Law and Policy for the Second Quantum Revolution

[Author Name Redacted][1]
[Word Count: 18616]

Abstract

We are living in the "second quantum revolution." Using theoretical insights from the first quantum revolution of the early 20th century, multidisciplinary teams have achieved fantastic advances in quantum metrology and sensing, in quantum communications, and in quantum computing. Metrology and sensing will enable high-resolution imaging, with attendant effects on everything from medicine to battlespace conflicts through enhanced sonar and radar. Quantum communications raise the specter of networks invulnerable to spying, and the fundamentals of such networks are already in place, with some technologies available commercially. Quantum computing, as many have observed, will degrade and in some cases render useless, the encryption that everyday commerce relies upon. But it will likely also enable simulation of complex systems and contribute to advances in machine learning.

The affordances and limitations of quantum technologies will shape who can access and use these innovations. Furthermore, quantum technologies will arrive at different times and thus create surprising path dependencies. For instance, many hold out quantum computing as a doomsday technology for privacy, yet, some doubt that general purpose quantum computers necessary for the privacy apocalypse can even be built. Even if built, only nation states and large companies will have access to the technology, and these technical and economic constraints will shape both how quantum computers might be misused and how regulation might work.

Excitement surrounding quantum computing should not cause us to overlook the advances in metrology, sensing, and communications that are already here and likely to be miniaturized and commercialized in ways quantum computers will not be for the foreseeable future. Indeed, in the short term, quantum may contribute to advances in communications integrity, confidentiality, and authenticity.

There is no legal literature on the consequences of quantum technologies broadly and only a thin exploration of it in the ethics literature. Thus, this article starts a policy conversation on the high-level issues raised by quantum technologies. Quantum technologies will create strategic concerns for national security and for the intelligence community. Already China and Europe have made large investments into quantum communications technologies in explicit attempts to create surveillance-detecting and surveillance-invulnerable networks, no doubt motivated by revelations of the National Security Agency's

[1] Thank you footnote: Lily Lin, Evan Wolff.

spying power. Quantum metrology and sensing raises similar strategic concerns, from the uncloaking of submarine movements and thus unsettling the balance of power reached through the nuclear triad to development of electronic-warfare resistant weapons. Combined these developments might mean that the golden age of signals intelligence may be yielding to a golden age of measurement and signature intelligence.

Responsive policy options could take many forms, from export control efforts and industrial policy to aggressive immigration policy aimed at attracting and retaining the best minds of the field. Steps can also be taken now to avoid meltdowns in confidentiality, integrity, and authenticity of data made possible if a general-purpose quantum computer is achieved. For instance, it is important to advance password complexity and to find more secure ways to sign software and digital certificates, because these technologies will be both made vulnerable by quantum computing, and be the kinds of attacks of most interest to entities likely to develop quantum computers.

The internet revolution arrived with no coherent legal regime or strategy. We need not be unprepared for the quantum revolution. As quantum technologies reach deployment readiness, we can make fundamental decisions on how policy should complement or inhibit them. At the highest level, we should promote quantum in the many ways it could contribute to human flourishing. These include medical diagnostics, advances in materials science and design, and drug discovery. But it would be naïve to overlook how quickly governments are adopting these technologies for military purposes, and in doing so, perhaps even creating a quantum "taboo." Thus, realists need to contemplate how quantum will affect nation-state conflict, whether and how quantum technologies should be commercialized, and what steps can be taken today to prevent quantum from being a destabilizing technology.

Introduction

We are on the precipice of a major technological turn, one that will have profound consequences for how we measure and sense the world, for how we communicate, and for how computing works. This turn follows a change in the physics used for these different functions: from classical physics with its rules for the things we interact with in daily life, to quantum physics, the rules that govern the interactions of the very small.

Einstein, Bohr, Plank, Heisenberg and others led the first quantum revolution by advancing theory in the early 20th century. Years and even decades after their deaths, scientists valorized their insights with clever experiments. These experiments revealed the characteristics of subatomic world. Because we have no experience of the subatomic world in daily life, quantum physics is counterintuitive and difficult to grasp. Quantum includes phenomena so strange that they include names such as "spooky action."

We now live in an era where scientists are converting quantum theory into usable technologies. In this second quantum revolution, technologies leverage the special physics of the very small to measure physical phenomena and time very precisely (quantum metrology), to create imagery or otherwise sense phenomena invisible to ordinary sight (quantum sensing), to distribute encryption keys and communicate information (quantum communications), and to engage in computing (quantum computing, hereafter "QC")[2] This article explains the affordances of quantum through the lens of these four areas of applied quantum physics. It then turns to a landscape of important policy and legal issues that applied quantum raises. Several quantum phenomena must be understood in order to reach these policy implications and they are treated here at the highest level possible.

Quantum computing receives special treatment here because the topic has captured the imagination of the popular press. The companies developing QC foresee awesome innovations. Leading companies such as IBM emphasize the fit between QC and the modeling of complex chemical reactions. The logic is that in order to model the unfathomably complex subatomic properties of chemical reactions, one needs a computer governed by quantum instead of classical physics. Other companies see possibilities for optimization across a wide range of disciplines from materials science to nuclear physics. With QC, instead of using wet or other physical labs, one might model every possible shape of an object, say an airplane wing, in order to test its properties. Other companies are betting on QC to solve intractable problems in machine learning imposed by the limits of classical computers. Such developers assume that *quantum parallelism* (see below section XXXX) will enable computers to consider every possible variation of complex puzzles simultaneously unlike today's classical computers, which must solve problems sequentially.

One often hears about the capacity for QC to break the most sophisticated encryption available today, leading to drastic problems with data confidentiality, data integrity, and authenticity of identity. It

[2] J. P. Dowling & G. J. Milburn, *Quantum technology: the second quantum revolution*, 361 PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A-MATHEMATICAL PHYSICAL AND ENGINEERING SCIENCES 1655 (2003).

is true that some encryption will become vulnerable if reliable QC is developed. Yet, in the meantime, other, important quantum innovations in metrology, sensing, and communications have already arrived or are close at hand. The affordances of technologies in the metrology, sensing, and communications space have strategic implications and could affect how conflict is waged. Yet, these other fields of quantum have not received the popular attention that QC has. In part, this is because of how unfamiliar measurement and sensing technologies are. After all, one fundamental technical article with implications for quantum sonar is titled, "Development of a SQUID-based airborne full tensor gradiometers for geophysical exploration."

This article brings these other, near-term sensing and communications developments into focus, and then explains the likely order in which QC will degrade encryption and password hashing. Understanding how quantum technologies will develop could elucidate a path for addressing its potentially destabilizing implications. The good news is that policy choices taken soon could blunt the consequences of QC on the confidentiality, integrity and authenticity of data. Counterintuitively, developments in sensing and communications create trickier problems, and ones that are more certain to arrive than QC.

We are at the cusp of a quantum revolution, yet we have not countenanced the social challenges presented by the technology. We have the opportunity to set normative goals for how the technology is applied, especially if the democratic west leads its development. What should those highest-level norms be? And how do we establish a quantum policy before the technologists write the rules?

Important quantum affordances

Quantum mechanics describes the phenomenon in the Hollywood trope of the superhero passing through walls because "we are mostly made up of empty space." In real life, we cannot phase through walls, however the atoms we are made up of are mostly empty space. Quantum mechanics help describe the counterintuitive and strange behaviors of nature at the atomic and subatomic scale. Our atoms have an outer layer of electrons that simultaneously have the property of particles, thus leaving the atom mostly empty space, and a probabilistic distribution – the electrons could be everywhere thus leaving no empty space. This allows the atoms that we are made up of to be at the same time made up of less material as well as solid.

At the quantum scale, nature is probabilistic and objects have attributes of both waves and particles. This differs from our day-to-day, classical physics life. In our ordinary lives, we can predict how objects will act by knowing their mass, inertia, and so on. Quantum requires us to accept a different of reality governed by probability. As such, quantum is as unsettling as is it profound.

To understand the second quantum revolution, it is most important to grasp three phenomena: superposition, the no-cloning theorem, and entanglement. Quantum technologies take advantage of these three phenomena to varying extent to produce some kind of useful functionality, just as in classical physics, tools may take advantage of gravity, work, and friction.

Superposition

The nature of light provides insight into all three important quantum characteristics. The question of whether light was a wave or a particle occupied a centuries-long debate among scientists. Light's wave-like properties, reflection, refraction, diffraction, and interference, are readily observable respectively, in mirrors; as light bends in lenses; as light "curves" around objects and creates fuzzy boundaries of shadows; and as light interferes with itself, creating peaks and ebbs of light energy. Diffraction and interference in particular suggest that light is a wave, because particles should not bend around objects, nor should they bend and then interfere with each other to create bands of energy that resemble waves.

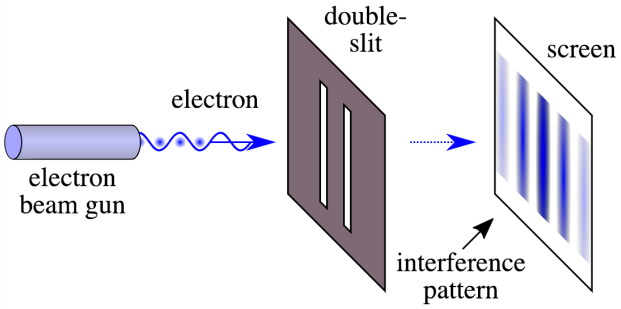

Figure 1 The initial setup of the double-slit experiment. The interference pattern suggests that the beam is a wave. Adjustments to the experiment show that light has wave/particle duality. Image public domain by Johannes Kalliauer for Wikipedia.

The famous double-slit experiment illustrates several quantum phenomena, including the dual wave/particle nature of small particles, and superposition. Full length books have been devoted to the experiment;[3] the complexity of which thus cannot be fully conveyed here.

The original goal of the experiment was to conclusively prove whether light was a particle or wave. Modern applications of the experiment are done with devices that can emit a single electron. Imagine there is a wall with two openings, if your object is a particle, say a tennis ball, then you would expect it to pass through only one of the openings and see a single spot where your object hits the other side. As you increased the number of tennis balls, you would expect eventually the shape of the two openings to be seen on the other side. If your object instead was a wave, e.g. a cup of water, you would expect it to pass through both of the openings and splash patterns on the other side.

In the experiment, a technician beams electrons through a filter that has two slits (see figure 1) with an energy-sensitive screen behind it. If the electrons were a like a tennis ball, they should create two bands on the screen corresponding to the filter's two slits. But instead an interference pattern emerges, suggesting that electrons are a wave. Logically, the electrons must have gone through one or the other slit, and then they interfered with each other after emerging from the slits. The post-slit interference created a wave pattern of convergence and interference. The pattern is brighter where waves are constructive, indicating a peak intensity, with dark areas between the bands indicating where the waves were destructive.

[3] ANIL ANANTHASWAMY, THROUGH TWO DOORS AT ONCE: THE ELEGANT EXPERIMENT THAT CAPTURES THE ENIGMA OF OUR QUANTUM REALITY (Dutton 2018).

But two strange phenomena can also be observed. First, without any alteration to the experiment, carefully inspecting the screen reveals that the energy is absorbed discretely, similar to behavior of a particle. A second observation requires an alteration to the experiment. The technician uses a device that emits a single electron at a time, and leaves it running for hours. Here too, an interference pattern emerges. But how could electronics fired sequentially create an interference pattern? The experiment indicates that somehow the electron goes through both slits, thus interfering with itself.

A third tweak makes the experiment even stranger. The technician adds an electron-detecting device to "see" which slit the single electron travels through (figure 2). With the detector in place, the single-electron emitter creates a different pattern. Instead of interference bands, the pattern is consistent with the electrons being a particle: two bands corresponding to the two slits. Thus, observing the electron causes it to behave like a particle instead of a wave.

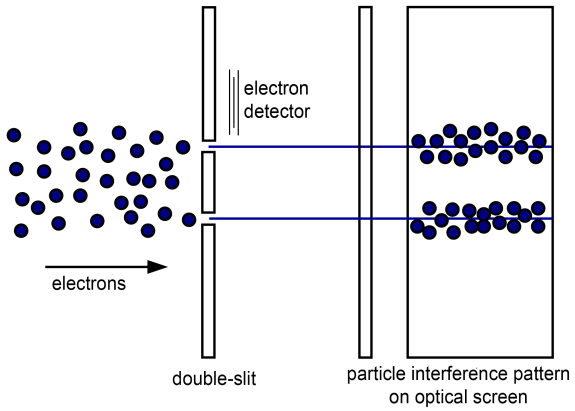

Figure 2 Adding an electron detector causes the probability wave to collapse, and the electrons act like particles instead of waves. The quantum wave behavior of the electron decoheres upon observation. Image public domain by inductiveload for Wikimedia with edits by the author.

We know now that light and electrons have the properties of both waves and particles. Quantum mechanics states that when we cannot know which slit the single photon traveled through, the photon exists as a probability wave. The electron was in a *superposition* of the different possible ways it could traverse the two slits, with the probability wave predicting where the electron is most likely to be. Quantum superposition states are both indeterminate and a combination of all possible states until observed. Once observed, in this case measured, the quantum state decoheres or collapses into a classical state of either passing through the left or right slit. In the case of the double-slit experiment, the single-electron detector "measured" the electron, causing its quantum state to decohere. The electron's path of left or right slit could be determined, and it exhibited the particle-like behavior of creating two bands of light instead of an interference pattern.

Metaphors help elucidate the strange nature of superposition. When we see white light, which is actually a combination of other visible wavelengths of light, it could be thought of as a kind of superposition. We could think of white light as being a mixture of all other colors of light, but in reality, it is our visual system that interprets this amalgam as white light.

Quantum technologies take advantage of superposition in clever ways. Consider that traditional computers are governed by classical information theory, and are limited by the affordances of the bit. A bit is binary and can be a 0 or a 1. Despite this limitation, microprocessors enable us to make sense of gigabytes or even exabytes at a time, enabling us to watch movies, communicate, and even use machine learning with consumer-grade computers.

Quantum computing operates on qubits, which are not limited to the classical 0 or 1. Qubits can be in a continuum of states—0 or 1 or somewhere between. Mastering superposition should enable a computer scientist to arrange an array of particles to compute all possible combinations of a problem. For instance, imagine having to program a computer to consider every possible chess move. A classical computer cannot possibly consider every move, so it reduces the problem to a digestible set of rounds and moves. Otherwise the gameplay would never progress. The promise of quantum is that in classical computing to solve larger problems, it increases complexity, which takes more time. Say you have N problems, conservatively it will take N time. In quantum computing the complexity of the problem is moved into the setup. If you have N problems it will take some constant X time, whether N is on the order of dozens or billions. Developers of quantum computers seek to leverage superposition and qubits so that particles could hold every possible move in every possible state of gameplay. A properly prepared QC would perform many more operations at the same time, only bound by the ability of the scientist to create, encode, and decode the qubits. This task is not so simple as we shall see.

No cloning theorem

This discussion of superposition has bled over into the next phenomenon, the "no cloning theorem." No cloning is a result of the Heisenberg uncertainty principle, which holds that it is impossible to know both the position and momentum of a quantum state with precision. Since the quantum state cannot be measured perfectly, it is also impossible to copy perfectly. Copying is a form of measurement, just like placing the single-electron detector near the slits in the double-slit experiment. Because copying measures, it collapses the quantum state.

The inability to copy upends what we expect about the world. In classical information theory, information can be copied perfectly, at least perfectly enough for most purposes. Copies, properly duplicated, read exactly the same as the original even if they are different on a quantum level. Both of these settled classical concepts are upended in quantum theory. Information cannot be copied without affecting its content, and each time identically-prepared information is read, it can produce a different outcome.

Just as superposition is key to QC, quantum's no cloning is a critical affordance for communications and encryption technology. Properly prepared quantum communications cannot be copied without introducing error, thus alerting the parties to the communication about the surveillant. As we will see, being able to know whether surveillance is present will be a key advantage to a quantum internet.

Entanglement

Entangled particles are linked, and even when physically separated with no way to communicate, entangled particles continue to exhibit concerted action. Entanglement has no analog in the classical world and it is so strange that Einstein referred to it as "spooky action."[4] One way to think of it is that entangled

[4] A. EINSTEIN, et al., THE BORN-EINSTEIN LETTERS: CORRESPONDENCE BETWEEN ALBERT EINSTEIN AND MAX AND HEDWIG BORN FROM 1916-1955, WITH COMMENTARIES BY MAX BORN (Macmillan 1971).

particles are part of a system, where measuring any part of the system reveals information about other parts.

When particles are entangled, measurement of one causes the other to act in a predictable fashion. Entanglement appears to violate relativity, because measurement causes the other particle to react instantly, faster than the speed of light, even when the particles are separated by great distances. Spooky action occurs without sending information through physical space. Thus, some literatures refer to this as quantum teleportation.[5]

Entanglement is a powerful technique that is core to QC, metrology, sensing, and communication. In QC, entanglement is used to create coordinated ensembles of particles. These ensembles combine to create exponential speedups in compute power. In metrology and sensing, an entangled photon can illuminate an object while another can be measured to learn about the target. In communication, entanglement can be used to exchange information at huge distances. As will be detailed below, in 2017, Chinese researchers maintained entangled photons at 1,200 kilometers using a satellite that communicated with two base stations.[6] The experiment foreshadows a future quantum internet, secured from surveillance by the no-cloning theorem, with information delivered instantaneously. As we will see, there are several caveats to this vision as a result of quantum affordances.

With this basic summary of superposition, no-cloning, and entanglement, we can proceed to see how clever scientists exploit these quantum affordances to provide utility in many contexts.

Applied quantum: metrology and sensing, communications, and computing

While commentators tend to think first of quantum computing, quantum technologies include many techniques that take advantage of the strange properties—superposition, no cloning, and entanglement—of very small particles. This section explains how the key affordances of quantum contribute to technologies in three domains: quantum metrology and sensing, quantum communications, and quantum computing.

Quantum metrology and sensing

The quantum world is sensitive to the smallest perturbations. Quantum metrology and sensing are clever techniques that use this sensitivity to measure things and sense phenomena. Quantum metrology and sensing most commonly rely on quantum entanglement and superposition, and their earliest applications relied on the "spin" of atoms. Entanglement enables illumination of objects by measuring a photon linked with another that is beamed against the object to be studied. Particles in a superposition state can be carefully measured to detect magnetic and electric fields, among other phenomena. These

[5] W. Pfaff, et al., *Unconditional quantum teleportation between distant solid-state quantum bits*, 345 SCIENCE 532 (2014). (Quantum state transfer between nodes containing long-lived qubits can extend quantum key distribution to long distances, enable blind quantum computing in the cloud and serve as a critical primitive for a future quantum network.")
[6] J. Yin, et al., *Satellite-based entanglement distribution over 1200 kilometers*, 356 SCIENCE 1180 (2017).

technologies are powerful, they could be miniaturized and commercialized, and their diffusion will have strategic implications.

Quantum metrology is so sensitive that it requires a recalibration of measurement standards. As this article is being written, scientists and policymakers are deliberating over how to measure the kilogram. The current standard, Le Grand K, a century old piece of platinum iridium alloy, loses and gains atoms, resulting in measurement differences in the tens of micrograms.[7] If a new proposal is adopted, the kilogram will be keyed to the Planck Constant and thus more congruent with quantum phenomena.[8]

Metrology based on quantum phenomena, such as the atomic clock, is decades old. The atomic clock uses the oscillation of atoms to count time. Since these oscillations are identical, atomic clocks around the world can be synchronized and relate perfectly matching time. Other common technology that leverage principles of quantum include Magnetic Resonance Imaging (MRI) to create images of body parts by detecting the magnetic spin of hydrogen,[9] Positron Emission Tomography (PET) which uses small amounts of radioactive material to image metabolic processes in the body,[10] and two-photon microscopy to fluoresce tissues[11] including in live animals.[12]

Modern quantum techniques such as entanglement and superposition promise new advancements through the use of quantum metrology. MRIs using quantum devices can detect with more sensitivity and increase the range of what is detectable. PET can use entangled photons to create three dimensional representations of radioactive markers. Further leveraging entanglement, two-photon techniques can image microscopic objects not viewable due to diffraction as well as possibly write on objects that are photo-sensitive.[13]

The quantum technologies discussed thus far raise few unmanageable privacy issues, because the subject of measurement must remain very still and would presumably know about the monitoring taking place. However, other uses of quantum metrology and sensing can be used against unwilling or unknowing subjects. To understand why, a diversion is necessary into trends in electronic warfare and a field known as measurement and signature intelligence (MASINT), intelligence that is based on the measurement of objects or their "signatures," such as how heat dissipates from a recently-fired weapon.

Quantum metrology is nicely posed to supplement and, in some cases, replace satellite-based Global Position Systems (GPS). GPS is provided by a network of satellites that are vulnerable to physical and electronic attack. The need is great, as military adversaries, particularly the Russian Armed Forces, have

---

[7] E. Gibney, *New definitions of scientific units are on the horizon*, 550 NATURE 312 (2017).
[8] A. Cho, *Plot to redefine the kilogram nears climax*, 356 SCIENCE 670 (2017).
[9] Abi Berger, *Magnetic resonance imaging*, 324 BMJ (CLINICAL RESEARCH ED.) (2002).
[10] Michael A. Taylor & Warwick P. Bowen, *Quantum metrology and its application in biology*, 615 PHYSICS REPORTS (2016).
[11] K. Svoboda & R. Yasuda, *Principles of two-photon excitation microscopy and its applications to neuroscience*, 50 NEURON 823 (2006).
[12] Anthony Holtmaat, et al., *Long-term, high-resolution imaging in the mouse neocortex through a chronic cranial window*, 4 NATURE PROTOCOLS 1128 (2009).
[13] Dmitry Strekalov & Jonathan Dowling, *Two-photon interferometry for high-resolution imaging*, 49 JOURNAL OF MODERN OPTICS 519 (2002).

best-in-class electronic warfare.[14] The idea is that in a conflict, Russian soldiers will befuddle our drones, missile systems, and even sea and land-faring vessels through GPS degradation or denial. To respond to these threats, the Navy has started training midshipmen on charts and sextants, but of course, if one cannot see the stars, these non-digital methods will fail too.[15]

The answer to new electronic warfare threats could come from carefully observing particles in quantum states locked within diamonds. Scientists have developed location measuring techniques using nitrogen vacancy chambers in diamonds. These are imperfections in diamonds, places where a single nitrogen atom is trapped by the strong bonds of neighboring carbon atoms, and thus relatively insulated from the outside world. The nitrogen atom can be manipulated to produce quantum effects, even at room temperature (we shall see later that other quantum phenomena require extreme cold). Shining a laser at the nitrogen atom causes it to emit light that reveals subtle variations in the Earth's magnetic field. These variations are unique and if carefully measured, can locate the device with precision greater than GPS. Properly equipped, comparisons between GPS and the quantum sensor should reveal when GPS is being jammed or degraded, and tell the operator where the vehicle is located with certainty. The nitrogen vacancy approach should also work deep below the earth's surface, in underwater caverns. A 2015 Air Force study of quantum technologies concluded that quantum navigation sensors would be ready for demonstration between 2020–2025.[16]

Interferometry devices represent another area of strategically-important quantum technology. Interferometers measure interference in light waves in order to measure phenomena, including extremely small differences in gravitational and magnetic fields. Dowling predicted an 8-fold increase in resolution for quantum devices such as satellite-based gravimetry. This would mean that oil fields and the fullness of water aquifers could be assessed from space.[17] Presumably one could also determine whether heavy matériel are camouflaged under netting or even concrete roofs. Some have speculated that the technology is sensitive enough to illuminate and measure things on other planets.[18]

Recall that entangled quantum states are linked perfectly, even over great distances. Entanglement has clear implications for sensing at a distance. Imagine generating an entangled photon pair where one is monitored in memory while sending the other into the environment. If the transmitted photon hits the body of a fighter jet, presumably the monitored half will reflect the condition of the transmitted one. Generate enough entangled photons and one could distinguish between that jet and the background of the sky.[19] The military applications of such quantum illumination for radar are many. Quantum radar can see vehicles that use stealth technology. For instance, one use foreseen by the Air Force is to use quantum

[14] Roger N. McDermott, Russia's Electronic Warfare Capabilities to 2025 (International Centre for Defence 2017).
[15] Geoff Brumfiel, *U.S. Navy Brings Back Navigation By The Stars For Officers*, NPR, February 22, 2016.
[16] USAF Scientific Advisory Board, Utility of Quantum Systems for the Air Force Study Abstract (USAF ed., 2015).
[17] Dowling & Milburn, PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A-MATHEMATICAL PHYSICAL AND ENGINEERING SCIENCES (2003).
[18] John Preskill, Q2B: Quantum Computing for Business (Keynote Address, Quantum Computing for Business 2018).
[19] Marco Lanzagorta, *Quantum Radar*, 3 SYNTHESIS LECTURES ON QUANTUM COMPUTING (2011).

technology to counter "DRFM jamming," a technique where an enemy fighter captures radar pulses and replays them at a different speed in order to confuse air defense systems.

The Chinese military has reportedly developed next-generation, sonar-like systems that can detect submarines and other underground objects based on their mass and shape.[20] In one publication key to the development, Chinese scientists suspended Superconducting Quantum Interference Device (SQUID) gradiometers from a helicopter to image underground mineral deposits.[21] If these technologies are successful, they will have strategic implications, possibly upsetting the world order reached through our nuclear triad. Consider that existing delivery mechanisms, such as ICBMs and supersonic stealth jets, are vulnerable to a series of techniques that might disrupt a first or second nuclear strike. ICBMs might be attacked "left of launch" or be intercepted by a missile. The stealth fighter has been shown not to be immune; one was apparently detected and shot down by the Army of Yugoslavia in 1991. On the other hand, submarines have remained the cornerstone of a guaranteed second strike, they in essence eliminate the ability of an attacker to mount any kind of successful nuclear war relying upon a surprise first strike. But what happens if quantum sonar degrades the secrecy of submarines and makes it possible to locate and disable them?

Quantum sensing gets stranger than radar and sonar. In quantum sonar and radar, entangled photons directly measure an object. Quantum also enables indirect measurement, by sensing how an object perturbs other things. The field of "ghost imaging" leverages quantum measurement to see things that are not in line of sight of a sensor. The U.S. Army's advances in ghost imaging could make it possible to see clearly on chaotic, turbulent, hot and smoky battlefields. Researchers could photograph an object not on the directly transmitted photons from an object, but indirectly from the scattered and reflected light from an object. The Army researchers claim the technology works on all wavelengths, meaning that shining different frequency light could reveal chemical composition of an object (perhaps revealing it to be real or a decoy).

Taken together, and even if just one or two of these technologies could reach a readiness level for deployment, quantum measurement and sensing will change how nations monitor, signal, and engage in conflict. If implemented, quantum could contribute to a core process in conflict: the speed and quality of the so called OODA loop. That is, the learning process of observing a situation, orienting oneself to it, taking a decision, and action, which might be inaction. Quantum could contribute to the observe/orient processes of the OODA loop. If we can understand and process an emerging, chaotic situation, we might be able to act before an adversary can, and we might be able to degrade adversaries' ability to observe and orient in the process.

---

[20] David Hambling, *China's quantum submarine detector could seal South China Sea*, NEW SCIENTIST, August 22, 2017.
[21] Wu Jun & Xie Xiaoming, The study of several key parameters in the design of airborne superconducting full tensor magnetic gradient measurement system (Society of Exploration Geophysicists 2016). L. Qiu, et al., *Development of a squid-based airborne full tensor gradiometers for geophysical exploration*, *in* SEG TECHNICAL PROGRAM EXPANDED ABSTRACTS 2016 (2016).

Quantum communication

Quantum measurement and sensing may lead to a "golden age" of MASINT. At the same time, the sun may be setting on our current "golden age of surveillance" for signals intelligence (SIGINT).[22] As information traverses the internet, operators of servers can log meta data about and, in many cases, even copy and examine the content of our email, photographs, and other communications. Because of this, some amount of internet traffic relies on encryption to prevent eavesdropping by intermediaries. But the most sophisticated governments can deny or degrade classical encryption, and in many cases, such as email, users typically send plain text messages. This is the equivalent of mailing a postcard, but worse because machines can read and remember many more postcards than a dishonest mail carrier.

A quantum internet changes these dynamics in three ways: First, a quantum internet would rely on fundamental technologies that make encryption more secure, such as quantum number generation and quantum key distribution. Even QC should not be able to break quantum encryption.

Second, and perhaps more interesting, is that quantum communication enables one to know when an eavesdropper is present. Currently, one must imagine a range of eavesdroppers in a threat actor analysis, and worry that one can never know whether, for instance, a government has used extreme measures to install monitoring equipment on internet infrastructure. Recent reporting has revealed that the NSA installed "splitters" to copy the light relayed at our most important internet exchanges. Nations also use submarines to tamper with intercontinental fiber optic lines. Quantum changes these dynamics, thus forcing a reexamination of the game theoretic strategy of SIGINT. If one can know whether a surveillant is present, one can change approaches.

Finally, quantum entanglement can change where communication takes "place," with implications for how governments justify interception of communications data. Currently governments see communications traversing international landing points as border crossings. The border crossing framing provides a broad rationale for surveillance: the state's traditional right to inspect people and things entering the country. A cleverly-designed quantum internet might avoid a traditional border crossing, and thus the ability and asserted right of states to inspect communications.

This section explains some of the fundamentals of quantum communication technologies, and their affordances and challenges in implementation in order to prepare the reader for a policy and legal discussion.

Quantum random number generation (QRNG)

Encryption requires the generation of large, random numbers. These random numbers form the very basis of the security provided by encryption, as ciphers are derived from the numbers. If an attacker can somehow interfere with the randomness, the attacker can make more educated guesses about the

[22] Peter Swire, *The Golden Age of Surveillance* (2015), *available at* https://slate.com/technology/2015/07/encryption-back-doors-arent-necessary-were-already-in-a-golden-age-of-surveillance.html.

cipher used to encrypt data[23] or even mount a kleptographic attack that creates a kind of back door to the communication. Quantum random number generation (QRNG) has been proven thus far to be truly random,[24] and thus could fundamentally strengthen encryption through eliminating the weakness that existing number generation is subject to error that can be exploited by sophisticated intelligence agencies. QRNG is commercially available[25] and an Australian academic group offers QRNG free online.[26]

Quantum key distribution (QKD)

The BB84 protocol demonstrates how two people can exchange encryption keys using quantum states (quantum key distribution, or "QKD") to create provably secure communication for one-time pads.[27] This is a kind of gold standard for communications security that if broadly adopted, could create substantial challenges for law enforcement and intelligence agencies that have already figured out how to degrade classical encryption.[28]

Under the protocol, Alice sends Bob a single photon, which Bob carefully measures. Alice and Bob then communicate over a classical channel (such as a phone or the internet) to discuss whether Bob's measurement of the photon is consistent with Alice's preparation of it.

Some additional details elucidate why this is consequential. In classical wiretapping, a notional eavesdropper, "Eve," "intercepts" Alice's communications to Bob. In the classical sense, "interception" means making a copy of the communication while it is in transit to Bob. Bob never knows the difference, because classical interception neither corrupts or degrades the communication.

But in quantum communications, if Eve intercepts Alice's photon, it is intercepted in the same sense as a football is intercepted: Eve ends up with the photon and the communication never happens. Of course, not getting Alice's photon may reveal presence of an eavesdropper (noise and error also "intercept" photons). But a clever Eve would capture Alice's photon and replay it to Bob. Here is where quantum's no-cloning theorem provides more security. Because of the no-cloning theorem, the Eve's interception causes error, making it apparent to Bob that portions of the key were measured when he parleys with Alice on the classical channel. That is, Eve intercepts Alice's football, tries to copy it, but ends up sending a different football to Bob. Alice and Bob can thus start over again until they exchange information free of interception. When this happens, Alice and Bob can compare portions of the communicated information; when it matches perfectly, they can use the remainder of the information as a shared key.

---

[23] Bruce Schneier, *Did NSA Put a Secret Backdoor in New Encryption Standard?*, WIRED November 15, 2007.
[24] Antonio Acín & Lluis Masanes, *Certified randomness in quantum physics*, 540 NATURE (2016);Peter Bierhorst, et al., *Experimentally generated randomness certified by the impossibility of superluminal signals*, 556 NATURE (2018).
[25] ID Quantique, *Quantis Random Number Generator* (2019), *available at* https://www.idquantique.com/random-number-generation/products/quantis-random-number-generator/.
[26] Centre for Quantum Computing and Communication Technology, *Welcome to the ANU Quantum Random Numbers Server*(2019), *available at* https://qrng.anu.edu.au/#.
[27] C. H. Bennett & G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, 560 THEORETICAL COMPUTER SCIENCE 7 (2014).
[28] Jeff Larson and Scott Shane Nicole Perlroth, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, THE NEW YORK TIMES, September 5, 2013.

Interception thwarted, Eve can still turn to other tools to interfere with Alice and Bob. For instance, because of the instability of quantum states, Eve could inject noise to deny or degrade the quantum channel and cause Alice and Bob to have to revert to other, less secure communication.

QKD is commercially available.[29] As early as 2009, three companies offered working QKD devices.[30] Yet, a U.S. Air Force advisory board threw cold water on QKD, finding that it significantly increases system complexity while providing "little advantage over the best classical alternatives."[31] The USAF's full report is not publicly available, but presumably the board meant that as system complexity increases, attackers direct decryption efforts at other vectors, such as poorly-chosen user passwords, or simple phishing.

Quantum internet

Scientists have already achieved several key steps towards the creation of a quantum internet.[32] Standing atop QRNG and QKD, a quantum internet could be immune to surveillance; at the very least, one would know when a party was attempting to monitor the network. Many countries may have strong incentives to do so given the surprising muscularity and ingenuity of the NSA as revealed by Edward Snowden.

Building a quantum web is among the explicit goals of the European Union's 1 billion Euro investment in quantum technologies.[33] However, the Chinese appear to be far ahead of everyone in quantum networking. Popular reports claim the country has a 2,000 km-long fiber network linking Beijing and Shanghai with a quantum channel.[34]

But the challenge of realizing a quantum internet is related to the very attributes that would give it so much privacy: the no-cloning properties of quantum. Scientists first implemented quantum communication over short distances, extending networks on optical fiber over a distance of about 100 kilometers.[35] Just as in ordinary fiber optic networks, light becomes diffused from the twists and turns of the fiber and needs to be "repeated," or boosted to travel to its final destination.[36] But the act of repeating requires copying, and thus the repeaters used are not truly quantum devices. Instead, just like today's network, they rely on trust. That is, these classical repeaters must decode the quantum state and relay it, giving the operators of the repeater the ability to monitor the communication. When the internet was first created, it was thought that repeaters would only forward communications, but now that storage is so inexpensive, these repeaters could copy the information before forwarding it.

---

[29] L. Oesterling, et al., Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information (2012).
[30] Valerio Scarani, et al., *The security of practical quantum key distribution*, 81 REVIEWS OF MODERN PHYSICS (2009).
[31] Board. 2015.
[32] Stephanie Wehner, et al., *Quantum internet: A vision for the road ahead*, 362 NATURE eaam9288 (2018).
[33] High Level Steering Committee, Quantum Technologies Flagship Intermediate Report (2017).
[34] Cade Metz and Raymond Zhong, *The Race Is On to Protect Data From the Next Leap in Computers. And China Has the Lead.*, NEW YORK TIMES, Dec. 3, 2018. 2018.
[35] Zhen-Sheng Yuan, et al., *Experimental demonstration of a BDCZ quantum repeater node*, 454 NATURE (2008).
[36] H. J. Briegel, et al., *Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication*, 81 PHYSICAL REVIEW LETTERS (1998).

Repeater node trust could be seen as a blessing or a curse—depending on one's perspective, it either can enable lawful access to otherwise unbreakable communications, or it represents a security loophole so problematic that one should remain on classical encryption techniques, which remain scrambled even when boosted. Still, even a classically-relayed quantum network is advantageous, in that if one controls the relay points, one could detect interception and still enjoy lawful access when needed. For instance, the political attributes of China probably fit neatly with the limits of classical repeaters. Those nodes could be operated by the military, and surveilled when desired by domestic law enforcement and intelligence, while denying that same ability to foreign adversaries. In the U.S., the private ownership of so much of the internet infrastructure suggests a different outcome: that classical repeaters will carry all the existing confidentiality degradations of our current internet—operator interception, businesses uses of others' internet traffic, and so on.

Research teams have demonstrated increasingly impressive quantum internet achievements. A team at TU-Delft used nitrogen vacancy chambers (the same imperfections in diamonds described above to measure magnetic fields) that trap electrons. The Delft team excited the electrons with a laser, causing the release of a photon. When measured, the electrons' spin were correlated more than 75% of the time despite being more than a kilometer away.[37]

Since then, Chinese scientists demonstrated entanglement at 1,200 kilometers by using its Micius satellite that beamed linked photons to two base stations.[38] The entangled photons guaranteed secure communication at a distance—for the 5 minutes or so that the satellite's cone covered the stations. The $100 million project is part of the Quantum Experiments at Space Scale program (QuESS), and has demonstrated a substantial goal in the space. Yet, it still faces many challenges. The Chinese team had to beam millions of photons a second to maintain the link, and only a handful reached the base stations because of atmospheric and other interference. But one could imagine a satellite network enabling global point-to-point quantum communication that is then relayed by space and terrestrial (including oceanic and even underwater) devices. To demonstrate that vision, Chinese scientists secured a videoconference from Beijing and Austria, a distance of over 7,000km, using a satellite that beamed a quantum key to stations between the two locations.[39]

Taken together, developments in QRNG and QKD afford determined and technically-sophisticated actors the ability to create rudimentary quantum networks based on classical repeaters. But the next steps are more consequential. Work is underway to invent quantum memory that could relay the communication without copying it, preserving its quantum nature and protection against cloning. This first step would secure intermediary points against interception, an important step towards guaranteed secure communications.

---

[37] B. Hensen, et al., *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres*, 526 NATURE (2015).
[38] Yin, et al., SCIENCE (2017).
[39] Sheng-Kai Liao, et al., *Satellite-Relayed Intercontinental Quantum Network*, 120 PHYSICAL REVIEW LETTERS (2018).

Once that feat is accomplished, a second one could occur that has even greater consequences. Recall that photons can be entangled and shared between two entities. When entangled, the photons operate as a linked system, where one photon's spin and polarity is linked to the other instantaneously, even if separated by long distances. If teleportation can be managed resiliently, why couldn't information be teleported instantly, thus faster even than the time it takes light to travel through the internet's tubes? There would be strong commercial incentives to do this, because even the tiny delays imposed by traversing fiber networks can affect computer security (for instance, when two distant computers must be kept in sync) or give slight advantages (or disadvantages) to those trading securities. Turning to communications privacy, teleportation would enable Alice and Bob to communicate without their communication being intermediated by physical infrastructure or repeaters. It is that physicality that governments use as a justification for intercepting communications. That is, the US government uses the border search doctrine to justify sweeping monitoring of international communications. But the development of quantum teleportation could deny governments both the technical ability and legal rationale (border search) used for interception. This and other implications of a fully-quantum network are detailed below.

Quantum computing

The hype and high stakes of quantum computing ("QC") make the topic difficult to study and to generalize about. Classical computing is based on the silicon chip, and we have decades of experience and benchmarks to make sense of the performance differences of classical computers. In QC, research groups use different technologies with different affordances and uses. Benchmarking QC requires consideration of several factors considered inconsequential in classical computing. This part begins by distinguishing three kinds of QC and then turns to the enormous technical challenges faced in developing a general-purpose QC. The challenges are so great that some think QC will arrive, but even if it does, the difficulty of the venture shapes who is likely to have QC, how it is likely to be used, and the practical ability of adversaries to interfere with it. This part concludes with a discussion of QC applications and their likely effects on the confidentiality, integrity, and authenticity of data.

Three kinds of QC

At least three categories of QC have emerged, and the attachment of "quantum" to them creates a confusing landscape, as each kind of technology has different characteristics. The Quantum Computing Report, a website run by an enthusiast, offers one of the most comprehensive surveys of the different quality and technical approach claims.[40]

First, some researchers are using classical computers to simulate QC. Quantum simulators can produce quantum-like effects without the complications (discussed below) raised by general-purpose quantum computers. It is hoped that simulation will enable both optimization of physical materials and testing of unfathomable combinations of chemicals in systems. Currently drug companies discover the

[40] Doug Finke, *Qubit Count* Quantum Computing Report(2018), *available at* https://quantumcomputingreport.com/scorecards/qubit-count/.

effects of new compounds by manually testing them in massive arrays. As you read this, machines full of petri dishes agitate materials collected from forests and oceans in search of promising interactions. A sufficiently complex and prepared quantum simulator could perform similar functions to benefit chemistry, physical design, and materials science. Such a quantum simulator would pay dividends in testing every possible permutation of a drug's molecules, or the shape of an airplane's frame, in order to find the best design possible.

Second, a field known as "analog quantum" concerns machines that achieve quantum effects in specially-prepared materials. D-Wave System's quantum annealer is the most well known device in this category. A quantum annealer uses a metal material that exhibits quantum properties as it is cooled. Unlike a general purpose QC, which uses gates to process qubits, the annealing process directly manipulates qubits. Annealing is uniquely well suited to optimization problems.

D-Wave Systems commercially offers a 2,000-bit quantum annealer, and this makes it appear to be far ahead of competitors in QC. However, quantum annealers are limited in function, and D-Wave's 2,000-bit machine will never be able to achieve the functionalities envisioned in general purpose QC. Furthermore, it is not clear that annealing can outperform classical computers configured to address optimization problems.[41] Yet, companies are investing in the technology, perhaps simply to start to think about the world and work from a quantum framework.

Finally, QC's holy grail is to develop a general-purpose device, one that can run panoply of algorithms very quickly and with manageable error. A true quantum computer will process an algorithm by manipulating qubits with gate functions. But as the next section explains, this is not so easy. The National Academies of Sciences characterizes today's QC as digital noisy intermediate-scale quantum (NISQ) devices.[42] NISQs have "primitive" gate operations manipulating physical qubits and are plagued by error and decoherence.

Quantum computing depends on getting everything right

Quantum computing depends on a number of technical feats. As of 2018, the National Academies of Science characterized the field as consisting of creating small, proof-of-concept demonstration devices.[43] This is because quantum computing requires a mastery of quantum superposition and entanglement, development of software and control systems, and management of costly, difficult physical conditions. A 2003 quantum technology overview by Dowling et al. noted that, "A solid-state quantum computer is

[41] ENGINEERING NATIONAL ACADEMIES OF SCIENCES & MEDICINE, QUANTUM COMPUTING: PROGRESS AND PROSPECTS (Emily Grumbling & Mark Horowitz eds., The National Academies Press 2018). ("…recent results…have shown that algorithms for classical computers can usually be optimized to the specifics of the given problem, enabling classical systems to outperform the quantum annealer.).
[42] NATIONAL ACADEMIES OF SCIENCES & MEDICINE. 2018.
[43] NATIONAL ACADEMIES OF SCIENCES & MEDICINE. 2018.

probably the most daunting quantum technological challenge of all and will require huge advances in almost all the areas of quantum technology we have discussed."[44]

Quantum computers are characterized by the integration of multiple qubits. For a quantum computer to work, one needs to be able to encode, manipulate, and maintain qubits. These functions require substantial technical expertise, reflected in the multidisciplinary nature of quantum computing teams (physicists, mathematicians, computer scientists, materials science).

QCs are plagued by decoherence—the information encoded into qubits can be lost, thus limiting the number of sequential operations that can be performed. Quantum computers require that their qubits be entangled, cohered into a group that can be operated upon. Quantum algorithms have to be crafted to be efficient enough to execute before coherence is lost, and this is challenging in part because quantum gates take time to execute. As of this writing, coherence is measured in hundreds of microseconds, a time too short for many quantum gates to process qubits. This is a time period so short that human experience has no analogue for it. A blink of the eye takes about 100,000 microseconds.

Significant work still needs to be done to create an ecosystem of quantum software, from a basic programming language to compliers. On the software front, many teams are developing languages to make interaction with quantum computers more routine and standardized. As of 2016, growing "zoo" of quantum algorithms included 262 papers.[45] Yet, even if tools exist to process information, it still is not clear how classical information—such as all those encryption keys that will be rapidly decrypted—can be converted into a quantum state. With current limitations, large datasets cannot be read in to a quantum computer in the short time that devices decohere.

Quantum computers need to be kept cold, colder than even the background temperature of the universe. Extreme frigidity is needed both to elicit quantum properties from materials (for instance, in analog quantum) but also because heat increases the chances that random energy collisions will generate noise that will interfere with quantum states or cause decoherence. Keeping quantum devices at 15 millikelvin (-273 degrees Celsius, -459 Fahrenheit) means that quantum computer scientists need liquid helium, an increasingly rare and valuable element, of which there is a finite supply of on Earth. There are current no limits on the usage of Earth's helium supply and an expectation that self-sustaining nuclear fusion, which would create helium via hydrogen fusion, will be solved before the Earth's supply runs out. Other quantum technologies do not require extreme cold, and this factor alone will determine what quantum technologies can be miniaturized.

Quantum computers are not fault tolerant. In addition to temperature, vibration and electromagnetic interference can easily destabilize quantum computers. Once error occurs, quantum

[44] Dowling & Milburn, PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A-MATHEMATICAL PHYSICAL AND ENGINEERING SCIENCES (2003).
[45] Ashley Montanaro, *Quantum algorithms*, 2 NPJ QUANTUM INFORMATION (2016);S. Jordan, *The quantum algorithm zoo*, *available at* http://math.nist.gov/quantum/zoo/.

devices are more sensitive to it. Consider that in classical computing, bits of data are either 0s or 1s. In that environment, error can be easily rounded to 0 or 1. Qubits have continuous variables, and thus cannot be rounded as easily as a binary classical bit.

The longer quantum devices run, the more performance degrades. Initially, one might suggest just adding more qubits to achieve reliability, but as more qubits are added, quantum devices become more prone to environmental interference. In classical computing, extra bits are used to correct ordinary errors that occur in processing. In quantum, many of the qubits employed are dedicated to error correction, so many that it creates significant overhead and degrades computing performance. As much as 90% of quantum resources might be dedicated to error correction.[46]

Taken together, these limits will shape the trajectory and offerings of quantum devices. Because of their expense and complexity, only large firms and governments are likely to be able to afford them. They are unlikely to be mounted in jets or submarines for forward-deployed use. Relatedly, larger firms are likely to offer quantum processing through the cloud until fundamental physical challenges are overcome and quantum devices reach a price point available even to medium-sized enterprises. Until then, quantum is likely to be offered as an enhanced service, one optimized for specific problems.[47]

A series of other strategic implications flow from these limitations. The need for liquid helium suggests that until quantum states can cohere at warmer temperatures, the presence of quantum computing could be inferred through supply channel surveillance of helium consumption. Additionally, the fragility of quantum states suggests that electronic warfare will play a role in conflict with adversaries.

Figure 3 A helium store outside Lewis Hall

Limits also come from our understanding of the quantum world. Since we have no natural day to day experience of it, quantum is counterintuitive, and we have only scratched the surface of its implications. Currently we envision quantum technologies through classical analogies and through the lens of the classical mechanics world. Imagine instead starting from a quantum frame. As quantum is better understood and intuited, its applications could be revolutionary.

Still, some argue that quantum computing will never be achieved; in fact some claim that quantum computing as a field is near its end. Physicist Mikhail Dyakonov summarized the challenges in a 2018 piece: "Such a computer would have to be able to manipulate—on a microscopic level and with enormous precision—a physical system characterized by an unimaginably huge set of parameters, each of which can take on a continuous range of values. Could we ever learn to control the more than 10^{300} continuously

[46] Matthias Möller & Cornelis Vuik, *On the impact of quantum computing technology on future developments in high-performance scientific computing*, 19 ETHICS AND INFORMATION TECHNOLOGY 253 (2017).
[47] Möller & Vuik, ETHICS AND INFORMATION TECHNOLOGY (2017).

variable parameters defining the quantum state of such a system? My answer is simple. *No, never.*"[48] A chorus of other commentators have downplayed quantum computing as an overhyped phenomenon. In 2015, a USAF advisory board found that technology advocates "herald[ed]" imminent breakthroughs but nevertheless, "no compelling evidence exists that quantum computers can be usefully applied to computing problems of interest to the Air Force."[49] The most specific critique comes from a 2018 National Academy of Sciences (NAS) survey of the field that made both economic and technological assessments. On the economic front, the NAS group observed that there are essentially no commercial uses for quantum computers (and obviously no consumer ones either). Without feasible commercial uses, funding for quantum computing is likely to be limited to governments and the largest technology companies. As such, quantum computing may lack a "virtuous cycle," like what was enjoyed with classical computers, with increasing commercial and consumer utility driving demands and willingness to pay for fantastic technological innovations. The NAS' technological critique is related to points related above surrounding the technical challenges of coordinating many qubits and managing error.[50] As a result of these challenges, NAS found it too uncertain to predict when a scalable quantum computer would be invented and that existing devices could never scale into general-purpose machines.

Quantum computing applications

Despite all these challenges, governments, large technology companies (Google, Microsoft, IBM, Fujitsu, Toshiba), have devoted major resources to QC and several startups (Rigetti, Xanadu, IonQ, Inc) are betting the company on it. Competition has produced wonderful resources to learn about and even experiment with quantum computing. For instance, IBM and others have made instructional videos, extensive, carefully curated explanatory material, and even made rudimentary quantum computers available through the cloud for anyone to tinker with.[51]

Interestingly, the idea of QC came from physicist Richard Feynman. Feynman's insight, delivered in a conference address, was that a classical computer could never simulate the complexity of particles governed by quantum physics. Thus, he challenged computer scientists to create a quantum mechanical computer, one sufficiently powerful to simulate atoms and complex biological systems.[52] Shortly thereafter, David Deutsch articulated a model for a universal quantum computer.[53]

Through leveraging superposition and entanglement, a general-purpose QC could achieve unconceived of performance compared to classical computers, at least when performing certain functions. In classical computing, complex problems are often divided up into subcomponents and processed serially, in parallel, on many computers. A properly tuned quantum computer would be able to consider every

[48] Mikhail Dyakonov, *The Case Against Quantum Computing*, IEEE SPECTRUM Nov. 15, 2018. 2018.
[49] Board. 2015.
[50] NATIONAL ACADEMIES OF SCIENCES & MEDICINE. 2018.
[51] IBM, *IBM Q Experience*, *available at* https://quantumexperience.ng.bluemix.net/qx/editor.
[52] R. P. Feynman, *Simulating Physics with Computers*, 21 INTERNATIONAL JOURNAL OF THEORETICAL PHYSICS 467 (1982).
[53] David Deutsch, *Quantum theory, the Church–Turing principle and the universal quantum computer*, 400 PROCEEDINGS OF THE ROYAL SOCIETY OF LONDON. A. MATHEMATICAL AND PHYSICAL SCIENCES 97 (1985).

possible arrangement of a complex problem because of superposition. This ability to encode all possible results sometimes termed *quantum parallelism*.[54] Such parallelism avoids the inefficiency caused by serial problem solving because "simultaneity [is] built into its very nature."[55]

A second affordance is worth mentioning here: Quantum computers are "reversible."[56] In classical computing, debugging occurs linearly, from the beginning to the end of the program. A reversible computer should be able to "go backwards" through its processes. This will have important applications in algorithmic fairness and other concerns with deep learning. By reversing the decision-making process, perhaps one could learn where unfairness is introduced into a model. In 2018, D-Wave Systems announced that it had developed a reverse annealing protocol.[57]

Quantum algorithms and encryption

A quantum computer's performance will depend on many factors, and will outperform classical computers in some situations. We might think of quantum computing as a tool that fits certain problems very well. For instance, classical computers are inefficient for factoring very large numbers, a task that increases exponentially in time with larger numbers.[58] Because of this inefficiency, RSA encryption and other schemes rely upon the exchange of very large prime numbers which are used to generate encrypted text. Because of the inefficiency, even if one combined all the computing power known, it would still take thousands of years to discover the factors used to create ciphertext.

Peter Shor theorized that quantum computers could overcome the inefficiency of factoring, thereby leading to an inconceivable loss of confidentiality and privacy.[59] Factoring is the kind of problem that is well suited to quantum computers, one that quantum computers could perform in polynomial time—about the same as it takes a classical computer to do basic math.[60]

The popular press heralds an end to confidentiality as a result of Shor's algorithm. However, a large-scale application of this algorithm is far off.[61] Even when it arrives, unless fundamental challenges in

---

[54] Möller & Vuik, ETHICS AND INFORMATION TECHNOLOGY (2017).
[55] Lov K. Grover, *Quantum computing*, 39 SCIENCES 24 (1999).
[56] Möller & Vuik, ETHICS AND INFORMATION TECHNOLOGY (2017).
[57] Trevor Lanting, Next Generation QA Hardware (2018).
[58] Möller & Vuik, ETHICS AND INFORMATION TECHNOLOGY (2017).
[59] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, 26 SIAM JOURNAL ON COMPUTING 1484 (1997).
[60] Möller & Vuik, ETHICS AND INFORMATION TECHNOLOGY (2017).
[61] Google scientists explain that to factor a strong key in a day, "would take 100 million qubits, even if individual quantum operations failed just once in every 10,000 operations." See also Dyakonov, IEEE SPECTRUM. 2018.("Experts estimate that the number of qubits needed for a useful quantum computer, one that could compete with your laptop in solving certain kinds of interesting problems, is between 1,000 and 100,000. So the number of continuous parameters describing the state of such a useful quantum computer at any given moment must be at least $2^{1,000}$, which is to say about 10^{300}."); NATIONAL ACADEMIES OF SCIENCES & MEDICINE. 2018.("…to create a quantum computer that can run Shor's algorithm to find the private key in a 1024-bit RSA encrypted message requires building a machine that is more than five orders of magnitude larger and has error rates that are about two orders of magnitude better than current machines, as well as developing the software development environment to support this machine." This report continues to asses that it is "highly unexpected" that a quantum computer that can break a 2,000-bit RSA key will be built within 10 years.) M. Mohseni, et al., *Commercialize early quantum technologies*, 543 NATURE 171 (2017);ASCR Workshop on Quantum Computing for Science. No. SAND2015-5022R; Other: 594789 United States 10.2172/1194404 Other: 594789 SNL English, pt. Medium:

quantum computers are addressed, relatively few entities will even have the capability to decrypt. Among those that do, each key will have to be broken separately. Suffice it to say, your email and credit card numbers won't be high on the list for decryption. Nation states will have voluminous numbers of strategically-important material to process first, including archived signals intelligence from yesteryear's conflicts.

Other kinds of encryption are degraded by Grover's algorithm. Grover's algorithm, first described as a mechanism to find an element in a database more efficiently than a classical computer,[62] can also be applied to other information problems. Grover's algorithm provides a quadratic increase in compute, because using it a quantum computer can solve a problem using fewer steps. Fewer operations mean that quantum computers could attack a 256-bit key with just 2^{128} operations instead of 2^{256}.[63]

Yet like Shor's algorithm, significant technical problems have to be surmounted with applications of Grover. Grover operations have to be performed serially, and thus there is a chance that its speed improvements "will be wiped out by the overhead of qubit operations being more expensive than bit operations, making Grover's algorithm useless—even if scalable quantum computers are built and run Shor's algorithm successfully."[64]

Still, whether we use quantum encryption or some resistant form of classical encryption, attackers rarely exploit the encryption itself. A summary of a 2015 study prepared for the Air Force concluded that quantum encryption would be more complex and offer no advantages over classical techniques.[65] Presumably the study authors concluded this because attackers exploit "side channels," anything from leaking heat from a system that gives clues to content or more simply, by fooling users into giving up their passwords. No encryption can protect users who make errors.

Law and policy for the second quantum revolution

This part turns to the legal and policy issues raised by the special affordances of quantum metrology and sensing, communications, and computing. It intends not to answer these questions, but rather to elucidate the landscape of probable areas of conflict.

Quantum strategic implications

This article argues that quantum computing has distracted the public from other consequential quantum technologies. When we instead focus on metrology, sensing and communications, scientists have gone beyond proof-of-concept phases into implementation and even commercial availability. Part XXXX

ED; Size: 59 p. (2015).("Although no proof has been obtained, mathematical evidence strongly suggests that neither quantum nor classical computers can solve worst-case NP-hard problems in polynomial time.").

[62] Lov K. Grover, A fast quantum mechanical algorithm for database search (ACM 1996).

[63] Daniel J. Bernstein, Grover vs. McEliece (Springer Berlin Heidelberg 2010).

[64] D. J. Bernstein & T. Lange, *Post-quantum cryptography*, 549 NATURE NATURE (2017).

[65] Board. 2015.