Notre Dame Journal on Emerging Technologies

Volume 3
Issue 1 *Artificial Intelligence*

Article 2

2-2022

The "Prime Factors" of Quantum Cryptography Regulation

Lindsay Rand
University of Maryland School of Public Policy

Theodore Rand
University of New Hampshire Franklin Pierce School of Law

VOLUME 3 FEBRUARY 2022 ISSUE 1

JOURNAL ON EMERGING TECHNOLOGIES

ARTICLES

THE "PRIME FACTORS" OF QUANTUM CRYPTOGRAPHY REGULATION

Lindsay Rand & Theodore Rand***

* PhD student at the University of Maryland School of Public Policy.
** J.D. Graduate, University of New Hampshire Franklin Pierce School of Law, 2021.

THE "PRIME FACTORS" OF QUANTUM CRYPTOGRAPHY REGULATION

Lindsay Rand & Theodore Rand

Quantum computing exhibits promise to be a revolutionary technology. While the use cases may not replace all tasks performed by classical computers, certain areas of "quantum advantage," a concept theorized by researchers, will impact everyone, even if in more nuanced ways. As the pace of quantum research accelerates, analysis and regulation of these complicated impacts on society, and a realistic timeline for their application, have become necessary.

Likely due to a combination of the esoteric nature of quantum technology and the relatively nascent stage of development, political and legal governance mechanisms have been slow to keep up with innovation and application. However, this policy lag time is not new. Many recent tides of technological change have been met with phases of straggling governance. But in the case of quantum computing, how soon should the United States and the rest of the world begin thinking about the regulatory framework necessary for facilitating innovation and minimizing deleterious consequences? And where should this process begin?

This Article asserts cryptography to be a critical starting point, as it could be a task for limited scope quantum computers with severe consequences. This Article surveys the risks of quantum computers to encryption and the applicable policy and legal levers to address concerns. As this Article shows, lawmakers must reassess regulations for the exportation of cryptographic products for the quantum regime. For example, current export regulations focus on bit length–which quantum cryptography directly undermines. Further, current controls prevent dispersion of physical products, while a rapidly growing amount of classical and, particularly quantum, computing now takes place "on the cloud." Finally, in the context of protective governance, policies will need to be put in place to facilitate post-quantum encryption deployment to critical industries. Beyond the realm of cryptography, many of these recommendations will

also apply to other emerging application areas for quantum computing, or even to non-quantum emerging technologies.

INTRODUCTION

The exponentially accelerating "disruptive" innovation of emerging technologies appears to be outpacing the United States legal system and international legal and regulatory regimes.[1] As society begins to gain a firmer grasp of classical computing, incoherence in current regulations generates confounding side effects.[2] Specific examples of the inability of existing infrastructure to adapt to modern needs include outdated modes of strategic intent and lack of communication across interest groups. Policymakers and lawyers have also to an increasingly digital environment.[3] Adapting policy to minimize these side effects will become increasingly important as more powerful computing technologies, such as quantum computing, enter the market.[4]

As quantum computing rapidly gains traction after decades of scientific development, current approaches to digital technology standards face imminent challenges. In 2006, a company called D-Wave® received the first patent for a working quantum computing system.[5] Since then, quantum computing has steadily emerged at the forefront of emerging technologies. Specifically, quantum computing portends a new era of technological capabilities, by providing the capacity for faster calculations and higher computing complexity.[6] Some

---

[1] *See generally*, Mark Fenwick et al., *Regulation Tomorrow: What Happens When Technology is Faster than the Law?*, 6 AM. U. BUS. L. REV. 561 (2017) (discussing the increasing rapidity of innovation and specifically how we have moved past a "post-fact" era) [hereinafter *Regulation Tomorrow*]; *Ibid.* at n. 26 ("Moore's Law notoriously states that the 'functional capacity of ICT products roughly doubles every 18 months', [*sic*] with the same dynamics manifesting in biotechnology, and namely in sequencing human genome. As a result, regulating innovation involves what is called a 'pacing problem' in the academic literature from the US, or the 'challenge of regulatory connection' or 'regulatory disconnection' in European-based scholarship.").

[2] *See, e.g.*, Philip J. Weiser, *The Future of Internet Regulation*, 43 U.C. DAVIS L. REV. 529, 531 (2009) (discussing an instance in which the under-regulation of peer-to-peer (P2P) agreements led to several Maine and Canadian universities and other governmental entities losing the ability to connect over wireless internet).

[3] Lewis Lloyd, POLICY MAKING IN A DIGITAL WORLD: HOW DATA AND NEW TECHNOLOGIES CAN HELP GOVERNMENT MAKE BETTER POLICY 9 (2020) ("Despite attempts at reform, policy making is still suffering from age-old pitfalls, including poor record keeping, limited public input, slow feedback and minimal evaluation, resulting too often in policy failure . . .").

[4] The precise timing and magnitude of the quantum computing market has been a topic of much discussion among scientists, legislators, industry stakeholders, and investors. *See*, *e.g.*, John Preskill, *Quantum Computing in the NISQ Era and Beyond*, INSTITUTE FOR QUANTUM INFORMATION AND MATTER AND WALTER BURKE INSTITUTE FOR THEORETICAL PHYSICS (July 30, 2018).

[5] U.S. Patent No. 7,135,701 (filed Nov. 14, 2006).

[6] *See infra,* Part I.

of these new capabilities will pose immediate security threats.[7] While many of these innovations increase the stakes for regulation, similar technological advances capable of creating security threats make it paramount for the United States, and the rest of the world, to be proactive in addressing cybersecurity issues posed by quantum decryption techniques. Specifically, policymakers must answer questions revolving around the allowable degree of technology transfer across industries and abroad, allowable (and conversely illicit) end-use applications, and how critical legal guardrails should be enforced, both nationally and globally.

In the case of quantum computing, the impacts from ill-fitting regulations range from inefficient to deleterious. In the most benign cases, application of the existing legal and regulatory framework may be onerous or result in vague definitions that do not match understood terminologies used by the technology community.[8] However, lapses with more gravitas could have dire national security consequences.[9] Inability to develop regulation for post-quantum encryption could leave critical infrastructure or classified information exposed.[10] Overly strict export controls may force quantum talent to move abroad, resulting in significant economic losses. Moreover, existential threats to the viability of the American legal system may result from insurmountable technological debt, and corporate inertia to adapt business models to

---

[7] *See* Lindsay Rand et al., STRATEGIC TRADE RSCH. INST., EMERGING TECHNOLOGIES AND TRADE CONTROLS 49-50 (2020), https://strategictraderesearch.org/wp-content/uploads/2020/10/Emerging-Technologies-and-Trade-Controls-1.pdf (discussing the notion of quantum information processing as falling into the "implied category"—concerns that are "less concrete" but generally related to the potential for massive speed increases for certain computational operations) [hereinafter EMERGING TECHNOLOGIES].

[8] *See*, *e.g.*, Robert Eiss, *Confusion over Europe's Data-Protection Law is Stalling Scientific Progress*, NATURE: WORLD VIEW (Aug. 25, 2020), https://www.nature.com/articles/d41586-020-02454-7 ("Advocacy by the European scientific community ensured that the GDPR incorporated multiple exemptions for research. But there is still no clarity around how to implement them.").

[9] *See*, *e.g.*, KLON KITCHEN & BILL DREXEL, QUANTUM COMPUTING: A NATIONAL SECURITY PRIMER 2 (Apr. 2021), https://www.aei.org/research-products/report/quantum-computing-a-national-security-primer/ ("Conceivably, if a government built one such quantum computer before alternative encryption arrangements could be found by other governments (which may also require using quantum computers), the quantum-enabled government could access other nations' information systems in a catastrophic 'quantum surprise.'").

[10] *Id.*; *see also* Fred Guterl, *Are We Ready For a 'Quantum Surprise' From China*, NEWSWEEK: TECH & SCI. (Oct. 25, 2019), https://www.newsweek.com/china-quantum-computing-1467835 ("The nightmare scenario, from the standpoint of U.S. national security, is that China develops a working quantum computer without tipping its hand. That would leave China free to decrypt secure communications and gain access to reams of U.S. intelligence data.").

accommodate legitimate public interest concerns.[11] Meanwhile, the increasingly influential role of high-technology firms and other private sector members limits the amount of oversight that the government can provide in regulating technology development.[12]

The issues posed by quantum technologies are already on the government's radar.[13] One example of growing policymaker understanding is the enactment of the National Quantum Initiative Act in 2018.[14] Under the Act, the Director of the National Institute of Standards and Technology (NIST) "shall allocate up to $80,000,000 to carry out the activities under [the Act] for each of fiscal years 2019 through 2033."[15] Various governance funding and resource allocation mechanisms have supplemented these funds, including the establishment of new National Quantum Research Centers and the Quantum Economic Development Consortium.[16] Similar efforts by other national governments have paralleled such initiatives.[17]

But the landscape of quantum computing will be an incredible challenge for the government to take on.[18] Not only are national governments around the world engaging in a "space race"[19] of sorts to

---

[11] Keith Porcaro, *Failure Modes for Data Stewardship*, MOZ://A 6 (Aug. 2020), (exploring why individual data stewardships fail to take root: "they don't attract users; they lack the power to achieve their goals; they are legally or financially untenable; they are conflict-riven; and so on").

[12] Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and how to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

[13] Walter G. Johnson, Comment, *Governance Tools for the Second Quantum Revolution*, 59 JURIMETRICS J. 487, 489 (2019) ("Federal lawmakers developed interest in quantum technologies in 2017, with Rep. Will Hurd describing quantum computers as 'the next big security risk' and joining calls for a 'new Manhattan Project.'").

[14] National Quantum Initiative Act, Pub. L. No. 115-368, 132 Stat. 5092 (2018).

[15] National Quantum Initiative Act, 15 U.S.C.A. §§ 8831, 8842, 8852 (Westlaw through Pub. L. No. 116-29).

[16] *NIST Launches Consortium to Support Development of Quantum Industry*, NIST: NEWS (Sept. 28, 2018), https://www.nist.gov/news-events/news/2018/09/nist-launches-consortium-support-development-quantum-industry.

[17] *See, e.g., A Roadmap for Quantum Technologies in the UK*, UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME 7-8 (Sept. 2015), available at https://epsrc.ukri.org/newsevents/pubs/quantumtechroadmap/ (discussing the UK's announcement of a "5-year £270 million investment to establish the UK National Quantum Technologies Programme – championed by the Quantum Technologies Strategic Advisory Board (QT SAB).").

[18] Lindsay Rand & Berit Goodge, *Information Overload: The Promise and Risk of Quantum Computing*, THE BULLETIN (Nov. 14, 2019), https://thebulletin.org/2019/11/information-overload-the-promise-and-risk-of-quantum-computing/ [https://perma.cc/8MD6-EZCA].

[19] *See generally*, Zeeya Merali, *Data Teleportation: The Quantum Space Race*, 492 NATURE 22 (2012).

achieve "quantum supremacy,"[20] but there has also been a monumental shift in the U.S. governments' role as an innovator.[21] And, despite the relatively "far-off" (i.e., five to ten years) timeframe for early quantum technologies, many view the government's current commitment to the technology as insufficient.[22] For instance, the United States' commitment to invest $1.1 billion in quantum computing pales in comparison to China's investment of more than $10 billion into its own research facility.[23]

But funding is not the only concern to a healthy and prosperous future for quantum computing. In fact, government funding may soon be dwarfed by private sector investment as potentially lucrative applications begin to emerge.[24] The government must create a regulatory environment that facilitates early innovation while providing the foundation for a more robust framework to develop as the technology becomes more sophisticated. The government must also find an appropriate balance between national security and international harmonization. Finally, and maybe most important, the government must do better with quantum than with traditional computing to understand what eccentricities may result from the diverging interests

---

[20] This concept has also been referred to as "quantum advantage." *See* Preskill, *supra* note 4, at 7. Roger Huang, *Here's Why Quantum Computing Will Not Break Cryptocurrencies*, FORBES (Dec. 21, 2020), https://www.forbes.com/sites/rogerhuang/2020/12/21/heres-why-quantum-computing-will-not-break-cryptocurrencies/?sh=523bccee167b ("When people talk about 'quantum supremacy", including reports from Google and/or China, they really mean that a quantum computer can do a certain task better than classical computers, perhaps one that is impossible to do in any reasonable timeframe with classical computers.").

[21] *See*, *e.g.*, James Vincent, *US Announces $1 Billion Research Push for AI and Quantum Computing*, THE VERGE (Aug. 26, 2020), https://www.theverge.com/2020/8/26/21402274/white-house-ai-quantum-computing-research-hubs-investment-1-billion ("Many policy advisors have worried that America is falling behind in AI and quantum research compared to rivals like China, and warn that these technologies are instrumental not only for economic development but also national security.").

[22] NAT'L SEC. COMM'N ON ARTIFICIAL INTEL., FINAL REPORT 256 (2021), https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf (noting that the United States must do more to keep up with China because of, among other things, the importance of "first-mover" advantage).

[23] COMM. ON TECH. ASSESSMENT OF THE FEASIBILITY & IMPLICATIONS OF QUANTUM COMPUTING, NAT'L ACAD. SCIS., ENG'G, & MED., QUANTUM COMPUTING: PROGRESS AND PROSPECTS 181 (Emily Grumbling & Mark Horowitz eds., 2019) [*hereinafter* QUANTUM COMPUTING: PROGRESS AND PROSPECTS].

[24] Elizabeth Gibney, *Quantum Gold Rush: The Private Funding Pouring into Quantum-Startups*, NATURE (Oct. 2, 2019) ("[I]n 2017 and 2018, companies received at least $450 million in private funding—more than four times the $104 million disclosed over the previous two years.").

between the public and private sector.[25] Only by understanding the intrinsic value of the technology can the government look to the future independently of industry projections to see the blind spots that may develop in our national approach.

This Article will discuss one subsection of the quantum computing landscape—post-quantum cryptography.[26] While there are many more considerations possible to extend the scope to other applications,[27] the goal of this Article is to determine what can be extrapolated from the regulation of digital computing, as well as current policies set out for quantum computing, to best facilitate innovation in quantum cryptography. While the government may no longer need to play a primary role in cutting-edge innovation as it did during the space race and other massive scientific endeavors, it needs to be a more cunning consumer of technology if it wants to let industry take the reins. In that sense, this Article examines the government's approach to regulating digital technology by focusing on its lack of independent scientific awareness in working with industry to develop effective regulation.

I. TECHNOLOGICAL BACKGROUND

While the hard science behind quantum computing may seem impenetrable, some discussion of the scientific context and state-of-the-art industry technology will help to better understand the policy and regulatory considerations. This section will outline the physical basis of quantum computing, identifying the characteristics that distinguish quantum systems from non-quantum counterparts. This section will then survey recent developments in the quantum computing field, and the evolving quantum landscape. Finally, this section will conclude with projected outlooks for quantum computer developments.

A. Quantum Computing

---

[25] Scott Buchholz et al., *The Realist's Guide to Quantum Technology and National Security*, DELOITTE (Feb. 6, 2020), https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html ("With a basic understanding of the science and the technology can leaders begin to identify the areas in which their organization could benefit from or be vulnerable to different quantum technologies.").

[26] Daniel J. Bernstein, Johannes Buchmann, & Erik Dahmen, POST-QUANTUM CRYPTOGRAPHY 7 (Springer-Verlag Berlin Heidelberg ed., 2009).

[27] Johnson, *supra* note 13, at 8 (showing a chart mapping out several dual-use applications for quantum technologies).

> *[N]ature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy*.[28]

1. Quantum Mechanics: The Foundation of Quantum Computing

Quantum mechanics is a fundamental physics theory for describing atomic and subatomic particles' interactions. Like other physics theories (*e.g.*, relativity), quantum mechanics came about as a way of describing observations that were not compatible with classical physics. A cornerstone of quantum mechanical theory is that, at a small enough scale, the position and momentum for an object is probabilistic rather than deterministic.[29] Subatomic particles are often used as examples, with their orbital positions or energetic states described as wave functions. The wave provides an amplitude of probabilities for a given observation.[30] Over the years, research has proven that other characteristics of certain particles may also exhibit quantum mechanical properties, such as angular momentum.[31] Beyond describing the state of individual particles, quantum mechanics can also explain the interaction of *groups* of quantum particles.[32] Quantum mechanics fundamentally describes the states of individual particles as superpositions of all possible states, but it also does this at the ensemble level for systems with

---

[28] Richard P. Feynman, *Simulating Physics with Computers*, 21 INT'L J. THEORETICAL PHYSICS 467, 486 (1982) (arguing for the utility of quantum computers).

[29] It is important to note that there is still a live debate within the academic community as to whether quantum mechanics is objectively probabilistic or if that characteristic of quantum mechanics is based on our flawed understanding or measurement techniques. *See*, *e.g.*, Lev Vaidman, *Quantum Theory and Determinism*, 1 QUANTUM STUD.: MATHEMATICS & FOUNDS. 5 (2014), https://doi.org/10.1007/s40509-014-0008-4.

[30] Lisa Zyga, *Does the quantum wave function represent reality?*, PHYS.ORG: QUANTUM PHYSICS (Apr. 25, 2012), https://phys.org/news/2012-04-quantum-function-reality.html ("[T]here are two prominent interpretations of the wave function dating back to its origins in the 1920s. In one view, the wave function corresponds to an element of reality that objectively exists whether or not an observer is measuring it. In an alternative view, the wave function does not represent reality but instead represents an observer's subjective state of knowledge about some underlying reality.").

[31] B. Zwiebach, Quantum Physics II, Lecture Notes 9: Angular Momentum 4 (Dec. 16, 2013), https://ocw.mit.edu/courses/physics/8-05-quantum-physics-ii-fall-2013/lecture-notes/MIT8_05F13_Chap_09.pdf ("The classical angular momentum operator is orthogonal to both lr and lp as it is built from the cross product of these two vectors. Happily, these properties also hold for the quantum angular momentum.").

[32] Brian S. Haney, *Quantum Patents,* 27 B.U. J. SCI. & TECH. L. 64, 72-73 (2020) (describing the ability to control qubit groups by utilizing their couplers: "links between qubits, called couplers, allow for the resulting states of multiple qubits to affect one another").

multiple quantum particles.[33] Finally, quantum mechanics asserts that some quantum objects have correlated properties, or are entangled, as a result of certain processes.[34]

Following its inception at the turn of the twentieth century, this probabilistic (i.e., non-deterministic) description of the universe was subject to significant scientific critique.[35] In 1935, three scientists (including Albert Einstein) wrote a now-famous critique of quantum mechanics.[36] It found quantum's lack of deterministic results and real-world describability fatally flawed.[37] In what is now referred to as "EPR," **E**instein, **P**odolsky, and **R**osen argued that the lack of certainty associated with quantum-mechanical measurements made the theory an incomplete system for describing real-world physics.[38] Ironically, this conclusion has become one of the field's fundamental tenets (and core motivations).[39]

However, modern-day scientists and engineers have embraced the distinct characteristics of quantum objects. In what is referred to as the Second Quantum Revolution, quantum mechanical properties are being used to develop new branches of quantum technologies.[40] Describing matter and its associated physics as a wave function allows for a more accurate description of microscopic matter and is particularly useful for

---

[33] *Id.*

[34] Eugenie Samuel Reich, *Quantum Computers Moves a Step Closer*, 467 NATURE 513 (2010) (describing how superposition and entanglement enable "calculations [that] can run in parallel—in principle allowing a quantum computer to race through problems that it would take a classical computer eons to solve.").

[35] One such source of criticism is included in the paragraph below, but there are many other helpful sources on the subject that are capable of being understood by non-physicists. *See, e.g.,* ROGER COLBECK & RENATO RENNER, INST. OF THEORETICAL PHYSICS, THE COMPLETENESS OF QUANTUM THEORY FOR PREDICTING MEASUREMENT OUTCOMES (July 11, 2013), https://arxiv.org/pdf/1208.4123.pdf.

[36] Albert Einstein et al., *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, 47 PHYSICAL REV. 777 (1935).

[37] *Id.* at 778-80.

[38] *Id.* at 780 ("Previously we proved that either (1) the quantum-mechanical descriptions of reality given by the wave function is not complete or (2) when the operators corresponding to two physical quantities do not commute the two quantities cannot have the same reality. Starting then with the assumption that the wave function does not give a complete description of the physical reality, we arrived at the conclusion that the two physical quantities, with non-commuting operators, can have simultaneous reality."). This proof has been rebutted by numerous hypotheses. *See, e.g.,* Arthur Fine, *Bohr's Response to EPR: Criticism and Defense*, IYYUN: THE JERUSALEM PHIL. Q. 31, 31 (2007).

[39] Andrew Zimmerman Jones, *EPR Paradox in Physics*, THOUGHTCO. (July 3, 2019), https://www.thoughtco.com/epr-paradox-in-physics-2699186 ("The EPR paradox (or the Einstein-Podolsky-Rosen Paradox) is a thought experiment intended to demonstrate an inherent paradox in the early formulations of quantum theory. It is among the best-known examples of quantum entanglement.").

[40] Johnson, *supra* note 13, at 487-88.

determining atom behavior. Further, particles, from this perspective, can be in more than one state simultaneously (or at least have the probability of being in more than one state simultaneously).[41] In quantum computing, this characteristic enables particles, referred to as qubits, to represent more than one unit of measurement at once; in comparison, classical computer bits must either be "1s" or "0s".[42] Theoretically, this means that qubits can perform multiple classical computations "in parallel" (comparable to multiple computers running the same operation and sharing their results, e.g., threading) on the same unit of storage.[43]

However, unfortunately for non-technical audiences, the key advantages of quantum systems are not always clear. Many papers and other academic resources that discuss quantum computing jump to the discussion of quantum entanglement–providing "weird" and "spooky" descriptions of particles communicating with each other over vast distances. Some even refer to it as a kind of "teleportation."[44] While this phenomenon creates an interesting visualization for a reader, it may not the most helpful way to think about "quantum advantage" (as the notion is presently understood).[45] Rather, consider the task of running the same

---

[41] While the wave-particle duality of quantum mechanics is somewhat beyond the scope of this article, the concept of quantum superposition provides that until a particle is observed, it is probabilistically capable of being in more than one state at any given moment in time. Richard Feynmann, *Space-Time Approach to Non-Relativistic Quantum Mechanics*, 20 REVS. MOD. PHYS. 367, 368 (superposition describes an instance where a sub-atomic particle occupies two independent positions simultaneously).

[42] *Id.* at 494.

[43] To readers with technical backgrounds, the concept can be visualized as a form of "threading." *See* Lindsay Rand, *Approaching Y2Q and Barely a Peep (or Tweet) from The Government*, THE BULLETIN (Feb. 27, 2019), https://thebulletin.org/2019/02/approaching-y2q-and-barely-a-peep-or-tweet-from-the-government/ [https://perma.cc/L4VL-AEJ7] ("For example, a two-bit system can be in one of four states (00, 01, 10, or 11. In comparison, a two-qubit system can be in all four states at the same time."); *see also,* David Deutsch, *Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer*, 400 PROC. ROYAL SOC'Y LONDON. SERIES A MATHEMATICAL & PHYSICAL SCIS. 97, 110-111 (July 8, 1984), https://doi.org/10.1098/rspa.1985.0070 (describing "quantum parallelism": "a method by which certain probabilistic tasks can be performed faster by a universal quantum computer than by any classical restriction of it.").

[44] *See generally*, Kelly McSweeney, *Quantum Entanglement and Teleportation is Sci-Fi Technology in Real Life*, NORTHRUP GRUMMAN: NOW. (Aug. 14, 2020), https://now.northropgrumman.com/quantum-teleportation-is-sci-fi-technology-in-real-life/. Readers should appreciate that whether teleportation can actually be accomplished by quantum entanglement depends on their interpretation of teleportation (a word rooted in science fiction).

[45] However, some modern quantum computing techniques, including certain types of ion traps, do hypothesize utilization of such entanglement principles to share data between two interconnected qubit systems. *See, e.g.,* U.S. Patent No. 11,195,117, at col.

computation on a regular computer, trillions of times, setting different values each time to determine which values made the computation "work." Now, think about the quantum mechanical property that allows a single qubit to be in multiple states, *at once*. In a single computation, a quantum computer could try virtually an infinite set of values in the computation *at once* (i.e., in "real-time"). Thus, several of the main advantages of quantum computers are the speeds at which they can operate, and the increase in dimensional complexity they are able to analyze. This means that quantum computers may be able to solve traditional problems faster than other computers and may be able to solve more complex problems than traditional computers.

Given these benefits predicted by theoreticians, scientists have long been developing the framework for operable quantum computers,[46] with the first mechanical model of one being described in 1980.[47] For the first couple of decades, quantum computing was primarily only a theoretical endeavor. However, with the emergence of modern experimental capabilities such as high-powered lasers,[48] and ultra-cold refrigeration techniques, experimental quantum computing has grown into a robust field. As practical research on quantum computing has evolved, critical limitations of theoretical predictions and prospects have been circumscribed.

Surprisingly or not, a vast majority of computational tasks performed on traditional computers do not work like that and thus do not require such a large computational advantage. For instance, when a user selects a song to play on Spotify®, the smartphone does not attempt to find a value by performing trillions of computations. It just picks the song and plays the audio track stored in cloud memory. Based on our present understanding of quantum computing algorithms, there would be no "quantum advantage" in selecting, recording, or playing such a song on a quantum computer.

4, ll. 42-45 ("There have been successful demonstrations of controlled entanglement of several-ion quantum registers in the past decade involving the use of qubit state-dependent forces supplied by laser beams.").

[46] Haney, *supra* note 32, at 68 ("A quantum computer is a physical system harnessing quantum effects to perform computation.").

[47] *See generally* Paul Benioff, *The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines*, 22 J. STAT. PHYSICS 563, 563 (1980), https://doi.org/10.1007/BF01011339.

[48] From more complex tasks like multi-system communications, to the more fundamental task of measuring qubit states, lasers are necessary for a vast majority of quantum setups. *See* Stephan Ritter & Jürgen Stuhler, *Lasers Shape the World of Quantum Technologies*, LASER FOCUS WORLD (July 14, 2020), https://www.laserfocusworld.com/lasers-sources/article/14177600/lasers-shape-the-world-of-quantum-technologies.

And even for calculations where quantum mechanics could be helpful, there are structural limitations based on the resultant math of quantum superposition (linear algebra) that diminish the factor of quantum advantage (based on currently-known algorithms).[49] There are also many serious (albeit predominantly engineering, rather than scientific) problems inherent in controlling a runtime environment of qubits to maintain the same state throughout a computation.[50] But to understand the motivation, a good foundation for the purposes of this Article is to grasp the speed capabilities of a system capable of being, and necessarily in, more than one state at one time.

There is also uncertainty over the best platform design[51] for quantum computing. There are several ways of implementing quantum computing (i.e., isolating and measuring qubits in a system). While there are several prevailing methods, for example, superconducting qubit systems,[52] that are popular in the industry today, many believe there is no clearly superior hardware implementation at this time.[53] Modern quantum computers (sometimes referred to as Noisy Intermediate-Scale Quantum (NISQ) computers) can only control a few dozen qubits at a time.[54] The parallelization of such a small number of computational bits, while academically interesting, would not be sufficient to achieve

---

[49] *See QC Ware,* Q2B | Prospects for Error Corrected Quantum Applications | Ryan Babbush | Google, YOUTUBE (Feb. 9, 2021), https://www.youtube.com/watch?v=_lyagy7_ty0 (discussing the value of quality algorithms).

[50] *See, e.g.*, Rob Matheson, *Uncovering the Hidden "Noise" that Can Kill Qubits*, MIT NEWS (Sept. 16, 2019), https://news.mit.edu/2019/non-gaussian-noise-detect-qubits-0916 ("[A] qubit's quantum "coherence" —meaning its ability to maintain the superposition state—can fall apart due to noise coming from environment around the qubit. Noise can arise from control electronics, heat, or impurities in the qubit material itself, and can also cause serious computing errors that may be difficult to correct.").

[51] Platform design in this context refers to the combination of the hardware and the software that comprise the user experience. For a variety of tools that can be used to design a quantum computing platform, *see Tools,* QUANTUM COMPUTING REP., https://quantumcomputingreport.com/tools/ (last visited June 28, 2021).

[52] *See, e.g.*, Jonathan Hui, *QC - How to Build a Quantum Computer with Superconducting Circuit?*, MEDIUM (Jan. 6, 2019), https://jonathan-hui.medium.com/qc-how-to-build-a-quantum-computer-with-superconducting-circuit-4c30b1b296cd ("In quantum computers, many university research groups bet on trapped ions. But the industrial giants do not necessarily agree with that. Indeed, the superconducting circuit seems to be their top choice.").

[53] *See* Elizabeth Gibney, *Quantum Computer Race Intensifies as Alternative Technology Gains Steam*, NATURE: NEWS (Nov. 17, 2020), https://www.nature.com/articles/d41586-020-03237-w.

[54] Martin Giles, *IBM's New 53-Qubit Quantum Computer Is the Most Powerful Machine You Can Use*, MIT TECH. REV.: COMPUTING (Sept. 18, 2020), https://www.technologyreview.com/2019/09/18/132956/ibms-new-53-qubit-quantum-computer-is-the-most-powerful-machine-you-can-use/.

meaningful quantum advantage for most computing operations.[55] But even a modest amount of scaling of such a system quickly leads to startling computational capacity that could have real-world implications.[56]

2. The Industry Landscape

Despite the many identified hurdles to practical quantum computers and the large variety in approaches to creating a quantum computer, there is hope in the sheer size of the growing quantum industry. As mentioned previously, the industry has increasingly taken center-stage in the development of innovative technology. Quantum computing is no different. In the past few years, typical industry heavyweights such as Google, IBM, Honeywell as well as small to midsize technology companies have significantly increased their spending on quantum innovation to battle for "quantum supremacy" or "quantum advantage."[57] But the race, however, for quantum advantage is defined by a greater opacity than many in previous private-sector races to innovate. This is likely due to the immense diversity in proposed quantum computing applications. For example, unlike 5G wireless technology, there is no single, clearly defined market for quantum innovation.[58] Rather, the varied and diverse application areas for quantum computers make it hard to define significant technology milestones, as the technology requirements vary for each application.

Further, this range in predicted quantum computer application has led to diverse, cross-sector interest. Actors across academia, government, and industry are investing resources into quantum computing. Among these actors, identified application interests include:

---

[55] *But see* Frank Arute, Kunal Arya, & Ryan Babbush, *Quantum Supremacy Using a Programmable Superconducting Processor*, 574 NATURE 505 (2019), https://doi.org/10.1038/s41586-019-1666-5. In this article, a Google research team discusses experimental results and a corresponding methodology justifying Google's claim of quantum supremacy.

[56] *See* Rand, *supra* note 42. ("[Q]uantum computers would be able to crack the most common encryption methods, as well as create other disruptions, because, in theory, they operate at much higher speeds than today's computers.").

[57] Robert Hackett, *Quantum Computing is Entering a New Dimension*, FORTUNE (Dec. 3, 2020, 8:00 AM), https://fortune.com/2020/12/03/quantum-computing-supremacy-google-ibm-honeywell-microsoft-alibaba/.

[58] Evan R. MacQuarrie, Christoph Simon, Stephanie Simmons, & Elicia Maine, *The Emerging Commercial Landscape of Quantum Computing*, 2 NATURE REVS. PHYSICS 596, 596 (2020), https://doi.org/10.1038/s42254-020-00247-5 ("Despite scientific advances and a wave of investment, the emerging quantum computing (QC) commercial market still faces a high level of both technological and market uncertainty.").

basic research, defense, finance, academia, medicine, etc.[59] Within each entity, there is also significant foundational variation; there is a mix of public and private industries and an extensive range in company ages. Many companies have been founded within the last five years, but longer-standing, larger defense contractors and computer companies are also developing new branches for quantum technologies.[60]

One remaining question in the race to quantum advantage is how much room is at the top, and thus how long can such a robust investment environment be maintained. After all, it appears as if an early customer of quantum products will be the government, which has previously shown a tendency to consolidate its expenditures on innovation fairly quickly.[61] Many have described the possibility of a winner-take-all scenario.[62] There is significant uncertainty as to how this relates to the various types of qubits that have been researched, and the extent to which different quantum computing platforms may produce their own unique markets. Even the extent to which this possibility is perceived by sector members may result in hesitancy to remain in the market too long without significant improvement. Given that quantum computers are likely to be technologies with long innovation timelines, failure to sustain interest from sector members could result in the stunting of technology development.

While quantum mechanics has yielded useful applications in terms of highly accurate simulations in the development of micro-devices—such as transistors and lasers, and medical research and imaging—the development of the quantum computer has been steady and largely nascent since about the 1980s.[63] In 1994, Peter Shor wrote a paper showing how the common practice of prime-factoring encryption could be reversed almost simultaneously by quantum computers.[64]

---

[59] *See* EMERGING TECHNOLOGIES, *supra* note 7 at 65.
[60] *Id.* at 59-61.
[61] Johnson, *supra* note 13, at 507 ("Quantum technologies arise from an atypical industry in which development pressures and funding arise in large part from national security applications, yet various commercial and civilian uses will follow closely behind. Early, practical quantum computing, communication, and metrology devices will be concentrated in the possession of government actors and large firms.").
[62] Ctr. for Strategic & Int'l Studies, *Cybersecurity in the Quantum Future*, YOUTUBE (June 15, 2021), https://youtu.be/vMZ6DmaBw40 (starting at 40:07: Josyula "J.R." Rao discussing how industry should approach the prospect of quantum computing) [*hereinafter* CSIS Video].
[63] *See generally* Richard P. Feynman, *Simulating Physics with Computers*, 21 INT'L J. THEORETICAL PHYSICS 467 (1982).
[64] *E.g.*, Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, 26 SIAM J. COMPUTING 1484–1507 (1997) (updating the earlier symposium paper presented in 1994).

Shor's work provided, among other contributions, an acute motivation for the development of quantum computers.

B. Quantum Cryptography

Perhaps one of the greatest motivators for industry engagement at present is concern over "quantum decryption" and related "post-quantum encryption." Any research into quantum computing will likely result in stumbling upon the main buzzword technologies in the purview of many scientists and government security departments: quantum decryption and post-quantum encryption. Specifically, quantum decryption refers to the predicted capability of quantum computers to decrypt prime-factorization encryption techniques that have become the most popular standard in industry.[65] And while there are many other potential use-cases for quantum computing, decryption is one that the government and private industry has been keeping a watchful eye on. After all, "[c]ryptographic technologies are used throughout government and industry to authenticate the source and protect the confidentiality and integrity of information."[66] Thus, post-quantum encryption, which refers to capabilities to encrypt information robust to quantum computing power, has also become a key interest.

1. Quantum Decryption

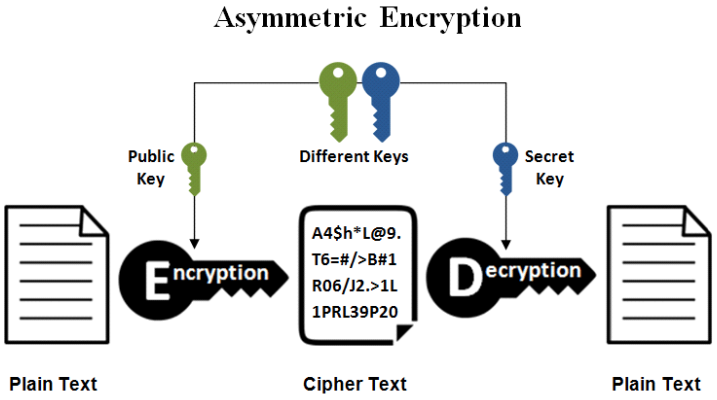
While further specifics of key encryption, and current regulation, are discussed in Part II, an essential aspect of the quantum computing landscape as it relates to decryption is the idea of integer factorization. Specifically, one and maybe the most popular forms of encryption, RSA encryption, is based on "prime factorization," a way of expressing numbers as a product of prime factors. A prime factor is a number that is only divisible (without producing a non-integer remainder) by itself and the number one. By encrypting numbers using prime factorization of a certain upper bound of computer bits, the time it would take for a classical computer to reverse the encryption would take a significant amount of time that is effectively treated as infinite for the purpose of

---

[65] Sunny Beatteay, *How Prime Numbers Keep the Internet Secure*, BETTERPROGRAMMING (Sept. 7, 2020), https://betterprogramming.pub/how-prime-numbers-keep-the-internet-secure-680cc1743133.

[66] William Barker, William Polk, & Murugiah Souppaya, *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*, (Apr. 28, 2021).

cryptography.[67] Further, encryption certificates allow for the communication of encrypted messages between trusted sources without sending secret passwords back and forth between the two parties.[68]



However, this thesis only holds true if we consider resource constraints (i.e., space, time, materials), coupled with the idea that a computer can only try one combination of values at a time. If, though, we consider a single computer that can try multiple combinations in a single execution, that computer can rapidly outpace a seemingly infinite number of classical computers with a relatively low number of memory storage units ("bits").[69] If a form of encryption is based on the principle that a computer can only try one combination of numbers at a time, the computer capable of trying multiple combinations at a time would pose an imminent threat to any data protected by such an encryption technique.

This concept is not new. Cryptographic algorithms are often "exposed" as having a weakness that makes replacement or modification necessary.[70] However, the threats posed by quantum computing are unique in that they defeat the goal of such an approach as prime

---

[67] Andreas Baumhof, *Breaking RSA Encryption – an Update on the State-of-the-Art*, QUINTESSENCE LABS (June 13, 2019), https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art/ ("It would take a classical computer around 300 trillion years to break a RSA-2048 bit encryption key.").

[68] This process is known as asymmetric encryption and is discussed in more detail in Part III. Asymmetric encryption. Gamze Maden et al., *Comparison of Symmetric and Asymmetric Cryptography Algorithms and a Better Solution: Hybrid Algorithm,* 2018 INT'L CONG. OF SCI. EDUC. AND TECH. 19, 21, https://perma.cc/5BP5-9W64.

[69] This concept is referred to as "Shor's algorithm," named after Peter Shor. *See* Shor, *supra* note 62 at 1484-1507.

[70] Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 429-30 (2012) ("[A]ll forms of encryption are subject to three basic categories of attack; 1) brute force attacks; 2) attacks that are more efficient than brute force; and 3) attacks assisted by a flaw known to the attacker, or "backdoors.").

factorization "head-on," in that a simple "patch" to replace a formulaic randomization will not suffice to defeat the decryptor. Rather, a whole new system is required to secure information from new quantum technology developments. Here, the distinct computational power quantum advantage referenced in the previous sections becomes a significant driver of disruption.

2. Post-Quantum Encryption

Despite the challenges posed by quantum decryption, researchers have developed several viable candidates to replace current encryption standards that would be "quantum-safe."[71] As quantum computing threatens to disrupt existing encryption standards, new methods for securing data have evolved. These methods, referred to as post-quantum encryption, have been under development by a narrow range of private sector actors and NIST.[72] The goal for post-quantum encryption is to develop problem designs that could challenge even quantum computers. Internationally, the European Telecommunication Standards Institute (ETSI) has created a "working group" for developing post-quantum encryption standards.[73]

While NIST has not promulgated official standards for post-quantum encryption, they are planning to release final standards by 2024.[74] Part of the difficulty inherent in developing quantum-safe encryption is the lack of access to quantum computing to sufficiently test proposed algorithms and their implementation on classical machines. However, several potential standards have emerged, in part because of a contest hosted by NIST to find the most effective post-quantum encryption techniques.[75] Competitions have yielded successful results in

---

[71] Lidong Chen, *Cryptography Standards in Quantum Time: New Wine in an Old Wineskin*, IEEE SEC. & PRIV. (2017).

[72] Dustin Moody, *The Future is Now: Spreading the Word about Post-Quantum Cryptography*, NIST: TAKING MEASURE, (Dec. 2, 2020), https://www.nist.gov/blogs/taking-measure/future-now-spreading-word-about-post-quantum-cryptography.

[73] *Quantum-Safe Encryption (QSC)*, ETSI (last visited Nov. 9, 2021), ("The ETSI Cyber Quantum Safe Cryptography (QSC) Working Group aims to assess and make recommendations for quantum-safe cryptographic primitives protocols and implementation considerations, taking into consideration both the current state of academic cryptography research and quantum algorithm research, as well as industrial requirements for real-world deployment.").

[74] Moody, *supra* note 70.

[75] *Id.* (discussing the "PQC competition": "We are now several years into the competition and hope to select the new quantum-safe algorithms that NIST will standardize in another year or two.").

other areas like the Advanced Encryption Standard (AES) and the third version of the Secure Hashing Algorithim (SHA-3).[76] However, the issue of whether patents should protect such encryption techniques has already become a sticking point for some companies remaining in the final stages of the competition.[77]

NIST will need to continue engaging in significant interactions with stakeholders once suitable technologies have been selected. Upon NIST's identification of a post-quantum encryption standard, the government will need to coordinate with the agency and relevant industry stakeholders to not only define an implementation timeline, but also to sort out issues related to, among other constraints, intellectual property.[78] Furthermore, many stakeholders will want to test how post-quantum encryption technology shifts impact their systems. A key question is whether post-quantum encryption will require significant hardware changes, and the extent to which hardware or software changes may impose new security vulnerabilities.

3. Projected Timeline to Disruption

Thus, because of the long-projected timeline to the deployment of post-quantum encryption, there are significant concerns regarding the timeline to quantum decryption disruption. Various reports have postulated short and long timescales until (Quantum Information Science) QIS technology application will become practical, including quantum decryption. In a 2020 survey conducted by RAND Corporation of several industry experts, the average year guessed as the advent of

---

[76] Joseph Lorenzo Hall, *What the Heck is Going on with NIST's Cryptographic Standard, SHA-3?*, CTR. FOR DEMOCRACY & TECH. (Sept. 24, 2013), https://cdt.org/insights/what-the-heck-is-going-on-with-nist%E2%80%99s-cryptographic-standard-sha-3/.

[77] NIST's stance on patent protection of subject encryption technologies has been developing throughout the competition, and it is currently a primary consideration in the adoption of a post-quantum encryption standard. *See* NIST, SUBMISSION REQUIREMENTS AND EVALUATION CRITERIA FOR THE POST-QUANTUM STANDARDIZATION PROCESS 9 (Dec. 2016), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf ("NIST does not object in principle to algorithms or implementations which may require the use of a patent claim, where technical reasons justify this approach, but will consider any factors which could hinder adoption in the evaluation process.") [hereinafter PQS SUBMISSION REQUIREMENTS].

[78] *See* Moody, *supra* note 70 ("NIST publishes cryptography standards so that government agencies know how to safely use crypto. These standards are documents that specify exactly how to implement various cryptographic algorithms in a standard way, so that a user's computer will be able to securely communicate with the intended recipient's computer. NIST's crypto standards are well regarded and are used by most public and private organizations around the world.").

quantum computers capable of breaking modern public-key cryptography was 2033.[79] An analysis published by the MIT Technology Review suggested about 20 years as a possible timeframe, based on the previous speed of innovation in quantum computing.[80] However, the ultimate achievement of a system capable of surpassing encryption standards is dependent on the ability to meet intermediate goals. For example, IBM declared its goal of 2023 for achieving a 1,000-qubit quantum platform.[81] Although such a system would not be large enough to break modern encryption, it could allow for the accelerated development of a system capable of performing error analysis programs and error correction models.[82] Thus, continued monitoring of the quantum technology landscape is vital in intermittently adjusting predictions for the quantum decryption timeline.[83]

Realistically, meaningful QIS technology capabilities lie in the medium to long-term future. In the medium-term future, specialized quantum computers will likely be achieved with the capability of performing a narrow group of task types. This means that certain actors will have limited capabilities to decrypt information, assuming that is a priority in developing specialized quantum platforms. However, these actors will be limited both by the amount of computing power they can devote to such tasks, since the number of operable quantum computers is likely to be low, and by the type of decryption they are able to perform. Early systems are likely to take the form of Noisy Intermediate Scale Quantum (NISQ) computers, for which many programs and models are already under development.[84] Although NISQ computers will not be as

---

[79] Marissa Norris, *Quantum Computers Will Break the Internet, but Only if We Let Them*, RAND CORP. (April 9, 2020), https://www.rand.org/blog/articles/2020/04/quantum-computers-will-break-the-internet-but-only-if-we-let-them.html.

[80] Craig Gidney & Martin Ekera, *How a Quantum Computer Could Break 2048-Bit RSA Encryption in One Hour*, MIT TECH. REV, (May 30, 2019), https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/.

[81] Jay Gambetta, *IBM's Roadmap for Scaling Quantum Technology*, IBM RSCH. BLOG: QUANTUM COMPUTING (Sept. 15, 2020), https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/ ("Our team is developing a suite of scalable, increasingly larger and better processors, with a 1,000-plus qubit device, called IBM Quantum Condor, targeted for the end of 2023.").

[82] *See id.*

[83] Q2B 2020, *Fireside Chat with John Preskill*, YOUTUBE (Feb. 9, 2021), https://youtu.be/OI501qtq1p4 (starting at 6:15: discussing aggressive roadmaps proposed by IBM and IonQ, and the importance of hitting intermediate timelines).

[84] *See* QUANTUM COMPUTING: PROSPECTS AND PROGRESS, *supra* note 23, at 59 ("The field is now entering the era of noisy intermediate-scale quantum (NISQ) devices – the race to build quantum computers that are sufficiently large (tens to hundreds or a few thousand qubits) that they cannot be efficiently simulated by a classical computer, but

efficient as post-NISQ, they will allow for quantum computers to perform more complex tasks (even if taking longer amounts of time) in the more immediate future.[85] In the long-term, more general quantum computers with wider sets of applications are possible and must also be considered, although not necessarily prioritized relative to other threats.

II. GOVERNANCE TRENDS AND CONSIDERATIONS

Given this uncertainty over timing, the U.S. government is actively developing an overarching strategy related to quantum encryption and has thus far developed a mixed framework to reflect its competing interests.[86] While the government views quantum decryption as a risk to national security, defense and security agencies and departments are also interested in the prospect of utilizing the capabilities of quantum computers to compete with national adversaries in security supremacy.[87] This is consistent with governance of other emerging technologies; policymakers attempt to strike a balance between being adaptive enough to apply to new technology for potential utility, but also preempt the efforts made by other countries in order to defend critical infrastructure. This section will briefly survey the main motives of policymakers in striking these balances in order to lay the groundwork for following sections which offer policy recommendations.

The balance between offense-defense interests in technology development and governance is not a new problem. This intragovernmental debate has been occurring since at least the Cold War in the context of modern technologies.[88] In the age of the Cold War and the nuclear weapon buildup, a key decision was whether to continue to increase nuclear stockpiles and engage the Soviet Union in technology competition, even if it led to destabilizing and ultimately dangerous

---

are not fault tolerant and so cannot directly implement the algorithms developed for ideal quantum computers.").

[85] *Id.* at 79–80 (describing several specific potential near-term applications for NISQ computers).

[86] HOMELAND SECURITY ADVISORY COUNCIL, FINAL REPORT: EMERGING TECHNOLOGIES SUBCOMMITTEE QUANTUM INFORMATION SCIENCE 20 (Nov. 2020), https://www.dhs.gov/sites/default/files/publications/final_emerging_technologies_quantom_report_1.pdf.

[87] *Id.* at 22 (discussing several capabilities of quantum computing including "highly sensitive tunnel detection," and "detection of WMD").

[88] Charles L. Glaser & Chaim Kaufman, *What is the Offense-Defense Balance and Can We Measure It?*, 4 INT'L SECURITY 44, 76 (1998) (discussing the ongoing debate as to the merits of the offense-defense balance: "During the Cold War, net assessments performed by civilian analysts established the foundation for extensive debate over NATO's prospects for defeating a possible Soviet offensive in Central Europe").

scenarios. This framework for analyzing development was referred to as the "security dilemma."[89]

In the modern context, the security dilemma has become even more complicated with the increased role of the private sector. While the government was the prime innovator during the Cold War, and thus had greater control over technology dispersion, the increased role of the private sector has led to more complicated governance questions. Fundamentally, the government has less control over how a technology is developed, and once developed, how it is dispersed and who it is transferred to. This has become a key issue in the context of technologies that have both civilian and defense applications - referred to as "dual-use technologies." Dual-use technologies have become a major government focus because the civilian applications produce market interest that spur private sector production that then leads to greater dispersion, which could enable defense applications to a wider variety of actors.[90]

Furthermore, as economic security becomes a greater geopolitical factor, the security dilemma and dual-use technology governance suffer from added complexity.[91] Now, governments must consider the increased security importance for civilian development of dual-use technologies in driving domestic economic gains. This has resulted in three competing considerations with regard to emerging technologies: the desire to foster innovation, the need to minimize security risks, and the importance of promoting opportunities for economic gains. Unfortunately, policies to support any one of these trends may negatively impact the other. For example, policies that impose overly burdensome controls on technology sales and transfers due to security concerns may stymie innovation by cutting off potential markets, thus preventing economic growth.[92] Thus, policies on technologies such as quantum computing must carefully weigh how individual policies would impact these overarching strategic aims.

Additionally, beyond governance of the technology itself, policies that dictate response to the technology may also be necessary. This is especially true in the case of quantum decryption. Once quantum

---

[89] Charles Glaser, *The Security Dilemma Revisited,* 50 WORLD POL. 171, 171 (1997).
[90] *See* EMERGING TECHNOLOGIES, *supra* note 7, at 5.
[91] *Id.*
[92] Johnson, *supra* note 13, at 503 ("As rigid regulatory approaches become more widespread in fields including health and the environment, critics accused these strategies of imposing onerous costs on industry, lacking efficiency and realistic enforceability, and snuffing out innovation."); *see also* Richard B. Stewart, *The Discontents of Legalism: Interest Group Relations in Administrative Regulation*, 1985 WIS. L. REV. 655, 66064 (1985).

encryption methods are formalized, the government will need to issue policies to foster, and in some cases enforce, its implementation to ensure that critical industries are safe. This means that in addition to governing entities involved in quantum computing development, policymakers will also have to consider governance regarding the technology trend across industries.

III. REGULATING QUANTUM CRYPTOGRAPHY

Given the legal risk exposure and security concerns associated with quantum decryption, both for the government and industry, the groundwork for a regulatory framework must be set forth. As this paper has shown, quantum technology disruptions, and specifically quantum decryption, impose significant privacy and security risks that could seriously harm domestic national security or critical infrastructure. This is exacerbated by the fact that the timeline to disruption is still fairly vague. However, breaches would have enormous legal impact as well, highlighting debates over encryption accountability for public and private entities, IP enforcement, technology transfer law, and antitrust/public-private relation law. Many of these legal frameworks are double edged swords in the case of quantum encryption (and emerging technology governance more broadly). On one hand, they introduce a uniquely powerful opportunity to regulate technology innovation, transfer, and use; on the other hand, overly rigid and burdensome law could hamper innovation or fail to respond quickly to technology-specific requirements.

The starting point of developing an appropriate regulatory scheme begins at the two binary poles of regulatory philosophy "command and control," and "decentralization."[93] On one end, "command and control" regulation regimes provide for rigid, predetermined standards to which industry players must adhere precisely in order to pass muster.[94] On the other end, decentralized sectors of industry exist in which the government plays a "hands-off" approach and lets industry players develop the rules of the road.[95] Since the turn of the twentieth-century, many hybrid approaches have begun to emerge.[96]

When applying regulatory themes to emerging technologies, considerations are often given to the those enunciated by the policies set

---

[93] *See* Johnson, *supra* note 13, at 504.
[94] *See, e.g., Id.* at 510-13.
[95] *Id.*
[96] *Id.* at 503–04.

forth in Part II, such as promotion of innovation, dispersion of technology, mitigating security risks, balancing offensive and defensive development, and engaging shareholders.[97] For quantum computing, like many other emerging technologies,[98] there are concerns unique to the specific technology that necessitate a unique balancing of the general features. And, as noted in Part II, a field with as vast a potential as quantum computing likely requires a compartmentalized approach within the broader ecosystem. However, it is important to keep in mind the fact that regulation in a field like quantum cryptography will have rippling effects throughout the larger ecosystem of quantum computing as well as the adjacent classical computing ecosystem.

Beyond the plethora of factors aforementioned, there are other features of innovation like those in quantum computing which make regulatory confrontation far more likely to occur with certain legal fields. One field of law that we are likely to see invoked by, among other factors, the magnitude of private sector involvement is the increasingly complex United States antitrust laws.[99] Specifically, quantum computing innovation is being taken on by private industries with the financial aid of the government.[100] But, in other innovative leaps, such as the Space Race, the government generally concentrated resources into a small number of proven companies and allowed for rapid consolidation. However, many scholars have opined that small and medium enterprises (SMEs) should be given a fair shake to participate in innovation and standards development.[101]

Going hand-in-hand with antitrust but also playing an independent role in the analysis is the patent system. Patentees have a right to exclude competitors from using patented technology.[102] So, in

---

[97] *See supra*, Part II; *see also Id.* at 502.

[98] Diana M. Bowman & Graeme A. Hodge, *Nanotechnology: Mapping the Wild Regulatory Frontier*, 38 FUTURES 1060, 1064 (2006).

[99] Mauritz Kop, *Regulating Transformative Technology in The Quantum Age: Intellectual Property, Standardization & Sustainable Innovation,* TTF Newsletter on Transatlantic Antitrust and IPR Developments (Nov. 23, 2020), https://ttlfnews.wordpress.com/2020/11/23/regulating-transformative-technology-in-the-quantum-age-intellectual-property-standardization-sustainable-innovation/ (listing necessary components such as quantum gates & multipliers, quantum integrated circuit chips, dilution refrigerators, etc.) [*hereinafter RTT Paper*].

[100] *See Information Overload*, *supra* note 18 ("Policy makers must confront the uncomfortable reality that the future of national security now relies on the government's ability to oversee, regulate, and adopt the research and emerging technologies developed by private companies").

[101] *See RTT Paper*, *supra* note 97 (discussing the interleaving roles of antitrust and intellectual property law in the development of modern technologies).

[102] 35 U.S.C. § 154.

theory, a technology company could (and many have)[103] patent a form of encryption, and prevent others from using the technique, and any associated products. As mentioned in Part I, NIST has already considered the effect of standardizing a patented encryption system, and the topic will likely become an important issue in coming years. In considering the topic of patents among other issues, it is important to think about the international effect of regulatory strategies. For example, China has been rapidly patenting quantum cryptography, which could hinder the United States' ability to compete in the space if innovators are not properly incentivized in the early-going stages.

A. The Current Regulatory Regime for Encryption and Cryptography

Some regulatory transition work has already started. For instance, in 2018 Congress enacted the Export Control Reform Act (the "ECRA"), which expanded the Executive Branch's authority to regulate and enforce export controls by requiring the Secretary of Commerce to establish controls on the export, re-export, or in-country transfer of "emerging or foundational technologies."[104] Among a large assortment of technological categories, the ECRA seeks to regulate the exportation of certain products for use in quantum computer development. But there are still many specifics of the ECRA that have not been established, specifically as it relates to quantum computing.[105] By looking at recent regulatory regimes and the underlying theory, the government may be able to better assess how to approach quantum computing regulation as it relates to cryptography.

Even if we take quantum computing out of the picture for a moment, regulating data security is an important and challenging issue. Not only are there technical challenges to overcome to prevent hacking, but there are also countercurrents to having robust security systems. Encryption is, at its essence, the process of transforming readable

---

[103] Greg Vetter, *Patenting Cryptographic Technology*, 84 CHI.-KENT L. REV. 757, 761–65 (2010) (describing the various schemes of commercialization and government intervention associated with the three "pioneer patents" of modern cryptography).
[104] While the U.S. Department of Commerce is required to impose export controls over emerging and foundational technologies, these terms are not defined in the ECRA, but attempts to craft such controls have begun. *See, e.g.,* Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201 (proposed Nov. 19, 2018) (An advanced notice of proposed rulemaking (ANPR) set out by the Bureau of Information Security (BIS)) [hereinafter ANPR].
[105] *Id.*

information so that it is not immediately recognizable.[106] While there are two main types of encryption, symmetric (or "private") and asymmetric (or "public") key systems, the more relevant form for this discussion is the public key system.[107]

Encryption is widely regulated globally, particularly because it is considered a "dual-use" technology.[108] Since the Cold War, United States encryption regulation has been characterized by two competing concerns: "(1) the ability of American high-tech industries to compete in foreign markets; and (2) the ability of criminal terrorists to threaten national security through the use of strong encryption."[109] As a result, there has been little restriction imposed on domestic encryption, or importation of cryptography products. But there is strict (though, easing) regulation on the export of encryption products.[110]

Generally, controls on the exportation of dual-use technologies are harmonized for many countries according to a set of principles known as the Wassenaar Arrangement[111] (while more specific and acute technologies may be covered by agreements such as the Nuclear Suppliers Group (NSG) or the Missile Technology Control Regime (MTCR)).[112] When it comes to cryptography, the Wassenaar Arrangement sets a lower bound for cryptography regulation, making symmetric cryptography products up to 56 bit key length, and asymmetric cryptography products up to 512 bit key length free from export restriction for all member states.[113]

In the United States, the Export Administration Regulations (EAR), administered by the Commerce Department's Bureau of Industry

---

[106] D. RICHARD KUHN ET AL., NAT'L INST. OF STANDARDS & TECH., INTRODUCTION TO PUBLIC KEY TECHNOLOGY AND THE FEDERAL PKI INFRASTRUCTURE §2.3 (2001), https://apps.dtic.mil/sti/pdfs/ADA394230.pdf ("In cryptography, a sender transforms unprotected information (plaintext) into coded text (ciphertext). A receiver uses cryptography to either (a) transform the ciphertext back into plain text, (b) verify the sender's identity, (c) verify the data's integrity, or some combination.").

[107] Symmetric key systems include, for example, protecting a document with a user password. While asymmetric systems utilize separate keys for encryption and decryption. The key for encryption is normally public, while the one for decryption is held private by the user or by a third-party (e.g., an escrow). Nathan Saper, Note, *International Cryptography Regulation and the Global Information Economy*, 11 NW. J. TECH. & INTELL. PROP. 673, 674-77 (2013).

[108] Kurt M. Saunders, *The Regulation of the Internet Encryption Technologies: Separating the Wheat from the Chaff*, 17 J. MARSHALL J. COMPUTER & INFO. L. 945, 950 (1999).

[109] Tricia E. Black, Note, *Taking Account of the World as It Will Be: The Shifting Course of U.S. Encryption Policy*, 53 FED. COMM. L.J. 289, 297 (2001).

[110] *Id. at* 297-98.

[111] Saper, *supra* note 105, at 678.

[112] EMERGING TECHNOLOGIES, *supra* note 7, at 15.

[113] Saper, *supra* note 105, at 678.

and Security (BIS), is the primary regulation for encryption exports.[114] The regulations specify that generally, symmetric encryption systems with key lengths of 56 bits or less, or asymmetric systems with key lengths of 512 bits or less, can be exported without restriction.[115] But encryption products for any length greater than that are considered "strong encryption" products and are subject to EAR regulation, unless they fall under the exemption for "mass market" encryption products.[116] Further complicating matters is the fact that additional controls in the United States restrict exportation to certain countries. The Office of Foreign Assets Control (OFAC) restricts the exportation of cryptographic software among other sensitive products to specific countries.[117] Within and in addition to these specific countries, OFAC administers restrictions against certain individuals and entities, "Specially Designated Nationals" (SDNs).

EAR restrictions apply to exports whether they are performed by the typical method of shipment, or electronic delivery over the internet.[118] And while the environment for exporters has become slightly more relaxed recently, private entities have begun to be saddled with a heavier burden in terms of compliance. As noted by one scholar:

> Today's private entities have much greater responsibility for ensuring compliance with any applicable regulations. The penalties for non-compliance are severe, and lesser involvement by the agencies on the regulatory side has made government resources available on the enforcement side. Therefore, more than ever before, private entities must make sure they have internal compliance or export management systems in place to avoid or minimize export control violations.[119]

---

[114] *Id.* at 680 ("Encryption products are regulated under Category 5, Part 2 of the EAR.")
[115] *Id.* at 678.
[116] *Id.* ("[I]f an encryption product is generally available to the public, for home or personal use, without continuing support by the supplier (e.g., a personal email security program), then its export is not restricted by this section.").
[117] *Id.* at 681.
[118] John F. McKenzie, *U.S. Export Controls on Internet Software Transactions*, 44 INT'L L. 857, 860 (2010).
[119] Christopher F. Corr, *The Wall Still Stands! Complying with Export Controls on Technology Transfers in the Post-Cold War, Post-9/11 Era*, 25 HOUS. J. INT'L L. 441, 491-92 (2003).

Based on this viewpoint, the cryptography regulation regime is a hybrid of soft and hard regulatory systems. While the subject matter of the regulations has been eased, the compliance and enforcement aspects of the regulatory process have posed increasing burdens on industry players.[120] One of the benefits of this regime is that compliance restraints "ease-in." The contributions to enforcement have steadily increased to better capture non-compliance as the technology has become more standardized. Scholars have argued that the cryptography regulations in the United States have placed substantial burdens on information technology (IT) and security firms, placing them at a competitive disadvantage.[121]

As we start to think about approaches to regulating quantum cryptographic products, whether those implementations on quantum or classical computers, one aspect of the discussion to consider is how quantum decryption would impact EAR regulation of exported encryption products. For starters, the export restrictions on "strong encryption" products may be less relevant if quantum decryption becomes widespread. Current notions of "strong encryption" are based on a premise rooted in classical computing principles.

B. Implementing and Enforcing Policies as Regulation

Given the policy goals set forth in Part II, we can hypothesize as to how the government can best implement such strategies in a way that will foster innovation while protecting national security. While there is still too much uncertainty to develop concrete regulatory standards, there are developments in both the public and the private sectors which may provide helpful clues as to how the issues of quantum cryptography will play out as the technology becomes more widely available.

1. The ECRA: A Starting Point for Quantum Hardware Regulation

One aspect of quantum computing that has already been the subject of proposed regulations is the cooling requirement for qubits to maintain proper states during computation.[122] Basically, lower temperatures slow down the movement of atomic and subatomic

---

[120] Saper, *supra* note 105, at 684.

[121] *Id.*

[122] *See generally* Kuan Yen Tan et al., *Quantum Circuit Refrigerator*, NATURE COMMC'N, June 16, 2016, at 1, https://doi.org/10.1038/ncomms15189.

particles, making them less likely to experience perturbations during computation that lead to errors.[123] In 2018, the Bureau of Industry and Security (BIS) issued an advance notice of proposed rulemaking[124] (or "ANPR") regarding the enactment of the Export Control Reform Act of 2018 (the "ECRA"). The ANPR outlines the type of emerging technologies that fall within the subject matter of the ECRA, and includes quantum computing among other technologies.[125] The ANPR reiterates the relatively narrow scope of the legislation, noting that "[c]ommerce does not seek to expand jurisdiction over technologies that are not currently subject to EAR."[126] Since the ANPR's issuance, BIS has received many comments regarding the proposed rulemaking and there are some reports of what could ultimately result.

While there have been political tensions surrounding the legislation's relatively slow rollout,[127] with some lawmakers complaining about the Commerce department's "troubling" lack of urgency, it has become more clear that the ECRA will address exports to China.[128] Specifically, the ECRA requires BIS to impose a licensing requirement for the export of subject technology to any country embargoed by the U.S., which would apply to China's arms-embargo.[129] China has also addressed the proposed regulations, noting that it opposes "the U.S.' generalization of the concept of national security and abuse of export

---

[123] *Id.* at 2.

[124] *See* ANPR, *supra* note 106.

[125] It should be noted that the ECRA did not originally offer a precise definition of what "emerging technologies" would be controlled by BIS. *See* Judith Alison Lee et al., *New Controls on Emerging Technologies Released, While U.S. Commerce Department Comes Under Fire for Delay*, GIBSON DUNN (Oct. 27, 2020), https://www.gibsondunn.com/new-controls-on-emerging-technologies-released-while-us-commerce-department-comes-under-fire-for-delay/.

[126] ANPR, *supra* note 106 (noting, e.g., "fundamental research" described in § of the EAR).

[127] *Inside U.S. Trade Quotes Kevin Wolf on Commerce Department's First Emerging Tech Export Control*, AKIN GUMP (Nov. 27, 2019), https://www.akingump.com/en/news-insights/inside-u-s-trade-quotes-kevin-wolf-on-commerce-department-s.html ("While some members of Congress say the Commerce Department has been slow to complete several export-control reviews mandated by the law, Wolf said whether an extraordinarily high bar is being used for controlling emerging technologies depends on one's definition of national security.").

[128] Mario Mancuso & Anthony Rapa, *Anticipating a Turning Point in US Export Controls for Tech*, LAW360 (Jan. 28, 2020), https://www.kirkland.com/publications/article/2020/01/anticipating-turning-point-us-export-controls-tech ("The new ECRA controls clearly are directed at restricting exports of cutting-edge technology to China.").

[129] *Id.*

control measures to interfere with and restrict the normal communications and cooperation between businesses."[130]

According to a status update from the agency, it plans to regulate exports of quantum diluted refrigerators, which are used to maintain an extremely low-temperature environment for the qubits of quantum computers.[131] Further, there are indications that the United States will propose bilateral controls on quantum dilution refrigerators to the 42 participants in the Wassenaar Arrangement. Imposing such controls bilaterally would help ensure that U.S. manufacturers would be competing on a level playing field in the marketplace. However, quantum dilution refrigerating technology was not included in controls that were released in October 2020, on six categories of "emerging technologies," suggesting that controls of the technology may ultimately be taken on unilaterally, if at all.

So, based on the information that has thus far been released about the ECRA, regulation will be targeted toward the hardware components of quantum computers rather than the cryptography products specifically. However, such a "heavy-handed" approach could have the effect of reducing the dispersion of quantum cryptography products, as materials for constructing quantum computers, like quantum dilution refrigerators, which are chokepoint technologies to the utilization of the technology for any purpose.

2. Grasping at Thin Air: Regulating Post-Quantum Encryption in the Cloud

There is more uncertainty as to how to regulate quantum computing software at this point in the life cycle of quantum computing innovation (because of the underlying uncertainty as to which specific hardware the code will be running on).[132] However, as quantum

---

[130] Alexandra Alper, *U.S. Finalizing Rules to Limit Sensitive Tech Exports to China, Others*, REUTERS (Dec. 17, 2019), https://www.reuters.com/article/us-usa-tech-china-exclusive/exclusive-us-finalizing-rules-to-limit-sensitive-tech-exports-to-china-others-idUSKBN1YL1B8 (quoting Chinese foreign ministry spokesmen Geng Shuang).

[131] *Id.* ("Major makers of the refrigeration devices include U.K.-based ICE Oxford, Finland-based Bluefors and U.S.-based Janis Research.").

[132] In a recent conference, Q2B, industry and government experts described the impending consolidation of the hardware side, and how it would affect the QIS software industry. *See* Yehuda Naveh, *Quantum Software Development Is Still In Its Infancy*, FORBES (June 23, 2021, 8:50 AM), https://www.forbes.com/sites/forbestechcouncil/2021/06/23/quantum-software-development-is-still-in-its-infancy/?sh=5e18480c6ddd.

computing hardware does become more stable in the coming years, the regulation of quantum computing software will become important in preventing bad actors from taking advantage of quantum computing's capacity for decryption.[133] Because of the nature of the technology, it is unlikely that a "command and control" approach to software regulation will be feasible. There are simply too many unknowns. For one, NIST has not yet set forth standards for quantum-safe encryption. One reason for the lack of clarity around quantum-safe standards is the recursive nature of such threat landscapes. Just like current cryptography techniques rely on classical computing capabilities, quantum-safe encryption will likely be dependent on developments in quantum computing, such as quantum-randomness.

Until there is more clarity as to what hardware will power quantum computers, there will be no way to precisely implement regulation to control access and transparency. However, certain themes have emerged in the space, based on modern computing standards. For one, access to computing power is no longer predicated on access to physical hardware.[134] Some have proposed strict export controls as a means of regulating the dispersion of quantum computing technology.[135] But it is almost entirely unclear how this would affect the ability of a foreign resident from executing code on a quantum computer through a cloud interface. This conundrum highlights the importance of updating enforcement regimes so that they can effectively fulfill the purpose of such traditional mechanisms as export controls.

3. Embracing a "Crypto Agility" Mindset to Quantum Cryptography Regulation

One reason why classical computing has frustrated lawmakers is because of the complex and intractable nature of digital technology. Because lawmakers do not necessarily have expertise in gaining understanding of issues related to technology, they are forced to rely on independent experts and experts from the industry to understand their

---

[133] Michael J. D. Vermeer & Evan D. Peet, *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption*, RAND CORP. 36-37 (2020), https://www.rand.org/pubs/research_reports/RR3102.html.

[134] *See, e.g., IBM Quantum Services*, IBM, https://www.ibm.com/quantum-computing/services/ (last visited Feb. 13, 2022).

[135] Mauritz Kop, *Establishing a Legal-Ethical Framework for Quantum Technology*, YALE J.L. & TECH.: BLOG (Mar. 30, 2021), https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology [https://perma.cc/4C7T-EV4B].

options when it comes to enacting regulations.[136] But such an approach is not sufficient alone in tackling such regulatory issues because it does not provide a fully informed analysis. While technology experts can be useful in understanding how certain technologies work, they are not themselves experts at lawmaking. Lawmaking requires an acute awareness of the *facts* inherent to a legal issue. For society to do a better job of regulating quantum computing, agencies and other government regulators must bring subject matter expertise *in-house*. They must find and employ lawmakers *who really understand how the technology works*, and what makes it different from current methods of computing.

While quantum computing is arguably more complex from a technological standpoint than transistor-based digital computers, our society is likely more able to comprehend the capabilities and efficiencies of quantum computing against the contrast of the digital computer. While there was a time when many in our society (including lawmakers) chose to remain ignorant of the workings of computers, many today have been forced to grapple with the technology at least to the extent necessary to understand the legal ramifications.

C. How Patent Law May Impact Quantum Computing Policy Goals

As mentioned in Part I.B, there are conundrums associated with patenting developments in the quantum cryptography space, and particularly techniques for post-quantum encryption, which would necessitate wide-scale adoption. Some have argued against the protectability of quantum computing innovation, arguing that it will overprotect the innovation of "first movers."[137] Such arguments could be addressed by creating "quantum overlays" of existing patent laws—introducing shorter IP protection durations of 3 to 10 years for "Quantum and AI infused creations and inventions."[138] However, such an approach would necessarily create mass confusion not only in industry, but also among investors and government stakeholders. After all, what value

---

[136] *See* Weiser, *supra* note 2, at 573.

[137] Mauritz Kop, *Quantum Computing and Intellectual Property Law*, 2021 BERKELEY TECH. L.J. COMMENTARIES, 101, 112, https://btlj.org/2022/02/quantum-computing-and-intellectual-property-law/ ("Strategically using a mixture of IP rights to maximize and protect the value of the IP portfolio of the quantum computer's owner can result in an unlimited duration of global exclusive exploitation rights for first movers absent compulsory licensing of standard essential patents (SEPs) in certain territories.").

[138] *Id.* at 113.

could a three-year patent term provide an investor when it is less than probable that a viable market for quantum computers will exist by then?

Further, there is mixed empirical evidence on the question of whether patent protection creates impenetrable barriers for small businesses in the computing industry, where most of the quantum computing innovation is taking place. Nevertheless, stakeholders are skeptical about the effect on innovation if patents become an impediment to entry in the space. For instance, regarding NIST's post-quantum encryption standard competition it made participants sign the following waiver for their submissions to the competition to be considered "complete."[139]

> *… I further declare that (check one):*
>
> > *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____ (print name of cryptosystem)_____; …*[140]

NIST's and others' concerns about patent protection negatively affecting the widespread adoption of post-quantum encryption techniques have historical basis.[141] After all, companies will be more hesitant to adopt new security measures for protecting data if such adoption requires a patent license to avoid risking a lawsuit.[142] At the same time, there could be a middle-ground of protection for "strong" post-quantum encryption while freeing up more mainstream techniques to allow for mass adoption.[143] Additionally, since the government has a pecuniary interest in the national security associated with post-quantum encryption, it is entirely possible that the government could play a key role in a public-private licensing scheme for such technologies that would

---

[139] PQS SUBMISSION REQUIREMENTS, *supra* note 78, at 8.

[140] *Id.* at 10. The declaration also requires applicants to disclose if their cryptosystems are subject to U.S. or foreign patents.

[141] *See generally*, Vetter, *supra* note 101.

[142] *Id.* at 764.

[143] For an example of how litigation risk was mitigated with respect to IBM's Data Encryption Standard (DES) patent, see *id.* ("In the case of DES, the government announced that IBM would grant nonexclusive royalty-free licenses for use of the standard, even if the resulting device, software, or technology infringed the DES patent.").

allow innovators to benefit from their research and development without passing all the burden onto the public.[144]

Besides creating explicit carve-outs for quantum-related technology as some authors suggest, which would likely lead to confusion and would require significant Congressional intervention, several considerations have been raised to promote a healthier ecosystem for innovation in this area. Beyond specific considerations, it is important to keep in mind that the United States' patent laws do not operate in a vacuum, and the ability to control international dispersion of quantum cryptography products depends to a large extent on how much patenting takes place internationally. Particularly, China has been rapidly increasing patenting in this area since approximately 2013.[145]

D. Broader Governance in Addition to Improved Legal Frameworks

While improved legal frameworks will enhance the government's ability to preserve core strategic objectives related to quantum computing and emerging technologies, they will not be a panacea. Instead, adjustments to the legal system must be complemented with policies that improve government engagement and promote a positive public-private relation. Key policy recommendations include: improved workforce education access; engagement across agencies and with the private sector; engagement with international actors; intra-government preparation; resource assistance for necessary technology preparations.

Improved internal knowledge. Given the rapidly changing landscape of quantum computing, and the esoteric and technical nature of the field, an internal knowledge within the government base will be important for ensuring an adequate response. To develop technical literacy across agencies, post-quantum cybersecurity task forces should be established to determine which knowledge bases each agency maintain and which knowledge areas are needed. This could include members from across the agencies who have fluency in different

---

[144] Beyond a simple licensing scheme, the government could also facilitate a patent pool to provide for a reduced barrier to entry while also providing some financial benefits to innovators.

[145] PATINFORMATICS, QUANTUM INFORMATION TECHNOLOGY (QIT): A PATENT LANDSCAPE REPORT 8 (2018), available at https://www.patinformatics.com/quantum-computing-report ("Since 2013, the number of publications that listed China as the priority country have grown by almost 750% which clearly demonstrates China's commitment to research in the quantum information technology field.").

knowledge areas necessary to understand quantum decryption developments, including quantum physics, materials science, advanced mathematics, and computer science. Once an understanding of the working knowledge is determined, the agencies could then seek out opportunities to fill voids in the necessary knowledge base. This could be achieved through hiring, webinars, fellowships, etc. Improved internal knowledge will also boost confidence of private sector and international actors in governance efficacy.

Interagency and private sector engagement. Beyond internal planning, agencies should also be involved in interagency quantum information science activities and private industry engagement. Both interagency and private engagement can lead to better awareness of the types of threats related to QIS technologies, as well as the different types of solutions to mitigate these threats. Interagency engagement will allow for each agency to determine its unique role within the federal government in preparing the country for QIS technology implementation. Private sector engagement will allow for a better understanding of how policy responses would impact the private market and would likely improve compliance by improving private sector understanding of the government's objectives.

Engagement with international actors. The government should also establish an international network, especially for legal implementations with global reaches. This is necessary given the sheer number of international collaborations and funding schemes required to meet the immense resource necessities of QIS technology innovation. By better understanding of the priorities and objectives of international entities, the government can help to ensure that it is aware of potential adversary capabilities and intent, as well as those of allies. Furthermore, it will help to foster a more collaborative, rather than secretive, approach towards quantum computing innovation and regulation. Finally, such a network can help to establish international buy-in for policies that require multinational commitment.

Intra-government preparation. The government, and each agency, must also adequately prepare to deploy post-quantum encryption. This first involves identifying assets and setting up prioritization schemes for deployment based on asset security levels. Once assets are identified and ranked and adequate institutional knowledge is built, the available post-quantum encryption options must be surveyed and assessed based on their utility in securing each agency's devices and assets. Options should derive from the pool of NIST-approved post-quantum encryption algorithms. Options should then be

assessed based on their feasibility of application to agency assets, including consideration for hardware and software needed for implementation. Options should also be vetted based on their security strength. In measuring this, the agency may find it beneficial to test competing options to verify that the implementation does not introduce new vulnerabilities.

Resource assistance for necessary technology preparations. Finally, through engagement with international and private industry members, and after assessing the needs of different agencies, the government should identify necessary technology areas and market gaps to support. Specifically, technologies that may not immediately have enough market interest to accelerate development may need to be supplemented with government funding and resource allocation. This is likely to include post-quantum encryption but could include other security-relevant technologies.

CONCLUSION

As this Article has shown, an exact timeline for quantum decryption is unknown, and despite cross-technology competition, immediate steps to prepare for its eventual deployment should be taken. There are many issues facing the United States government, even within the cryptography domain.[146] Certain emerging technologies, such as artificial intelligence, are competing with quantum computing for resources in application-based research. While it may be convenient to discount the value of quantum computing during its early stages of development, there are plenty of signs that a "wait-and-see" approach would be unwise. Instead, the government should begin to slowly ramp up internal knowledge, protocols, and funding to support a robust post-quantum encryption ecosystem.

Further, given the major risks associated with quantum computing, both legal and policy preparations will be necessary. Even though legal frameworks are not currently as suitable for emerging technologies as they should be, they do offer unique benefits for producing enforceable and clear rules of the road for new technologies. Thus, efforts to overhaul the legal system as it pertains to emerging technologies, and especially quantum computing, should begin.

---

[146] Bill Chappell et al., *What We Know About the Apparent Russian Hack Exploiting a U.S. Aid Agency*, NPR: NATIONAL SECURITY (May 28, 2021, 12:50 PM), https://www.npr.org/2021/05/28/1001237516/what-we-know-about-the-apparent-russian-hack-exploiting-a-u-s-aid-agency.

However, adjustments to the legal framework will also require policies that reinforce a more technologically savvy and collaborative government approach. Increasing technological literacy within the government and creating cross-sector networks will be essential in identifying areas for government involvement and establishing greater trust and efficacy of political and legal governance mechanisms.