Quantum Power Play: Navigating the New Landscape of Cybersecurity and Defence

15 minutes read
07 Aug. 2025

Rachel Hunt
Cybersecurity

In a digital era, quantum computing threatens defence encryption. In defence, encryption isn't just tech – it's sovereignty. Are we ready?

In brief

- In the digital age, cybersecurity in defence is vital, with encryption ensuring the security and integrity of communications and data. Today, quantum computing threatens this security, with nations and private companies competing existing cryptographic systems.
- Defence operations, Strategic, Operational and Tactical levels, with each level's encryption implications differing. Given the vast number of devices and components at each level, securing data across these levels presents significant challenges and risks.
- For effective risk mitigation, defence entities should follow cybersecurity principles, focusing on adopting governance and project delivery, need to incorporate post-quantum security tools. Technically, understanding data cryptanalysis and staying updated with cryptographic advances is vital.

In an increasingly digital age, the defence and national security industries place a significant emphasis on robust cybersecurity, with encryption playing a pivotal role in securing communications and data. This importance is underscored by the paramount need for preserving confidentiality and maintaining communication integrity to protect a nation's sovereignty, as evidenced by historical events such as the use of the Enigma machine during World War II.

Presently, quantum computing introduces a comparable challenge to the Enigma, driving the defence industry's reliance on cybersecurity and encryption technologies. The advent of quantum computing presents both intriguing prospects and formidable challenges. The superior computational capabilities of quantum computing pose a threat to the security of encrypted data by potentially rendering current encryption cryptographic systems, such flaws are not newly theoretical—remember the "harvest now, decrypt later" strategy discussed in our previous cybersecurity insights—vulnerable to decryption. This vulnerability is exacerbated by its discipline. In the defence industry's risk agenda, which is defined by the consequences of failure, does not leave room to keep risk unrecognised and not mitigated.

Defence operates at three levels of influence: Strategic, Operational and Tactical. The impact of changes to encryption standards varies across these levels, with the Strategic level facing the most significant risks due to the vast quantities of data it controls and its reliance on encryption. It must ensure control over both internal operational and strategic information to generate predictions about future engagements and reveal confidential intentions. Another overarching national defence effort, The deep volume and variety of devices on the modern cyber-physical battlefield highlight the complexity and importance of this task.

To mitigate potential risks, it has become increasingly clear that defence organisations should undertake risk assessments and implement strategies to address these risks. This proactive approach ensures the preparedness and resilience against post-quantum security requirements. Our a technical level, it's crucial for defence organisations to stay proactive, understand their data in depth, and keep themselves updated with the latest cryptographic advancements. The adoption of Post-Quantum Cryptography (PQC) algorithms should be a priority. Another area the defence organisation should consider is the usage of innovative approaches like Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNG) to enhance the current cyber security posture. However, the adoption of these solutions must be approached with caution.

Have to quantum computing differentiated from today's computers?

For centuries, people have sought to solve complex computational problems. The advent of classical computers has enabled the efficient resolution of many such challenges. However, classical computing has its limitations, and numerous problems of interest remain beyond its capabilities. Notoriously, classical computers struggle with only possible model, and researchers have long sought more powerful computational frameworks.

Quantum computing is one such model, offering a means to address some of these challenges with the reach of classical computers. While there have been various models proposed that could theoretically outperform classical computers, many have remained where it comes to practical implementation. There is, however, significant roadblocks such as scalability issues and an inability to surpass what is called 'noise', purely unwanted data alterations that cause errors/mistakes, leading to incorrect and misleading results. After all, what good is a computing device if its results can't be trusted due to constant interference from random impacts? Quantum computing has made significant strides in addressing these challenges, demonstrating enhanced stability compared to other computational models, suggesting it has the potential to provide useful results.

Numerous tech-focused articles delve into the technicalities of quantum computing, touching on aspects such as qubits, superposition, and entanglement. These impressive scientific concepts, some of which have been mentioned in our previous insights, underpin the operation of quantum computers. However, this study zeroes in on Shor's algorithm, a quantum algorithm that's renowned for its further understanding of quantum computing's impact. Consider the analogy of trying to explain television's societal influence by starting the explanation with the principles of vacuum tube design functions and display mechanisms. While such approach might enter the bigger picture. Similarly, a deep understanding of quantum properties doesn't necessarily translate into clarity about the wider implications and advantages of quantum computing. Rather than dissecting the technical mistake underpinning quantum computing, this article focuses on exploring the tangible consequences and benefits this technology can provide.

Quantum computers' ability to crack complex computational problems presents both advantages and risks. On the one hand, they offer significant benefits and potential applications across various industries, from medical design to financial portfolio optimisation. On the other hand, they pose considerable risks to cybersecurity.

Quantum computing is a double-edged sword for cybersecurity

Quantum computing's accelerated progress over the past decade, including through its technological breakthroughs and increasing investment from governments and private entities, underscores its transformative emergence, if people so forward. Where the traditional cryptographic systems on with no value may no longer be considered secure.

But it's not just about the hardware; cutting-edge algorithms are continually being developed, requiring fewer resources to compromise conventional cryptography. As these developments evolve, they spark a dual sword and scale of track, all infrastructure, data, and communications, are directly at the line of fire of this quantum revolution.

A particularly worrisome threat is the growing use of the "harvest now, decrypt later" attack by malicious cyber actors, including state-sponsored and highly organised criminal entities. In this approach, adversaries actively gather a wealth of encrypted data today, patiently waiting until they possess the power of quantum computers to decrypt this information in the future. This enabling strategy is being applied across all sectors of the economy and in parts of the community as the underlying value of data and the decreasing costs of storage^{1} make it increasingly viable.

The rise of this cyber threat is just mirrored by the co-emergence of insider threat in its palpable among some adversaries, motivated and in the means to access and exploit the most secure of infrastructure in their design and operation as well as the most highly held information.

The chilling truth is that even the most highly protected secrets could be revealed before they are considered secure enough for those who own them.

The "harvest now, decrypt later" attack underscores the immediate risks quantum computing poses to cybersecurity. As quantum computing advances, attackers are increasingly motivated to execute this strategy, anticipating that at-scale decryption solutions will soon become available.

To maximise the effectiveness of such attacks, perpetrators typically target:

1. Structured data encrypted with a single key, as a successful breakthrough can reveal a large volume of information, increasing the likelihood of acquiring valuable data.
2. Data with a long shelf life, as delayed decryption and extended data longevity improve the chances of retaining valuable information in the future.

As quantum hardware continues to develop and the cost of attacks decreases, even short-lived and less structured data will be a higher risk of being targeted as the world gets closer to the first cryptographically relevant quantum computer. A cryptographically relevant quantum computer is a quantum computing device capable of performing tasks that compromise modern cryptographic systems.

The development of quantum technology not only introduces risks but also offers opportunities to improve existing security systems. Two promising and increasingly secure quantum-based approaches that can enhance current encryption methods are Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNG).

QKD enables the secure exchange of cryptographic keys between two parties, utilising the fundamental properties of quantum mechanics to ensure the key's confidentiality. In the event of eavesdropping attempted, the quantum states are disturbed, alerting the communicating parties and enabling them to respond accordingly. QRNG, on the other hand, leverages the inherent unpredictability of quantum phenomena to generate truly random numbers. These random numbers can be employed in various cryptographic applications, including the security of encrypted data and order it harder and thereby more expensive for adversaries to break.

While these two solutions alone will not eliminate the risks associated with quantum computing, they hold the potential to enhance existing encryption approaches. They also complement other forms of current cybersecurity technical technologies as well as largely leveraging existing infrastructure. This means such options provide a bridge between today's most commonly used forms of encryption and what will come next in a post-quantum computing landscape and help "buy down" the risks associated with the "harvest now, decrypt later" attack.

Addressing the risks associated with quantum computing, downside and upside, primarily depends on classical approaches, with the development of quantum-safe cryptography being a central aspect of this effort. Quantum-safe cryptographic algorithms are founded on certain assumptions, with one of the most critical being the hardness assumption^{2}. This particular assumption takes into account the computational resources required for an attacker might have and the level of difficulty they would face when attempting to solve a problem or by breaking a cryptographic system. The security of cryptographic algorithms hinges on these hardness assumptions which, broken for many algorithms, particularly asymmetric ones.

To address these challenging problems, researchers have focused on the development of Post-Quantum Cryptography (PQC) algorithms^{3}, which incorporate problems that are difficult for quantum computers to solve. While the development of PQC algorithms alone will not eliminate the risks, it does provide a crucial foundation for tackling the issue.

In response, organisations need to start developing a comprehensive strategy to mitigate the risks and take a whole-of-enterprise approach to understanding the implications of legacy infrastructure and data as well as the implications for technology that will be completely disrupted by the compact power of quantum-based infrastructure, applications and technologies.

The first step in this strategy involves gaining a thorough understanding of the data they possess, how it is stored, and the duration it needs to remain confidential. This knowledge is crucial for organisations to better assess their potential use cases, fix long-popular and simply informed about the threat advancements in cryptography, organisations can effectively navigate the challenges posed by quantum computing.

What role does encryption have in National Security interests?

The defence and national security industries prioritise cybersecurity increasingly effectively. With the rapid advancement of quantum computing technology, ensuring the security of encrypted data has never been more critical. It has the form of communications and infrastructure. The security of this challenges and consequences of failure remain is extremely high, a key driver for why the Defence industry continuously invest significant resources to combat the latest threats as well as deal with legacy vulnerabilities.

The preservation of confidentiality and the safeguarding of communication integrity, whether it's in the field or between offices in the Defence force, hold paramount importance for a nation's sovereignty. A glaring lack of cybersecurity could lead to the loss of vital data, jeopardising the nation's security. In the realm of modern conflict, the Enigma machine played a pivotal role, ensuring that critical messages dispatched to the front lines remained safeguarded strategic and operational secrets. The risk of not dramatically turned when Allied forces managed to decipher the Enigma's keys, leveraging the advent of computing technology to expedite the trajectory of enormous battles. Fast forward to the present day, Quantum computing presents a similar challenge to the Defence industry, with the potential to decrypt sensitive data at unprecedented speeds and disrupting defence strategies. As history often has a tic of repeating itself, the lessons learned from past may very well dictate how successfully we navigate this new era of quantum-encrypted communication.

It is essential for the Defence industry to rely on cryptographic technology that is both reliable and effective, in ways that can extend decades and be subjected to constant use and adaptation. Stakeholders therefore remain vigilant in their efforts to ensure the most advanced and secure encryption methods are employed to protect their assets and interests.

By way of example, in military communications systems, cryptography plays a critical role, as it safeguards sensitive data and communications between military personnel and allies between the millions of allied nations, thwarting interference, misinformed actions and espionage. Consider a situation where a nation's military communication systems are dependent on antiquated cryptographic technology, leaving it vulnerable to adversaries.

Aggressive engaged with quantum computing capabilities could intercept, decode, and manipulate classified information to their advantage, jeopardising national security and military operations. Such a compromise could result in strategic failures, loss of life and lasting harm to a nation's global reputation.

This imbalance is not acceptable and severely affects a nations ability to defend its interests.

The impact of changes to encryption will change depending on the type and level of communications being encrypted. Continuing the example, Defence operates at three levels of influence, Strategic, Operational and Tactical.

Strategic

The strategic level pertains to national policy and theatre level movements, is defined by large scale, high importance information with both short- and long-term implications. The information encompasses long term strategic continuing information such as capability planning and development blueprints, pre-planned operational movements and engagements, and critical intelligence gathering and analysis. Given the vast quantities of data and the significant long-term implications associated with this information, such strategic often include intelligence agencies and their coalition counterparts as well as trusted defence industry capabilities partners. This balance of power is given over and actual conflict circumstances is mainlined or but based on the ability of a nation and/ or its allies to secure its environments.

Strategic level encrypted communications and data therefore routinely have medium to long life spans with a high level of protection against adversaries. The risk of "harvest now, decrypt later" attacks on this information is even more lengthy cultural at time, would have significant implications for a nation's ability to secure national policy and engage in conflicts at all levels. Securing strategic level communications, tradecraft and classified information with post-quantum cryptography is a form of many governments and defence organisations are the challenges posed to a nation by quantum computing. While it is certainly an important consideration, it is not the only problem to be addressed with the development of robust quantum cryptography.

Operational

The operational is the level of campaigns and major operations to achieve a specific national objective in line with some given strategic intent.

Operational communications and data often have short- to medium-term life spans with decisions having the potential to impact both the tactical and strategic levels. Data associated with operational level movements has a medium life span and is of medium importance. The information encompasses the movement of forces, adversaries identified as advance operational level movements and strategic-effective or tactical-effective changes in operational tempo such as a shift from offensive to defensive operations. These opposing forces would then be able to position themselves to best respond to those operational movements and cause significant disruption, effect, should they be military or, not far away threat active to interfere with a conflict zone for a range of reasons related or unrelated to the conflict itself.

Tactical

The tactical is the level of small-unit tactics, engagements and individual battles, it is defined by short-term communications with highly time-sensitive information and intelligence. The ability for these actors to decrypt this information is vital time would allow them to disrupt or prevent these tactical level movements or operations and conflict to a conclusion. The time sensitive nature of these communications, with data life on the scale of minutes or even seconds, means the impact of decryption will only be felt once processing speeds advance sufficiently to crack and view processing.

Tactical level data may also be subject to "Harvest Now, Decrypt Later" attack to understand small unit tactics and deployment of high value assets. This would enable threat actors to use tactical level information gathered in the past to generate predictions and assessments about future engagements, generating a potentially operational or even strategic level effect through the exploitation of tactical level data. Securing tactical level communications with PQC is therefore essential to ensuring threat actors do not gain complete access to tactics, techniques and procedures.

This presents a significant problem due to the breadth and quantity of devices carried at the tactical level on the modern cyber-physical battlefield, each with its own cryptography and communications need. The administrative and technical burden in identifying, updating and retrofitting these devices to tactical level units should not be underestimated.

The quest for quantum-secure cryptographic solutions

Solutions to the challenges posed by quantum attacks on cryptography as a response require not only technical advancements but also improvement of the overall organisational cyber maturity. From a governance perspective, response requires policy development and the establishment of new cryptography standards.

Post Quantum Cryptography algorithms

The most fundamental response to these challenges is the development of new cryptographic algorithms. These PQC algorithms are designed to withstand attacks from both classical and quantum computers.

The US Government's National Institute of Standards and Technology (NIST) is playing a central role in the development of PQC algorithms. Recognising the need for new cryptographic standards, NIST initiated a multi-wide open competition to assist in identifying and evaluate novel PQC algorithms. This rigorous, multi-phase process involves collaboration with experts from academia, industry, and government agencies. The development of new algorithms is approaching its final stage, with final recommendations expected in areas 2024 with the finalised standards on the selection process and the standards.

NIST's primary goal is to standardise one or more PQC algorithms that demonstrate robust security properties, efficient performance and practical applicability. By establishing these new standards, NIST aims to facilitate the widespread adoption of PQC, ultimately ensuring the continued protection of sensitive information while we learn more about the potential third frequency quantum computing capabilities and vulnerabilities.

However, despite the promise of PQC, several challenges must be overcome before these new algorithms can be widely implemented.

- First, PQC algorithms tend to be more computationally demanding than their classical counterparts, which may result in performance bottlenecks.
- Furthermore, most PQC algorithms require larger key sizes, leading to increased storage and transmission costs.
- The diversity of cryptographic algorithms fundamentally hinges on the assumption of complexity—the idea that there is an efficient method to solve a given problem using the resources at hand.

This is particularly relevant when discussing Post-Quantum Cryptography (PQC), where quantum computing represents an added resource. This assumption is continually challenged by making the design of these algorithms public, thereby inviting everyone to attempt to crack them. This is exactly the approach that the National Institute of Standards and Technology (NIST) adopts.

It is important to remember that trust in the security of cryptography algorithms is built over time. This, making a direct leap from classical algorithms to PQC ones could entail certain risks. Given that PQC algorithms are currently under rigorous scrutiny and recent studies have highlighted potential vulnerabilities^{4}, caution is advised. Interestingly, one of the final contenders in a recent algorithm competition was broken using just a laptop^{5}, leading to its elimination at the final stage.

Therefore, the transition to PQC algorithms requires thoughtful deliberation. One feasible solution could be the "double-wrapping" method^{6}. In this approach, a message is encrypted twice, first, with a classical algorithm to counter known threats, and then with a quantum algorithm to fend off attacks from quantum computing.

Governmental approaches – Australia and its closest allies

Governments around the world are taking steps to protect against the potential risks associated with quantum computing. These steps include investing in research and development, forming partnerships and developing regulations.

On December 19, 2022, President Biden signed into law H.R.7535, the Quantum Computing Cybersecurity Preparedness Act^{7}. This act encourages federal government agencies to adopt technology that will protect against quantum computing attacks. The act also requires NIST to develop standards for post-quantum cryptography.

In addition, the United States government has outlined its goals to maintain the nation's competitive advantage in quantum information sciences (QIS) while safeguarding the quantum component to the nation's cybersecurity, economic and national security in National Security Memorandum 10^{8}. The memorandum aims to balance the competing requirements of fostering a robust quantum ecosystem by maintaining United States leadership in QIS through continued investment, partnerships and a balanced approach to technology promotion and protection.

The United Kingdom government has been working on a new quantum strategy^{9} to mitigate the risks associated with quantum computing. To date, the conversation in that nation has focused less on risk mitigation and more on the quantum research and commercialisation agenda that will enable responses to risk.

The Australian National Quantum Strategy^{10} launched on May 2, 2023, establishes a long-term vision for Australia to capitalise on the opportunities presented by quantum technologies. However, it notably lacks direct reference to the cybersecurity consequences of current and emerging quantum technologies and quantum computing. Finally, the Strategy should inform the new National Cyber Security Strategy^{11} due for release later in 2023, the requirement for articulating the intersection has not yet been stated.

Returning to the defence environment, the AUKUS trilateral security agreement between Australia, the United Kingdom, and the United States underscores the importance of collaboration among these nations in developing responses to risk. This alliance will contribute vitally to enhancing their cyber and joint quantum capabilities among other aspects of emerging technologies for military application. There will invariably be spill-over benefits for non-defence environments also.

Industry response

In response to the rapid development of quantum technologies and their cyber risks, many organisations have started to prioritise post-quantum network solutions as part of implementing digital transformation or technology refresh strategies. However, developing technical solutions alone is insufficient to resolve the underlying risks. Organisations must implement proper management processes and treat the challenge as an organisation-wide project, also addressing implications for processes and workforces.

As mentioned above, a first step in the journey is gaining a comprehensive understanding of the data held and stored as well as its expected lifespan. Following this is mapping organisation risks to enterprise-wide impacts. At this stage, it is important to acknowledge that the set of quantum-risks identified will lead to updating cybersecurity and IT strategies accordingly.

Risk organisation is a good practice, as it enables better informed decisions when planning remediation and properly prioritising responses, to match the same way as it does in cybersecurity. Strategically, these steps will culminate in developing an enterprise-wide timeline and allocating a budget for a post-quantum implementation strategy.

Raising awareness at different levels of the corporate hierarchy is equally important, as each level of stakeholders plays an independent role in remediation and should receive appropriate information to enable efficient mitigation.

As mentioned above, a first step in the journey is gaining a comprehensive understanding of the data held and stored as well as its expected lifespan. Following this is mapping organisation risks to enterprise-wide impacts. At this stage, it is important to acknowledge that the set of quantum-risks identified will lead to updating cybersecurity and IT strategies accordingly.

Risk organisation is a good practice, as it enables better informed decisions when planning remediation and properly prioritising responses, to match the same way as it does in cybersecurity. Strategically, these steps will culminate in developing an enterprise-wide timeline and allocating a budget for a post-quantum implementation strategy.

Raising awareness at different levels of the corporate hierarchy is equally important, as each level of stakeholders plays an independent role in remediation and should receive appropriate information to enable efficient mitigation.

Summary

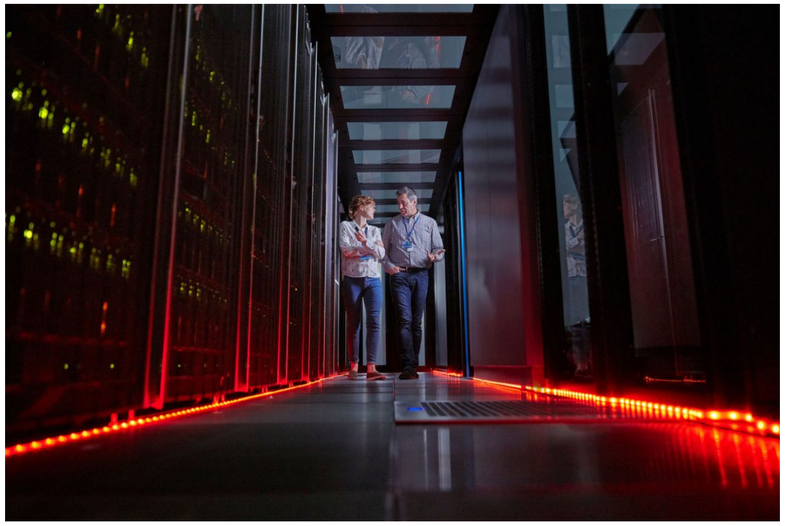
In the digital era, the defence and national security sectors in Australia heavily prioritise cybersecurity and encryption to ensure communication and data protection against adversaries. The rise of quantum computing presents potential threats as it could compromise encrypted defence data. Recognising these risks, the defence sector should adopt cybersecurity principles, focusing on governance and project delivery, and incorporate post-quantum cryptography tools. Understanding quantum cryptanalysis and staying abreast of advancements in Post-Quantum Cryptography (PQC) algorithms is further cybersecurity while exercising caution in implementing these

About this article

Accessibility
Cookie Preferences

Cybersecurity

Our latest thinking



Quantum computers will break the existing confidentiality paradigm. The only question is when?

Quantum-in-cyber risk needs attention today

31 Jan 2023 | **EY Global**

Ready your quantum workforce

We explore the skill gap challenges related to quantum technologies. Learn what practical steps talent leaders can take now.

25 Nov 2022 | **Robin Brown + 3**

EY refers to the global organisation, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.