ExpertView

Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
16/23

# Future-Proofing Encryption: The Imminent Threat of 'Store Now, Decrypt Later' and Quantum Computing

**Captain Sunil Tyagi**
*Senior Fellow, CAPS*
*07 November, 2023*

**Keywords:** Quantum Computing, Store Now Decrypt Later (SNDL), RSA Algorithm, Shor's Algorithm

## Introduction

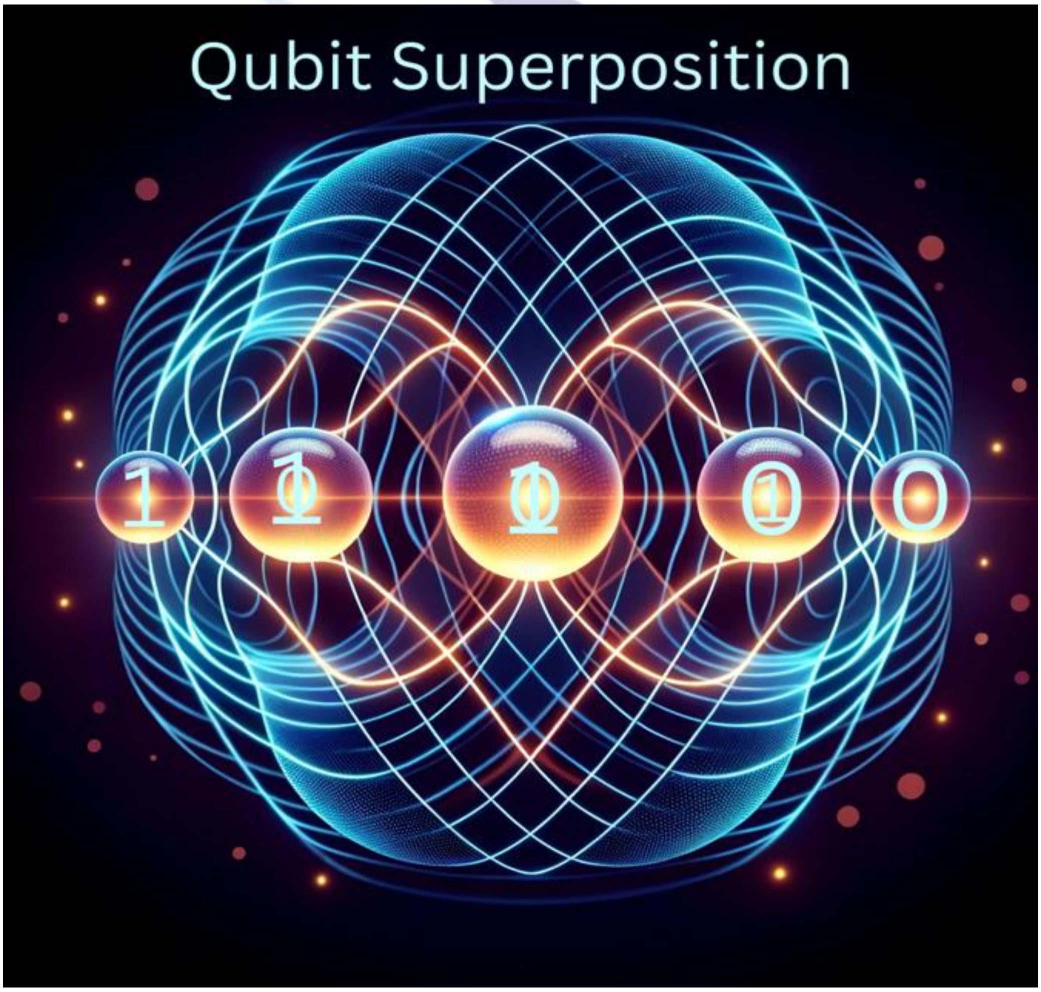
The advent of quantum computing has cast a shadow of uncertainty over the robustness of existing military encryption methods. Classical encryption algorithms like RSA, named after its three scientists, Riverst, Shamir, and Adelman, who created the algorithm, was once considered secure, but are now susceptible to being cracked by quantum computers. The Store Now, Decrypt Later (SNDL) approach is a specific and emerging threat in this context. This tactic capitalises on the weaknesses inherent in RSA encryption when faced with machines possessing immense computational capabilities. As a result, SNDL poses a significant risk to the confidentiality of critical military data and communications. Given the rapid advancements in quantum computing technology, it is becoming increasingly crucial for cybersecurity experts, military officials, and tech aficionados to fully grasp the ramifications of SNDL-based threats. Moreover, it's vital to actively explore and implement defensive strategies to safeguard against such vulnerabilities. This article aims to provide an in-depth analysis of the rise of quantum computing, its impact on military encryption standards, and potential countermeasures to neutralise the threats posed by SNDL tactics.

## Store Now, Decrypt Later (SNDL)

SNDL refers to the interception and storage of encrypted data to decrypt later. This approach assumes that the encrypted data can be decrypted in the future by exploiting advancements in technology, computational power, or breakthroughs in encryption algorithms. There's always a possibility of significant advancements in the field of cryptanalysis, which could lead to the discovery of vulnerabilities or weaknesses in encryption algorithms. There is also a strong possibility that the computational capabilities may increase so much in the future that it would be possible to crack even the best encryption methods. Storing encrypted data could be a way to prepare for such breakthroughs.

In his report, Ravi Sen, a cyber-security expert at Mays Business School, Texas, mentions[1] that many states and non-state actors are indulging in data breaches and stealing billions of records worldwide every year. It is feared that Chinese threat groups may already be collecting the encrypted data with long-term utility aims[2]. In April 2023, US FBI director Christopher Wray revealed to a US Congress panel that Chinese hackers outnumber FBI cyber staff 50 to one, and the US and other countries are facing immense cyber threats, particularly from China[3].

**Figure 1: Qubit Superposition image**



*Source*: Author's articulation

## The Rise of Quantum Computing and its Implications

*Understanding Quantum Computing*

Quantum computing is a revolutionary technology that leverages the principles of quantum mechanics to perform computations. Unlike classical computers, which use bits to represent information as either 0 or 1, quantum computers use quantum bits or Qubits. Qubits can exist in multiple states simultaneously, thanks to a property called superposition.

This unique characteristic enables quantum computers to solve complex problems exponentially faster than classical computers. Tasks that would take years or even centuries for classical computers to complete can be solved in a matter of seconds or minutes with quantum computers. This speed and computational power have significant implications for various industries, including military encryption.

*The Implications for Military Encryption*

RSA encryption, a cryptographic method used by military institutions and other organisations, hinges on the computational complexity of breaking down large composite numbers into their prime components. In contemporary RSA-based cryptography, the prime numbers employed can be astonishingly large, often extending up to 617 decimal digits[4]. Attempting to factorise such an enormous public number, which serves as a cornerstone in RSA encryption, presents a formidable challenge. This is true even when utilising the most advanced factoring algorithm available today, known as the General Number Field Sieve, on cutting-edge supercomputers.

To put this into perspective, even if one were to deploy the General Number Field Sieve algorithm on a state-of-the-art supercomputer, the process of factorising such a colossal number—a product of two prime numbers—would be an endeavour spanning years. For instance, a study by Kleinjung et al. in 2010 illustrated the magnitude of this challenge[5]. They demonstrated that cracking a 232-digit RSA encryption would necessitate nearly 2000 years of continuous computing on a single-core 2.2GHz AMD Opteron computer.

However, the entire landscape has undergone a seismic shift with the advent of quantum computing. In stark contrast to traditional computing methods, quantum computers can solve these complex computational challenges in a significantly shorter time frame. This is mainly due to the utilisation of Shor's algorithm, which is specifically designed for quantum computing environments to factor large prime numbers efficiently. As a result, RSA encryption, once considered impervious, becomes vulnerable. Quantum computing coupled with SNDL threatens to upend today's cryptography security paradigm. The compromise of military encryption poses severe consequences for national security. Unauthorised access to sensitive information can lead to intelligence leaks, compromised communications, and potentially catastrophic outcomes on the battlefield. Security professionals and military personnel must understand these implications and take proactive measures to protect against SNDL.

In the following sections, we will explore advancements in encryption technology that aim to provide resistance against quantum attacks and discuss countermeasures and strategies to mitigate the threat posed by Store Now Decrypt Later attacks on military encryption systems.

## Protecting Against Store Now Decrypt Later Attacks

### *Advancements in Encryption Technology*

People are aware of this threat posed by SNDL and quantum computers combination. The US NSA publicly stated in 2019 that a sufficiently large quantum computer could undermine all presently deployed public key algorithms[6] . In future, quantum computing will inevitably break the encryptions as we know them today; it is just a matter of when that will happen. US Congress passed legislation in December 2022 mandating all agencies to start transitioning right now to new methods of cryptography that quantum computers can't break[7].

Advancements in encryption technology are crucial to protect against SNDL powered by quantum computers. Post-quantum cryptography is an area of research focusing on developing encryption algorithms resistant to quantum attacks. These new encryption algorithms aim to provide quantum-resistant security and ensure the confidentiality and integrity of sensitive data.

Lattice-based cryptography is one such promising approach. It utilises mathematical structures called lattices to create encryption schemes that are resistant to quantum attacks. Code-based cryptography is another technique that relies on error-correcting codes to secure communications. Both lattice-based and code-based cryptography offer potential solutions for protecting military encryption systems from SNDL coupled with quantum computers.

By adopting these improvements in encryption technology, military organizations can move away from the less secure RSA encryption to more robust post-quantum cryptographic methods. This shift could significantly bolster the protection of their critical data and communication channels.

### *Countermeasures and Mitigation Strategies*

In addition to advancements in encryption technology, implementing countermeasures and mitigation strategies is essential for protecting against SNDL attempts. Continuous monitoring may be required to prevent the theft of encrypted data. Vulnerability assessments play a critical role in identifying and patching susceptibility in military encryption systems, which could lead to encrypted data getting into the hands of the enemy. Regularly scanning for weaknesses and promptly addressing them helps maintain the system's integrity and prevents potential exploitation by adversaries.

Implementing multi-factor authentication (MFA) and access controls adds an extra layer of security to military communication systems. MFA requires users to provide multiple forms of identification before accessing sensitive information, making it more difficult for unauthorised individuals to gain access. Regular training and awareness programs are essential for safeguarding against SNDL attacks. Educating military personnel about the risks associated with leaking sensitive, albeit encrypted, information can substantially reduce the likelihood of security breaches due to human error.

## **The Importance of Collaboration and Preparedness**

Close collaboration between data security professionals and military personnel is crucial in addressing the evolving threat landscape posed by SNDL tactics. Data security professionals can leverage their expertise in encryption technologies and cyber defence by working together. At the same time, military personnel can provide valuable insights into the specific needs and requirements of military operations. Sharing knowledge and expertise between these two groups can lead to the development of effective countermeasures against SNDL attacks.

Regular communication and information sharing are essential for enhancing preparedness and response capabilities. By maintaining open lines of communication, data security professionals can stay informed about emerging threats and vulnerabilities specific to military encryption systems.

This enables them to proactively identify potential risks and develop mitigation strategies before adversaries exploit them.

### Investing in Research and Development

Continued investment in research and development is essential to stay ahead of emerging threats posed by SNDL attacks. Funding research on post-quantum cryptography and encryption technologies is crucial for developing robust solutions that can withstand quantum computing advancements.

Collaboration with academia and industry is also vital for accelerating innovation in military encryption. Military organisations can tap into a diverse pool of knowledge, resources, and expertise by partnering with experts from academic institutions, government agencies, and technology companies. This collaborative approach fosters the exchange of ideas, promotes interdisciplinary research, and leads to the development of cutting-edge encryption technologies resistant to quantum attacks.

Investing in research not only helps develop new encryption algorithms but also supports ongoing efforts to evaluate the effectiveness of existing cryptographic systems against emerging threats. Through rigorous testing, analysis, and evaluation, researchers can identify vulnerabilities in current encryption protocols used by the military. This knowledge informs the development of more robust defences against SNDL and quantum computers combo.

By prioritising collaboration between data security professionals and military personnel and investing in research and development initiatives, we can enhance our collective ability to protect military data and communications from SNDL attacks.

### Conclusion

In conclusion, SNDL tactics, in combination with quantum computers, pose a significant threat to military encryption. The emergence of quantum computing has raised concerns about the security of traditional encryption algorithms, such as RSA, which are vulnerable to quantum attacks. To protect against this threat, advancements in encryption technology, such as post-quantum cryptography, are necessary. Implementing countermeasures and mitigation strategies, such as continuous monitoring, multi-factor authentication, and regular training programs, can also help mitigate the risk. Collaboration between security professionals and military personnel is crucial for addressing the evolving threat landscape. Additionally, investing in post-quantum cryptography research is essential to avoid this imminent threat and ensure the security of military data and communications. By taking these measures, we can strengthen military encryption systems and safeguard sensitive information from the threat posed by SNDL and quantum computers combination.

***(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])***

## Notes:

[1] Ravi Sen, "Here's How Much Your Personal Information Is Worth to Cybercriminals – and What They Do with It," PBS NewsHour, May 14, 2021, https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it. Accessed on 15 Aug 2023.

[2] Simon Sharwood, "China May Steal Data Now, Decrypt Later with Quantum Tech," The Register, accessed May 17, 2023, https://www.theregister.com/2021/11/29/china_quantum_ai_offensive. Accessed on 17 Aug 2023.

[3] "Chinese Hackers Outnumber Our Cyber Staff Fifty to One: FBI Director Christopher Wray," *The Economic Times*, April 30, 2023, https://economictimes.indiatimes.com/tech/technology/chinese-hackers-outnumber-our-cyber-staff-fifty-to-one-fbi-director-christopher-wray/articleshow/99893077.cms. Accessed on 19 Aug 2023.

[4] RSA Laboratories, "The RSA Challenge Numbers," https://web.archive.org/web/20130921041734/http://www.emc.com/emc-plus/rsa-labs/historical/the-rsa-challenge-numbers.htm. Accessed on 28 May 2023.

[5] Thorsten Kleinjung et al., "Factorization of a 768-Bit RSA Modulus (Version 1.4)," *Lect. Notes Comput. Sci.* 6223 (2010): 20.

[6] "Are Tried and True Encryption Standards Going by the Wayside?," Rambus, https://www.rambus.com/blogs/are-tried-and-true-encryption-standards-going-by-the-wayside/. Accessed on 29 May 2023.

[7] Jen Sovada, "Congress Just Passed Critical Quantum Cybersecurity Legislation– Why It's Significant," SandboxAQ, December 21, 2022, https://www.sandboxaq.com/post/congress-just-passed-critical-quantum-cybersecurity-legislation-why-its-significant. Accessed on 21 Aug 2023.