The Promise and Peril of Quantum Computing and Its Implications for Cyber Insurance

Cameron R. Argetsinger*

Abstract: *Quantum computing, like artificial intelligence, is one of several emerging technologies that could either save the planet or end the world, depending on which expert is holding forth on the issue. Still mostly theoretical, quantum computing promises to turbocharge computer processing speeds, allowing future quantum computers to solve in a matter of milliseconds complex mathematical equations that would take conventional computers thousands or even millions of years to perform. It is too early to know whether the potential benefits of quantum computing will outweigh the potential risks, or how those risks may be mitigated by modern cyber insurance policies. This article explores the promise and peril of quantum computing and the potential coverage implications under cyber insurance policies.*

Quantum Computing on the Horizon

Since the dawn of the computer age to the present, all information that has ever been processed by computers can be reduced in simplest form to a series of "bits," binary packets represented as either a 1 or a 0.[1] Although processing speeds have increased exponentially in that time, the bit-based system imposes hard limits on the speed at which modern-day, "classical" computers can perform certain complicated calculations.[2] Quantum computers, while still largely theoretical, could change that. In quantum computing, the bit is replaced with the "quantum bit," or "qubit," which harnesses the seemingly mystical properties of quantum physics. Whereas a

Journal of Emerging Issues in Litigation / Winter 2024, Vol. 4, No. 1, pp. 65–73.

ISSN 2835-5040 (print) /ISSN 2835-5059 (online).

classical bit can be in only one state at a time, that is, 1 or 0 (on or off), a qubit can be in one of multiple states of 1 and 0 at the same time, through quantum principles of superposition and entanglement.[3] Once realized, this innovation will generate tremendous computing power, allowing a quantum computer to make many calculations at the same time, in contrast to a classical computer, which must perform each calculation separately. Quantum computers may be able to solve in seconds certain complex mathematical problems that would take classical computers trillions of years.[4]

The upside is huge. Applying quantum computers in fields like chemistry and materials science could allow for modeling and simulation of complex systems intractable to classical computers and result in startling breakthroughs.[5] Scientists could use quantum computers to predict complex chemical reactions to design longer-lasting batteries or sustainable plastic alternatives.[6] Quantum computing could allow researchers to simulate protein folding, a complex biological process that could result in innovations in medicine.[7]

But experts are equally concerned about the risks of quantum computing. All modern internet and digital security is founded on the integrity of cryptographic algorithms, a type of computer code that is based on complex mathematical problems that cannot be easily solved by classical computers. These algorithms are baked into the world's information infrastructure, protecting everything from financial information and medical data to email traffic and state secrets. The $2 trillion e-commerce industry is predicated on the un-solvability of these cryptographic algorithms.[8] Quantum computers, which soon may be able to calculate difficult mathematical equations in little or no time, could render these encryption technologies totally obsolete.[9] The risk that all the world's secret data suddenly could become available to anyone with a quantum computer threatens to overshadow the benefits of quantum computing, and has been referred to ominously as "Q-Day," or the "Encryptogeddon."[10]

When Q-Day arrives, potential effects could include widespread data breaches of sensitive health and financial personal data.[11] Private internet and messaging exchanges could be more susceptible to interception and decryption.[12] The integrity of digital documents

could be threatened as quantum computers are employed to forge digital signatures of authenticated documents.[13] Cryptocurrencies and blockchains, which rely on encryption technology, are likewise ripe for disruption by quantum applications.[14] Perhaps the biggest risk is that bad actors will harness quantum computers to exploit presently unforeseeable vulnerabilities.[15]

Fortunately, experts estimate that quantum computers capable of achieving Encryptogeddon, if they ever arrive, are still at least seven to ten years away.[16] But advances in quantum computing are coming at a rapid clip. In 2019, Google researchers announced that their quantum computer had performed a calculation in 3 minutes 20 seconds that would take a modern classical computer about 10,000 years.[17] IBM recently announced that it had used a quantum computer to perform a more practical application involving magnetic fields that could not be performed by any of the world's fastest non-quantum supercomputers.[18]

Indeed, criminal groups are already taking steps in anticipation of future quantum advances, by engaging in "steal now, decrypt later" (SNDL) attacks (also referred to as "harvest now, decrypt later," or "store now, decrypt later").[19] In these operations, cybercriminals hack and steal encrypted data that cannot be decoded using current technology, and then store it in anticipation of one day having access to a quantum computer capable of decrypting the data. Many types of financial and intellectual property data have a high enough value and a sufficiently long shelf life to warrant this type of attack. For example, an aerospace company could lose billions in future revenues if its proprietary designs are stolen.[20] Other types of intellectual property data, financial data, healthcare data, and other sensitive data could hold sufficient value to be relevant in ten years, if and when Q-Day arrives.[21] Significantly, the victim of an SDNL attack may have no idea that its data has been lost or stolen until years after the fact.

In response to Encryptogeddon scenarios, researchers at the National Institute of Standards and Technology (NIST) and elsewhere have begun to develop new "post-quantum cryptography" (PQC) techniques that will be resistant to quantum-based computing technologies.[22] But even if these new standards are effective, it will take years to transition the world's existing

quantum-susceptible hardware and software to PQC standards.[23] Much like the Y2K transition, governments and corporations will be in a race against time to identify and patch all potential security risks before quantum computers arrive.[24]

Cyber Insurance Coverage for Quantum Computing Risks

When and if the dangers of quantum computing materialize, cyber insurance may provide some coverage for the losses that ensue. Cyber insurance is a relatively new form of insurance coverage, compared to more traditional insurance products.[25] While the scope of coverage varies, cyber insurance policies generally are written to insure against liabilities and losses arising from a policyholder's online or electronic activities, such as selling on the internet or storing data on an internal network.[26]

Most cyber policies provide both first-party coverages (i.e., coverage for direct losses to the policyholder, as well as lost business revenue) and third-party coverages (i.e., coverage for the policyholder's liability to third parties). Key first-party coverages include:

- *Data/privacy breach response*: covers the costs a policyholder incurs in responding to a data or privacy breach, such as retaining privacy counsel, notifying customers whose data was wrongfully accessed, providing credit-monitoring services to those customers, and retaining forensic analysts to determine the scope and cause of the breach.
- *Extortion*: covers the cost of responding to a ransomware attack, including payment of ransom demands.
- *Business interruption*: covers the policyholder's revenue lost due to the necessary suspension of operations due to a data breach or network failure.
- *Dependent business interruption*: covers the policyholder's revenue lost due to the necessary suspension of operations due to a data breach or network failure affecting a third party on which the policyholder depends for its own operations.

Key third-party coverages include:

- *Data/privacy breach liability*: covers the policyholder's liability to third parties arising out of the loss or compromise of their data.
- *Media liability*: covers intellectual property infringement, other than patent infringement, resulting from the advertising of policyholder's services.
- *Regulatory liability*: covers regulatory fines and penalties for privacy violations, often including the cost of defending such regulatory proceedings.

In theory, cyber insurance should respond to many of the types of risks that are likely to come from quantum computing. If a cyber criminal were to use a quantum computer to decrypt and steal a policyholder's customer data, a conventional cyber insurance policy likely would cover the costs of responding to the breach, as well as the cost of defending claims any brought against the policyholder by disgruntled customers. If a quantum-driven cyberattack took down a policyholder's computer network, it is likely that lost revenue the policyholder sustained while its network was down would be covered by a cyber policy's business interruption coverage.

However, other significant hazards that could be spawned by quantum's decryption capabilities would not be covered by cyber insurance. Intellectual property theft, like the example above of the aerospace company losing its proprietary designs, is a major quantum computing threat, but one that would not be covered by any standard cyber insurance policy.

Another issue concerns SNDL attacks, where criminals are stealing data that cannot be decrypted using current technology in the hope of decrypting it years from now with the help of yet-to-be-developed quantum computers. Many cyber insurance policies contain a "prior acts" exclusion that bars coverage for data breaches or security events that occurred prior to a specified "retroactive date," which often is the same date as the policy's inception date or perhaps a few years prior. The exclusion applies regardless of whether the policyholder discovered the breach or event prior to the retroactive date, and regardless of whether it knew it had suffered any loss prior to the retroactive date. Experts believe that many SNDL attacks are

occurring without the victim's knowledge, and the harm will only come to fruition many years in the future when the harvested data can be decrypted. These attacks will not be covered by cyber policies that have retroactive dates falling after the dates of the initial data theft. Although it is possible to purchase cyber insurance with no retroactive limit, insurers may become increasingly reluctant to sell such coverage as SNDL exposures continue to grow.

Further, just as cyber threats evolve, so too do cyber insurance policies. Virtually all cyber policies are written on a one-year, "claims-made" basis, meaning that the policy only responds to claims that are "made" (or to events that occur) during that single policy year. Each year, the policyholder must purchase a new policy to cover future prospective threats that might unfold in the next policy period. Insurance companies continually revise their policy forms to respond to new conditions, and to limit their own exposures to new cyber threats.

One way that insurers have responded to growing cyber threats is by rewriting the policy language of their other, non-cyber, forms of insurance coverage in order to eliminate the possibility that those policies might also provide coverage for losses deemed to be cyber risks—so-called silent cyber.[27] Because of the potential that quantum computing may cause massive cyber losses across all industries, it is likely that insurers will take steps to curtail their own quantum exposures by rewriting current cyber policies to restrict coverage.

Another way that cyber insurers deal with increased risk of aggregate losses is by increasing premiums. In 2022, average cyber insurance premiums surged by 50 percent, driven by a spate of ransomware attacks, which resulted in large payouts under many cyber policies.[28] Because the Encryptogeddon envisioned by many experts would affect many policyholders all at once and dwarf even the largest ransomware events, cyber insurers undoubtedly will adjust rates skyward to reflect that risk.

Between policy revisions and price increases, certain cyber coverages could become unavailable or prohibitively expensive. For example, cyber insurers may become unwilling to underwrite contingent business interruption, which covers the policyholder for lost revenue when it suspends operations due to a breach or network failure that affects a third party on which the policyholder relies

for its operations. Quantum computing threats could make this coverage problematic for a number of reasons. First, many companies increasingly rely on a small number of web service providers, such as Amazon, Microsoft, or Google, for various cloud-based functions.[29] A quantum attack on one of these providers could potentially disrupt the businesses of countless other companies insured under cyber policies, creating the possibility of massive aggregate business interruption losses.[30] Second, contingent business interruption exposes insurers to the cyber security practices of third parties, which the insurer has little or no ability to police. As experts have warned, the mitigation of quantum risks will require virtually all private and public enterprises to undertake a costly and time-consuming transition to quantum-resistant PQC standards, which may take 10-15 years to accomplish. While a cyber insurer can confirm whether its policyholder has implemented the necessary changes, it cannot easily do so for all third parties on which the policyholder depends. As a result, insurance companies may back away from this coverage.

Conclusion

It is too early to know whether quantum computers will yield doomsday on earth or an earthly paradise or something in between. While cyber insurance may provide some coverage for hazards that result from quantum computing, those policies may not respond to many of the risks, and insurance companies will take care to minimize their own exposure to difficult-to-predict losses in this arena by revising policy language and increasing premiums. In the meantime, businesses should stay tuned to developments on this front, including by implementing PQR standards as they become available and keeping track of changes in the cyber insurance marketplace.

Notes

* Cameron Argetsinger (cargetsinger@andersonkill.com) is a Shareholder in the D.C. office of Anderson Kill. He focuses his practice on insurance recovery counseling and dispute resolution.

1. Filipe Beato, Anne Ardon, Itan Barmes, & Chris Knackstedt, *Transitioning to a Quantum-Secure Economy: White Paper*, World Economic Forum (2022), https://www3.weforum.org/docs/WEF_Transitioning %20to_a_Quantum_Secure_Economy_2022.pdf.

2. Deloitte, *Quantum Cyber Readiness: Deloitte's Perspective on Transitioning to a Quantum Secure Economy* (2022), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-deloitte-quantum-cyber-readiness-perspective-2022.pdf.

3. Zach Montague, *The Race to Save Our Secrets From the Computers of the Future*, New York Times (Oct. 22, 2023), https://www.nytimes.com/2023/10/22/us/politics/quantum-computing-encryption.html.

4. Kenneth Chang, *Quantum Computing Advance Begins New Era, IBM Says*, New York Times (June 14, 2023), https://www.nytimes.com/2023/06/14/science/ibm-quantum-computing.html.

5. Montague, *supra* note 3.

6. Karen Hao, *China Seeks a Quantum Leap in Computing*, Wall Street Journal (Oct. 6, 2022), https://www.wsj.com/articles/china-competing-us-quantum-computing-11664997892; *see also* Chang, *supra* note 4.

7. *Id.*

8. Editors, *Quantum Computers Will Break the Encryption That Protects the Internet*, Economist (Oct. 20, 2018), https://www.economist.com/science-and-technology/2018/10/20/quantum-computers-will-break-the-encryption-that-protects-the-internet.

9. Beato et al., *supra* note 1.

10. Montague, *supra* note 3; *see also* Beato et al., *supra* note 1.

11. *Id.*

12. Deloitte, *supra* note 2.

13. Beato et al., *supra* note 1.

14. Forbes Technology Council, *13 Risks That Come with the Growing Power of Quantum Computing*, Forbes (Nov. 8, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/11/08/13-risks-that-come-with-the-growing-power-of-quantum-computing/?sh=5d96e9ad54b8.

15. *Id.*

16. Jack Hidary, *Jack Hidary Says You Can't Afford to Ignore Quantum Computing*, Economist (Nov. 18, 2022), https://www.economist.com/the-world-ahead/2022/11/18/jack-hidary-says-you-cant-afford-to-ignore-quantum-computing. *See also* Montague, *supra* note 3.

17. Chang, *supra* note 4.

18. *Id.*

19. Hidary, *supra* note 16.

20. *Id.*

21. Leonard Kleinman, *The Quantum Effect on Cybersecurity*, Forbes (Feb. 9, 2023), https://www.forbes.com/sites/forbestechcouncil/2023/02/09/the-quantum-effect-on-cybersecurity/?sh=135098e4314e.

22. Montague, *supra* note 3.

23. Deloitte, *supra* note 2.

24. *Id.*

25. Kelly B. Castriotta, *A Semantic Framework for Analyzing "Silent Cyber,"* 27 Connecticut Insurance Law Journal 474, 479 (2021).

26. International Risk Management Institute, *Glossary*, "cyber and privacy insurance," https://www.irmi.com/term/insurance-definitions/cyber-and-privacy-insurance.

27. Castriotta, *supra* note 25 at 476-77.

28. Marnie Muñoz, *Cyber Insurance Premiums Surge by 50% as Ransomware Attacks Increase*, Insurance Journal (June 14, 2023), https://www.insurancejournal.com/news/national/2023/06/14/725215.htm.

29. Kenneth S. Abraham & Daniel Schwacz, *Courting Disaster: The Unappreciated Risk of a Cyber Insurance Catastrophe*, 27 Conn. Ins. L. Journal 407, 447 (2021).

30. *Id.*