of comparing the lifetime of systems against the probable date for the emergence of a cryptographically relevant quantum computer.

- Work needs to be done to merge the two approaches so that an energy organisation can develop a clear understanding of which systems require attention, and which systems are either low risk or will be managed by third-parties.
- The resulting process needs to be streamlined and optimised to handle a large number of complex systems, and needs to be designed to be usable by engineers without the need for significant training in quantum computing technology.
- By explicitly adjusting the likelihood analysis to take into account a specific window of time (i.e. the likelihood of an attack within the next 10, 15, 20 years) it is likely to directly affect risk levels using MOSCA's inequality.
- **Improve scalability and usability of approach:** When exploring an entire sector of technologies, scalability of the approach will be key. In other words, the approach must be simple or scalable enough to enable organisations such as NG ESO to set up best practices for managing the quantum threat, that ensure common principles are applied throughout the organisation.
  - To identify all potentially vulnerable systems, a systematic discovery of systems that are reliant on public-key cryptography is required. This may require the employment of third-party crypto-finding tools and interrogation of the SBOMS of critical systems.
  - For the simple energy system worked example in Appendix 1, a significant amount of analysis was required to generate the most impactful and least disruptive controls.
  - The proposed asset model captures very little data about a system, but is still difficult to complete. Even in the simple problem in Appendix 1, there were unknowns and dependencies that could not be resolved without further research.
  - In order to make this more usable from a practical point of view, work is required to streamline and optimise the proposed Quantum-Aware Risk Management process – for both the asset model and the resulting analysis.
- **Develop a better heuristic to determine which mitigation to apply where:** In order to understand exactly which mitigations are feasible in different scenarios, more work needs to be done on characterising and specifying a number of key areas and their implications.
  - One of the largest unknowns identified was the lack of specification for what sort of system/device/communication channel can handle PQC. It will be important to characterise the practical implications of implementing PQC on embedded systems and how the protocols will be handled by networking middleware and security devices. This depends on a number of factors, including the technical specification of the device and the ease with which new cryptographic algorithms can be introduced into the system. More analysis is required to determine which factors limit the deployment of PQC.
  - In addition, where key rotation frequency needs to be increased, there will be a commensurate increase in bandwidth consumption and latency, which must be characterised
  - More work is required to systematically identify vulnerable systems within the energy sector and to address the wider issue of making sensible decisions in the presence of uncertainty that cannot be trivially resolved.

The ultimate goal of this work, which subsequent phases would take forward to the next stage of development, would be to develop a clear, usable roadmap for upgrading energy system assets that are most vulnerable to the quantum threat, building on the initial Quantum Aware Risk Management Process that we present here. To design this will involve consultation and collaboration with energy security professionals (in the first instance, NG ESO), on priorities, costs and timelines; user interfaces, and the best way to ensure outputs are compatible with practical operational and IT processes.

## 5 References

- [1] "X-Force Threat Intelligence Index 2024," 2024. Accessed: Apr. 27, 2024. [Online]. Available: <https://www.ibm.com/reports/threat-intelligence>
- [2] "National Risk Register 2023 edition," Aug. 2023. Accessed: Apr. 25, 2024. [Online]. Available: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1175834/2023\\_NATIONAL\\_RISK\\_REGISTER\\_NRR.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1175834/2023_NATIONAL_RISK_REGISTER_NRR.pdf)
- [3] J. Easterly, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years," Cybersecurity and Infrastructure Security Agency. Accessed: Apr. 23, 2024. [Online]. Available: <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>
- [4] "Cyber-Attack Against Ukrainian Critical Infrastructure," Cybersecurity and Infrastructure Security Agency. Accessed: Apr. 26, 2024. [Online]. Available: <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>
- [5] "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," Microsoft. Accessed: May 08, 2024. [Online]. Available: <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/>
- [6] "Future energy," NGESO. Accessed: Apr. 27, 2024. [Online]. Available: <https://www.nationalgrideso.com/future-energy>
- [7] J. Chen, H. Du, J. Yan, R. Zgheib, and M. Debabbi, "A Data Integrity Attack Targeting VSC-HVDC-Connected Offshore Wind Farms," in *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2023 - Proceedings, 2023*. doi: 10.1109/SmartGridComm57358.2023.10333872.
- [8] "Applications and protocols," Open Quantum Safe. Accessed: Apr. 23, 2024. [Online]. Available: <https://openquantumsafe.org/applications/>
- [9] "51% Attacks," MIT Digital Currency Initiative. Accessed: Apr. 25, 2024. [Online]. Available: <https://dci.mit.edu/51-attacks>
- [10] "ICS Focused Malware," CISA. Accessed: Apr. 23, 2024. [Online]. Available: <https://www.cisa.gov/news-events/ics-advisories/icsa-14-178-01>
- [11] "Steady progress in approaching the quantum advantage ," Apr. 2024. Accessed: Apr. 26, 2024. [Online]. Available: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage#/>
- [12] "NCSC Annual Review 2023," Nov. 2023. Accessed: Apr. 26, 2024. [Online]. Available: <https://www.ncsc.gov.uk/collection/annual-review-2023>
- [13] "Microsoft shifts to a new threat actor naming taxonomy," Microsoft. Accessed: Apr. 26, 2024. [Online]. Available: <https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/>
- [14] T. Alsop, "Quantum Technology Historic Public Funding as of 2022, by country ," 2023.
- [15] M. Swayne, "Russian scientists expect a 50-qubit quantum computer by end of 2024," *The Quantum Insider*. Feb. 24, 2024. Accessed: Apr. 24, 2024. [Online]. Available: <https://thequantuminsider.com/2024/02/24/russian-scientists-expect-a-50-qubit-quantum-computer-by-end-of-2024/>
- [16] UK Gov, "UK exposes attempted Russian cyber interference in politics and democratic processes ," Dec. 2023.
- [17] M. Gault, "Iran Unveils 'Quantum' Device That Anyone Can Buy for \$589 on Amazon," *Vice*. Accessed: Apr. 27, 2024. [Online]. Available: <https://www.vice.com/en/article/7kxx4g/iran-unveils-quantum-device-that-anyone-can-buy-for-dollar589-on-amazon>

- [18] M. Hamilton, "India: A Growing Cybersecurity Threat," Dark Reading. Accessed: Apr. 27, 2024. [Online]. Available: <https://www.darkreading.com/threat-intelligence/india-a-growing-cybersecurity-threat>
- [19] J. Potter, "4 Countries That Began Funding Quantum Initiatives In 2022," The Quantum Insider. Accessed: Apr. 27, 2024. [Online]. Available: <https://thequantuminsider.com/2023/05/16/4-countries-that-began-funding-quantum-initiatives-in-2022/>
- [20] R. Lakshmanan, "Alert: Brazilian Hackers Targeting Users of Over 30 Portuguese Banks," The Hacker News. Accessed: Apr. 27, 2024. [Online]. Available: <https://thehackernews.com/2023/05/alert-brazilian-hackers-targeting-users.html>
- [21] S. Singh, "APT-36 Uses New TTPs and New Tools to Target Indian Governmental Organizations," ZScaler Blog. Accessed: Apr. 27, 2024. [Online]. Available: <https://www.zscaler.com/blogs/security-research/apt-36-uses-new-ttps-and-new-tools-target-indian-governmental-organizations>
- [22] "Pakistan launches nanotechnology and quantum computing centers to drive innovation." Accessed: Apr. 27, 2024. [Online]. Available: <https://www.islamabadsce.com/pakistan-launches-nanotechnology-and-quantum-computing-centers-to-drive-innovation/>
- [23] Agencies, "Pakistan must collaborate with China on AI, quantum computing," The Nation. Accessed: Apr. 24, 2024. [Online]. Available: <https://www.nation.com.pk/03-Feb-2023/pakistan-must-collaborate-with-china-on-ai-quantum-computing>
- [24] J. Sullivan, "Russian cyber operations: state-led organised crime," Nov. 2018. Accessed: Apr. 24, 2024. [Online]. Available: <https://www.rusi.org/explore-our-research/publications/commentary/russian-cyber-operations-state-led-organised-crime>
- [25] "Cybercrime in Russia and the CIS. Trends, Analytics, Forecasts 2023–2024." Accessed: Apr. 27, 2024. [Online]. Available: <https://www.facct.ru/resources/research-hub/cybercrime-trends-annual-report-2023-2024/>
- [26] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Secur Priv*, vol. 16, no. 5, 2018, doi: 10.1109/MSP.2018.3761723.
- [27] M. Mosca and J. Mulholland, "A Methodology for Quantum Risk Assessment," Jan. 2017.
- [28] C. Ma, L. Colon, J. Dera, B. Rashidi, and V. Garg, "CARAF: Crypto Agility Risk Assessment Framework," *J Cybersecur*, vol. 7, no. 1, 2021, doi: 10.1093/cybsec/tyab013.
- [29] "Guidelines for Quantum Risk Management for Telco," Sep. 2023. Accessed: Apr. 25, 2024. [Online]. Available: <https://www.gsma.com/get-involved/working-groups/wp-content/uploads/2023/09/Guidelines-for-Quantum-Risk-Management-for-Telco-v1.0.pdf>
- [30] C. C. Lee, T. G. Tan, V. Sharma, and J. Zhou, "Quantum Computing Threat Modelling on a Generic CPS Setup," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2021. doi: 10.1007/978-3-030-81645-2\_11.
- [31] "Improving our understanding of Critical National Infrastructure," Apr. 2023. Accessed: Apr. 25, 2024. [Online]. Available: <https://www.npsa.gov.uk/resources/cni-criticalities-kb-flyer>
- [32] M. Kannwischer, "Speed Evaluation," Github. Accessed: Apr. 27, 2024. [Online]. Available: <https://github.com/mupq/pqm4/blob/master/benchmarks.md>
- [33] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH," in *CoNEXT 2020 - Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies*, 2020. doi: 10.1145/3386367.3431305.
- [34] P. Kampanakis and D. Sikeridis, "Two Post-Quantum Signature Use-cases: Non-issues, Challenges and Potential Solutions," in *7th ETSI/IQC Quantum Safe Cryptography Workshop*, Seattle, 2019.
- [35] I. Tzinis, K. Limniotis, and N. Kolokotronis, "Evaluating the performance of post-quantum secure algorithms in the TLS protocol," *Journal of Surveillance, Security and Safety*, vol. 3, no. 3, 2022, doi: 10.20517/jsss.2022.15.



- [36] "Post-Quantum Cryptography - Selected algorithms 2022." Accessed: Apr. 25, 2024. [Online]. Available: <https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>
- [37] "The Heartbleed Bug." Accessed: Apr. 25, 2024. [Online]. Available: <https://heartbleed.com/>
- [38] "CWE Category: Cryptographic Issues." Accessed: Apr. 25, 2024. [Online]. Available: <https://cwe.mitre.org/data/definitions/310.html>
- [39] D. Adrian, "Post-quantum cryptography is too damn big." Accessed: Apr. 25, 2024. [Online]. Available: <https://dadrian.io/blog/posts/pqc-signatures-2024/>
- [40] Sergiu Gatlan, "Google Chrome's new post-quantum cryptography may break TLS connections," Bleeping Computer. Accessed: May 08, 2024. [Online]. Available: <https://www.bleepingcomputer.com/news/security/google-chromes-new-post-quantum-cryptography-may-break-tls-connections/>
- [41] "NIST Risk Management Framework." Accessed: Apr. 25, 2024. [Online]. Available: <https://csrc.nist.gov/Projects/risk-management/about-rmf>
- [42] "Guide for conducting risk assessments," Sep. 2012. Accessed: Apr. 25, 2024. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- [43] "Open Quantum Safe - TLS." Accessed: Apr. 26, 2024. [Online]. Available: <https://openquantumsafe.org/applications/tls.html>
- [44] "No Place to Hide: Serious and Organised Crime Strategy 2023-2028," Dec. 2023. Accessed: Apr. 25, 2024. [Online]. Available: [https://assets.publishing.service.gov.uk/media/65798633254aaa0010050bdc/SOC\\_Strategy\\_23-28\\_V9\\_Web\\_Accessible.pdf#:~:text=This%20complex%20web%20of%20organised%20criminal%20business%20operating,happen%20or%20provide%20a%20safe%20haven%20for%20criminals.](https://assets.publishing.service.gov.uk/media/65798633254aaa0010050bdc/SOC_Strategy_23-28_V9_Web_Accessible.pdf#:~:text=This%20complex%20web%20of%20organised%20criminal%20business%20operating,happen%20or%20provide%20a%20safe%20haven%20for%20criminals.)



## Appendices

Appendix 1: A worked example of the risk management process

ESO

# 1 System of interest

This fictional system of interest is based on a generic use case common within energy systems worldwide. It should not be taken as a literal example of a real-world system.

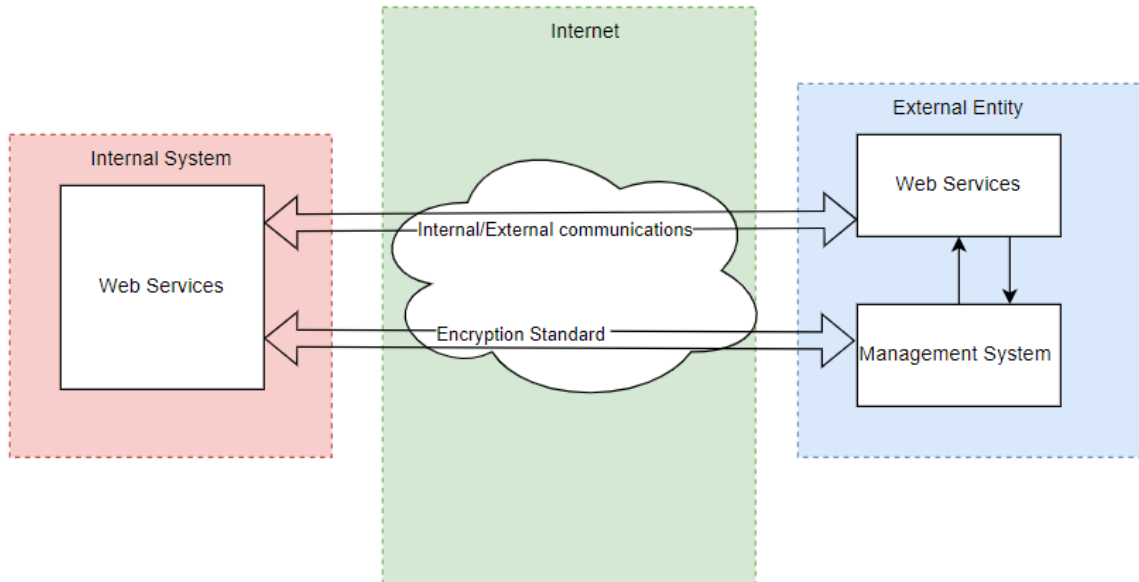


Figure 9 – The system of interest for analysis

In Figure 9 an example energy system is presented.

The “Internal system” is power balancing system operated by NGESO.

The “External entity” is a large power generation facility.

The “Web services” of the “external entity” process bids and offers from the balancing system to generate more power on the grid.

The “Management system” provides operational metering data about the energy generated to the balancing system.

All communications are performed using TLS encryption to secure JSON (Java Script Object Notation) payloads containing the relevant data.

## 2 Model analysis

In this section we shall apply the steps of the quantum-aware risk management process outlined in the main report, Section 3.5, to the system of interest.

### 2.1 Prepare

#### 2.1.1 Performing a system risk assessment

Threat sources can be found in the main report, Section 2.4. For this activity, high-capability nation state attackers with an objective to undermine grid stability shall be assumed.

Threat events can be found in the main report, Section 2.3.3 and are contextualised for this system in Table 7.

Vulnerabilities can be identified by cross-referencing the vulnerable software libraries identified in 2.3.1 against the use case. In this case we find that TLS versions 1.2 and 1.3 are vulnerable to quantum-enabled attacks.

At this stage in the RMF an organisational level risk assessment would be performed. For this example system we shall perform a lower-level system risk assessment. Each kill chain is assessed against the application to identify how the threats would be applied to this system.

Kill chain name	Interactions with this system
<b>Basic eavesdropping (K1)</b>	The basic eavesdropping scenario assumes that the encrypted communications are entirely performed using public-key encryption. This is not applicable in this case.
<b>Advanced eavesdropping (K2)</b>	<p>The communication between the load balancing system and power plant's bids/offers system is potentially vulnerable to advanced eavesdropping. This is reliant on the attacker i) having access to a cryptographically relevant quantum computer and ii) being able to launch a man-in-the-middle attack between the two entities.</p> <p>The communication of operational metering data between the load balancing system and the power plant is potentially vulnerable to advanced eavesdropping. This is reliant on the attacker i) having access to a cryptographically relevant quantum computer and ii) being able to launch a man-in-the-middle attack between the two entities.</p>
<b>Issuing malicious commands over an encrypted connection (K3)</b>	<p>The sending of bids/offers between the power plant and the balancing system is potentially vulnerable to malicious interference. This is reliant on the attacker i) having access to a cryptographically relevant quantum computer and ii) being able to launch a man-in-the-middle attack between the two entities.</p> <p>The sending of operational metering data from the power plant to the balancing system is potentially vulnerable to malicious interference. This is reliant on the attacker i) having access to a cryptographically relevant quantum computer and ii) being able to launch a man-in-the-middle attack between the two entities.</p>
<b>Installing signed malicious firmware/software (K4)</b>	<p>Computational assets within the balancing system are potentially vulnerable to maliciously signed software being installed on them. This is reliant on the attacker i) having access to a cryptographically relevant quantum computer and ii) the attacker being able to insert malicious software into the balancing system supply chain.</p> <p>Computational assets within the power plant are potentially vulnerable to maliciously signed software being installed on them. This is reliant on the attacker i) having access to a cryptographically relevant quantum computer and ii) the attacker being able to insert malicious software into the balancing system supply chain</p>

Table 7 – Kill chains applied to the system of interest

This analysis yields seven attack scenarios to assess for likelihood. For “Technical likelihood” only the technical feasibility of the attack is considered, under the assumption that the threat actor has access to a cryptographically-relevant quantum computer.

Scenario ID	Scenario description	Technical likelihood	Justification
1	Attacker decrypts the bids/offers between the balancing system and the power plant	High	Both systems are static, so launching a man-in-the-middle attack is relatively easy. There is no time limit on this type of attack, as the encrypted traffic and key exchange can be performed offline after being captured.
2	Attacker decrypts the operational metering data between the power plant and the balancing system	High	Both systems are static, so launching a man-in-the-middle attack is relatively easy. There is no time limit on this type of attack, as the encrypted traffic and key exchange can be performed offline after being captured.
3	Attacker falsifies a bid from the power plant to the balancing system	Moderate	It is assumed that any attacker with access to a cryptographically-relevant quantum computer has the technical capability to create a realistic looking data structure. This attack would be time limited by the key exchange frequency between the systems.
4	Attacker identifies the session key between the two entities and falsifies an acceptance from the balancing system to the power plant. To maximise the impact of this attack, the attacker also prevents legitimate data from being received by the power plant.	Moderate	It is assumed that any attacker with access to a quantum computer has the technical capability to create a realistic looking data structure. This attack is against the session key, so would be time limited by the key exchange frequency between the systems.
5	Attacker sends false operational metering data from the power plant to the balancing system	Moderate	It is assumed that any attacker with access to a quantum computer has the technical capability to create a realistic looking data structure. This attack would be time limited by the key exchange frequency between the systems.
6	Attacker installs signed, malicious software on the balancing system	Moderate	Obtaining the public key would be trivial through OSINT. Calculating the private key is assumed to be within the attacker's capability. The attacker must then find a way of injecting the signed, malicious software into the balancing system supply chain. The amount of time that the attacker has to do this is a function of how frequently trusted suppliers rotate their signing keys. A full analysis would consider the controls in place around the installation of signed software for the facility, but as the key rotation is potentially multiple years, for this analysis it is assumed that the attacker would eventually find a way.

Scenario ID	Scenario description	Technical likelihood	Justification
7	Attacker installs signed malicious software on the power plant	Moderate	Obtaining the public key would be trivial through OSINT. Calculating the private key is assumed to be within the attacker's capability. The attacker must then find a way of injecting the signed, malicious software into the balancing system supply chain. The amount of time that the attacker has to do this is a function of how frequently trusted suppliers rotate their signing keys. A full analysis would consider the controls in place around the installation of signed software for the facility, but as the key rotation is potentially multiple years, for this analysis it is assumed that the attacker would eventually find a way.

Table 8 – Quantum-enabled attack scenarios and their technical likelihoods applied to the system

Adverse impacts of each scenario are considered in Table 9.

Scenario ID	Impact description	Impact level	Justification
1	Bids/offer information is revealed to the attacker approximately 8 hours after transmission.	Very low	Bids/offers are typically issued on a 30 minute basis and are published on a website after acceptance. This assessment assumes that new shared secrets are established between parties for each bidding period and that the shared secrets are not reused across multiple bidding periods. Longer periods of key reuse would undermine this assumption.
2	Operational metering data is made available to the attacker.	Very low	There is very little an attacker can do with operational metering data. Aggregates of this data are regularly published on websites and the totals from various power sources (gas, solar, nuclear, imports, biomass, wind, coal) are published live through the ESO app.
3	A power plant receives a false request asking for power that is not required.	Moderate	In the event that the power plant acted on the bid, different types of power plant will have different levels of impact depending on their ramp up time and output power, etc. If the plant in question is a large provider, then over-producing would potentially cause an increase in grid frequency. For this to be problematic, the excess energy generation would have to be sustained, requiring a persistent attack. Automated control systems would attempt to compensate for this and in extreme cases some suppliers would disconnect from the grid if it exceeded their operating frequency. Energy export via interconnectors would also provide an avenue to release excess energy. As a result of existing controls and balances, it is not considered that this attack alone poses a significant threat to grid stability but could have financial impacts should the over-producing plant seek remuneration.
4	Energy that was relied upon for grid stability does not get generated.	High	If the power plant is a significant supplier to the grid, an attacker could cause a frequency reduction by preventing them from receiving bids, whilst maliciously offering to fulfil them on the plant's behalf. For this attack to have a significant impact, the generator would need to be a significant contributor, or the attack would need to be launched against several generators simultaneously. Independent frequency measuring systems would detect this, and the attacker would need to compromise operational metering data (see scenario 5) to create the illusion that the power plant was acting on the bids. A full analysis of this scenario would require a detailed knowledge of the alternative communications channels between the balancing system and power plants and their ability to intervene in a timely manner.

Scenario ID	Impact description	Impact level	Justification
5	Balancing system makes an incorrect decision based on inaccurate operational metering data.	High	The impact of this scenario is dependent on how large a generator the power plant is. It is also assumed that the attacker is only targeting a single source of operational metering data and not multiple power plants at once. Regardless, inaccurate operational metering data could result in a power plant looking like it is running at capacity when it is not running at all. In this situation the balancing system would lose that power plant as an option, limiting their ability to balance the grid.
6	Balancing system computers become compromised by malware.	Very High	Malware installed on the balancing system could jeopardise the system's ability to operate.
7	Power plant computers become compromised by malware.	Very High	Not only could losing the computer system jeopardise the power plant's ability to operate, but all other scenarios (miscommunication of operational metering data, false bid acceptance) are potentially realisable once the power plant computers can no longer be trusted.

Table 9 – Quantum-enabled attack scenarios and their impacts

Finally, an overall risk score can be assigned to the attack scenarios. For this analysis the risk matrix found in Appendix I, Table I-2 from NIST SP800-30 is used to calculate risk level from likelihood and impact.

Scenario ID	Technical Likelihood	Impact	Risk level
1	High	Very low	Low
2	High	Very low	Low
3	Moderate	Moderate	Moderate
4	Moderate	High	Moderate
5	Moderate	High	Moderate
6	Moderate	Very High	High
7	Moderate	Very High	High

Table 10 – Quantum-enabled attack scenarios and their overall risk levels

### 2.1.2 Common controls identified

Common controls to apply to these attack scenarios are listed in the main report, Section 3.4.



## 2.2 Categorise

Using the information model from the main report, Section 3.3 we can construct the following information model for the system.

Readers are reminded that this system is fictional and asset details do not directly correspond to a real-world system.

### Functional assets:

- Grid balancing (criticality: high)
- Power generation (criticality: high)

### Computational assets:

- System balancing web services (processing power: high, memory capacity: high)
- Power plant web services (processing power: high, memory capacity: high)
- Power plant management services (processing power: high, memory capacity: high)

### Operational information assets:

- Bids/offers (confidentiality impact: low, confidentiality lifetime: 30 mins, integrity impact: high)
- Acceptance data (confidentiality impact: moderate, confidentiality lifetime: 30 mins, integrity impact: high)
- Operational metering data (confidentiality impact: low, confidentiality lifetime: n/a, integrity impact: high)
- Balancing system services software (confidentiality impact: low, confidentiality lifetime: multiple years, integrity impact: high)
- Power plant services software (confidentiality impact: low, confidentiality lifetime: multiple years, integrity impact: high)

### Communication channel assets:

- Web service-Web service communications (latency demand: 1 minute, bandwidth demand: low)
- Operational metering data communications (latency demand: 1 second, bandwidth demand: low)

### Public-key cryptography assets:

- TLS 1.3 on Web service-Web service communications (key rotation period: 30 mins, underlying algorithm: Diffie-Hellman)
- TLS 1.3 on operational metering data (key rotation period: unknown, underlying algorithm: Diffie-Hellman)
- Unspecified authentication algorithm between internal system and external entity (key rotation period: unknown, underlying algorithm: unknown)
- Digital signatures on balancing system software (key rotation period: dependent on supplier, underlying algorithm: unknown)
- Digital signatures on power plant software (key rotation frequency: dependent on supplier, underlying algorithm: unknown)

Note that for real systems, not all properties will be known during the initial phase of the assessment. Making decisions in the face of these uncertainties will be important to the success of future phases of the work. It is also noteworthy that not all algorithms will be discovered simultaneously for all systems, so the asset list may highlight areas that require investigation.

## 2.3 Select

The final phase of the assessment is to assign possible mitigations to the risks identified, given the characteristics of the system.

Both communication channel assets are using public-key cryptography assets that are vulnerable to quantum-enabled attacks. While the digital signatures have not had an underlying algorithm specified, for the purposes of this analysis it will be assumed that they are vulnerable.

Risks have been grouped for ease of analysis.

Mitigation Type	Description	Applicability to web service-web service channel (risks 1,3, and 4)	Applicability to operational metering channel (risks 2 and 5)	Applicability to digital signatures for power plant/balancing system software (risks 6 and 7)
<p><b>Post Quantum Cryptography (PQC)</b></p>	<p>Replace at risk cryptography with an algorithm specifically designed to be resistant to quantum computers</p>	<p>All of the computational assets for this service are characterised by high computational power and high memory, making the implementation of PQC feasible.</p> <p>The bid/offers information asset being communicated by the channel has a high confidentiality impact rating for only 30 mins, currently thought to be below the threshold for being vulnerable to a quantum-enabled attack.</p> <p>The current control's key rotation frequency is 30 minutes, which is below the feasibility threshold for an attack against the integrity for the asset.</p> <p>The latency demands of the channel are extremely relaxed, meaning altering the underlying cryptographic algorithm is unlikely to have an impact.</p> <p>TLS supports downgrading the underlying algorithm to find a system that works for both entities, so the upgrade would not need to be simultaneous. However, until both the power plant and the balancing system support PQC a vulnerable algorithm would be used.</p> <p>Checks would need to be made to ensure that the intermediate networking systems could support the PQC algorithm.</p>	<p>The properties of this channel are similar to the web service-web-service channel. The notable exceptions being that the acceptable latency constraint is tighter, and the confidentiality impact is lower.</p> <p>An analysis would need to be performed on the feasibility of deploying PQC on the assets involved and impacts on intermediate networking equipment, above and beyond the properties identified in the asset model.</p> <p>The lower confidentiality impact further erodes the argument for upgrading to PQC.</p> <p>Overall, this would be a high complexity upgrade to perform with a moderate impact on the associated risks.</p>	<p>The computational assets that support this scenario are characterised by high computational power and high memory, making the implementation of PQC feasible.</p> <p>The confidentiality impacts of the information asserts involved are low. Limiting the benefits of PQC.</p> <p>The integrity impacts of the information assets involved are high. Increasing the benefits of PQC.</p> <p>There are no known bandwidth constraints for the transfer of digital signatures, making the use of PQC signatures feasible.</p> <p>Key rotation frequency is out of the hands of the consumer without an explicit contract.</p> <p>The adoption of PQC would need to be negotiated with the software supplier to be feasible.</p> <p>The operating systems of the affected devices may require</p>

Mitigation Type	Description	Applicability to web service-web service channel (risks 1,3, and 4)	Applicability to operational metering channel (risks 2 and 5)	Applicability to digital signatures for power plant/balancing system software (risks 6 and 7)
		<p>Overall, this would be a moderate complexity upgrade, with a moderate impact on the associated risks.</p>		<p>upgrading as current operating systems do not support PQC signatures out of the box.</p> <p>Overall, this would be a high level of complexity to upgrade with a high impact on the associated risks.</p>
<b>Hybrid approaches</b>	<p>Replace broken cryptography with a hybrid of a standard cryptographic approach and a PQC approach</p>	<p>This is similar to the PQC scenario, with the added advantage of not being entirely reliant on unproven technology. The increased computational demands are likely to be within the computational power/memory limits of the assets involved.</p> <p>Overall, this would be a moderate complexity upgrade, with a moderate impact on the associated risks.</p>	<p>This is similar to the PQC scenario, with the added advantage of not being entirely reliant on unproven technology. The increased computational demands are likely to be within the computational power/memory limits of the assets involved. But the increased latency introduced by that computation would need to be assessed to see if it was acceptable.</p> <p>Overall, this would be a high complexity upgrade, with a moderate impact on the associated risks.</p>	<p>Using both a traditional and a PQC signature to validate the integrity of the software would carry additional computational cost and process overhead.</p> <p>Overall, this would be a high level of complexity to upgrade, with a high impact on the associated risks.</p>
<b>Key lengthening</b>	<p>Increase the key length for a standard cryptographic approach</p>	<p>Keeping a traditional algorithm with a longer key size would preserve the confidentiality of the data for longer and lengthen the amount of time a given session could be left</p>	<p>Keeping a traditional algorithm with a longer key size would preserve the confidentiality of the data for longer and lengthen the amount of time a given</p>	<p>Given the infrequency of key rotation for digital signing process, this mitigation is unlikely to have</p>

Mitigation Type	Description	Applicability to web service-web service channel (risks 1,3, and 4)	Applicability to operational metering channel (risks 2 and 5)	Applicability to digital signatures for power plant/balancing system software (risks 6 and 7)
		<p>running without needing to change keys.</p> <p>Key lengthening still requires a software algorithm change to the system and would have an impact on the bandwidth consumed by the key exchange.</p> <p>Overall, this would be a moderate complexity upgrade with a low impact on the associated risks.</p>	<p>session could be left running without needing to change keys.</p> <p>Key lengthening still requires a software algorithm change to the system.</p> <p>Overall, this would be a high complexity upgrade (given the assessment requirements) with a moderate impact on the associated risks.</p>	<p>much impact on the risk.</p> <p>As with all signature-based mitigations, there is additional complexity stemming from the fact that the signatory is outside of the managing organisation.</p> <p>Overall, this would be a moderate complexity upgrade with a low impact on the associated risks.</p>
<p><b>Increase key exchange frequency</b></p>	<p>Mandate the rotation of private keys</p>	<p>For small confidentiality lifetimes, like those associated with the information assets for this scenario, rotating the keys more frequently is likely to be a cheap way of ensuring that the attacker cannot access the information within the time window that it is sensitive.</p> <p>Key rotation mechanics already likely exist within the system, so it is likely that this is a low complexity upgrade.</p> <p>Overall, this would be a low complexity upgrade with a low impact on the associated risks.</p>	<p>For latency constrained scenarios, increased key rotation can introduce an unacceptable delay. Such a change would need to be assessed before implementation.</p> <p>Key rotation mechanics already likely exist within the system,.</p> <p>Overall, this would be a moderate complexity upgrade with a low impact on the associated risks.</p>	<p>Rotating the private key/public key pairing for the digital signature for a piece of software introduces an overhead to ensure that the current public key is still valid. This would not only require an update at point of install, but would potentially require checks every time the system was run, depending on operating system configuration.</p> <p>Overall, this would be a high complexity upgrade, with a moderate impact on the associated risks.</p>

Mitigation Type	Description	Applicability to web service-web service channel (risks 1,3, and 4)	Applicability to operational metering channel (risks 2 and 5)	Applicability to digital signatures for power plant/balancing system software (risks 6 and 7)
<b>Architectural changes</b>	Restructure the system in a way that limits the man-in-the-middle opportunities for the attacker	<p>Rearchitecting the solution to avoid man-in-the-middle attacks would likely require significant investment and analysis.</p> <p>Overall, this would be a high complexity upgrade with an unknown impact on the associated risks.</p>	<p>Rearchitecting the solution to avoid man-in-the-middle attacks would likely require significant investment and analysis.</p> <p>Overall, this would be a high complexity upgrade with an unknown impact on the associated risks.</p>	<p>Other controls could be introduced to ensure the integrity of the software from different suppliers. For example, secure web portals to push updates from authenticated users. However, this would need to be negotiated on a case by case basis with suppliers.</p> <p>Overall, this would be a high-complexity upgrade with an unknown impact on the associated risks.</p>
<b>Alternative key exchange mechanics</b>	Continue to use symmetric cryptography, but find alternative channels to establish the shared secret	<p>There are no other well-established communication channels that would allow the secure passing of private keys for this scenario.</p> <p>Physically transferring symmetric keys is possible, though carries its own risks in terms of the security of the courier and the physical security of the portable media being used to store the keys. Additional policies would need to be put in place to ensure that this was done in a secure manner.</p> <p>Overall, this is a high complexity upgrade with a high impact on the level of risk.</p>	<p>There are no other well-established communication channels that would allow the secure passing of private keys for this scenario.</p> <p>Physically transferring keys would carry the same issues as risks 1,3, and 4.</p> <p>Overall, this is a high complexity upgrade with a high impact on the level of risk.</p>	Not applicable.

Mitigation Type	Description	Applicability to web service-web service channel (risks 1,3, and 4)	Applicability to operational metering channel (risks 2 and 5)	Applicability to digital signatures for power plant/balancing system software (risks 6 and 7)
Phase out asset	Accelerate the removal of the asset with an intent to either a) discontinue the service being supported by the asset function, or b) replace the asset with an asset that can support one of the above mitigations	Not applicable: service is still required.	Not applicable: service is still required.	Not applicable: service is still required.

Table 11 – An evaluation of the common mitigations against each risk

In summary, the options for securing this system against quantum-enabled attacks are:

For risks 1, 3, and 4 the mitigation assessments are:

- Post Quantum Cryptography (PQC): moderate complexity, moderate impact
- Hybrid approaches: moderate complexity, moderate impact
- Key lengthening: moderate complexity, low impact
- Increase key exchange frequency: low complexity, low impact
- Architectural changes: high complexity, unknown impact
- Alternative key exchange mechanics: high complexity, high impact
- Phase out asset: n/a

For risks 2 and 5 the mitigation assessments are:

- Post Quantum Cryptography (PQC): high complexity, moderate impact
- Hybrid approaches: high complexity, moderate impact
- Key lengthening: high complexity, moderate impact
- Increase key exchange frequency: moderate complexity, low impact
- Architectural changes: high complexity, unknown impact
- Alternative key exchange mechanics: high complexity, high impact
- Phase out asset: n/a

For risks 6 and 7 the mitigation assessments are:

- Post Quantum Cryptography (PQC): high complexity, high impact
- Hybrid approaches: high complexity, high impact
- Key lengthening: moderate complexity, low impact
- Increase key exchange frequency: high complexity, moderate impact
- Architectural changes: high complexity, unknown impact
- Alternative key exchange mechanics: n/a
- Phase out asset: n/a

### 3 Conclusions

This analysis assumes that the risks associated with this system are likely to manifest within the lifetime of the system. In some ways this is dependent on the expected date of a cryptographically relevant quantum computer being developed, but all of the functions being performed within this system are essential services and unlikely to become obsolete before the advent of such devices.

The risk assessment does not include any risks around the compromise of authentication keys. This omission is considered to be an artefact of the asset model, which does not explicitly record authentication algorithms. This should be amended in the future.

For the communication of bids/offers and acceptances (associated with risks 1,3, and 4) the highest impact change would be to establish a shared secret between the two entities via the transportation of physical media. This would introduce new risks and require new policies on both sides. The adoption of a hybrid PQC solution like Boring-SSL [43] would have a moderate impact on the risks with moderate complexity. This is seen as the superior solution to adopting a PQC-only approach as it also mitigates the risk that a vulnerability is found in the PQC algorithm itself.

For the communication of operational metering data (associated with risks 2 and 5), the latency requirements demand that a more careful analysis be performed to have confidence in any solution. The only high-impact solution is to adopt physical key exchange, which seems feasible initially given the static nature of the relationship between the entities. However, it is important to note that the balancing system is likely required to interact with a large number of market participants, and that list is likely to grow as the energy sector becomes more distributed, so the complexity of the solution will grow. Lengthening the keys may be quicker to achieve than completely changing the underlying algorithms and could buy the system some extra time until upgrading to a PQC or hybrid approach could be fully analysed and explored.

For the checking of digital signatures, (risks 6 and 7) the technical likelihood is predicated on the existence of a cryptographically-relevant quantum computer. There is no opportunity for an attacker to launch a delayed attack (like a SNDL attack against the confidentiality of shared data). As a result there is less urgency to address this challenge than the other risk types, despite its higher consequences. Much of the complexity arises from the need to negotiate the software signature technique with the software vendor, and the lack of support for PQC in current operating systems. Architectural changes, using PQC to establish secure tunnels between the vendor and the installer would protect against tampering of the software between release and installation, thus partially reducing the risk. However, other sources of tampering would still be undetectable in the event the attacker had access to a cryptographically-relevant quantum computer.





Faraday House, Warwick Technology Park,  
Gallows Hill, Warwick, CV346DA

[nationalgrideso.com](http://nationalgrideso.com)

**ESO**