Law and Policy for the Second Quantum Revolution

Chris Jay Hoofnagle[1]
[Word Count: 20,000]

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)[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 quantum computers foresee awesome innovations. Leading companies such as IBM emphasize the fit between quantum computers 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 quantum computers, 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 quantum computers to solve intractable problems in machine learning imposed by the limits of classical computers. Such developers assume that *quantum parallelism* (see below

[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).

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 quantum computers to break the most sophisticated encryption available today, leading to drastic problems with data confidentiality, data integrity, and authenticity of identity. It is true that some encryption will become vulnerable if reliable quantum computers are 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 quantum computing 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 quantum computing 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 quantum computing 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 quantum computing.

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.

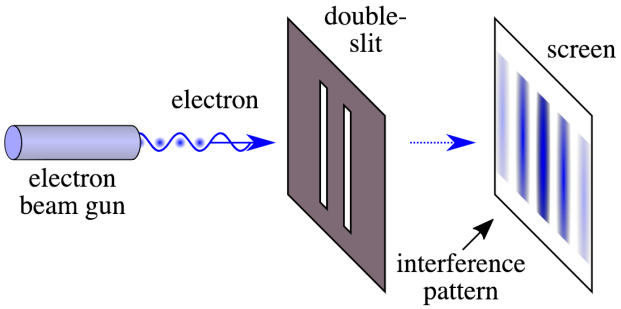

Figure 1 The initial setup of the double-slit experiment. The interference pattern suggests that the beam is a wave. Adjustments to the experiment show that light has wave/particle duality. Image public domain by Johannes Kalliauer for Wikipedia.

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

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

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.

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.

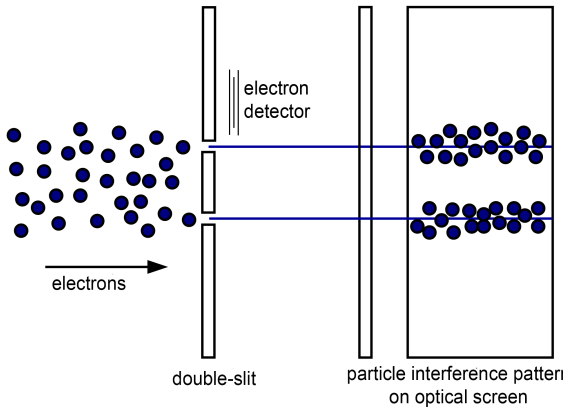

Figure 2 Adding an electron detector causes the probability wave to collapse, and the electrons act like particles instead of waves. The quantum wave behavior of the electron decoheres upon observation. Image public domain by inductiveload for Wikimedia with edits by the author.

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 quantum computer 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 quantum computing, 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 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 quantum computing, metrology, sensing, and communication. In quantum computing, 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

[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).
[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).

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 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]

---

[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).

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 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

[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).

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 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

[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).
[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).

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.

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 quantum computing 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

[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.

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 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.

---

[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.

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.

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

[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.

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.

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

[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).
[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).

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.

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 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 quantum computing, research groups use different technologies with different affordances and uses. Benchmarking quantum computing requires consideration of several factors considered inconsequential in classical computing. This part begins by distinguishing three kinds of quantum computing and then turns to the enormous technical challenges faced in developing a general-purpose quantum computer. The challenges are so great that some think quantum computers will arrive, but even if it does, the difficulty of the venture shapes who is likely to have quantum computers, how it is likely to be used, and the practical ability of adversaries

[39] Sheng-Kai Liao, et al., *Satellite-Relayed Intercontinental Quantum Network*, 120 PHYSICAL REVIEW LETTERS (2018).

to interfere with it. This part concludes with a discussion of quantum computing applications and their likely effects on the confidentiality, integrity, and authenticity of data.

Three kinds of quantum computers

At least three categories of quantum computers 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 quantum computers. 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 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 quantum computer, 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 quantum computing. 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 quantum computer. 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, quantum computing'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.

---

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

[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.).

The National Academies of Sciences characterizes today's quantum computers 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 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).

quantum computers 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

[42] NATIONAL ACADEMIES OF SCIENCES & MEDICINE. 2018.
[43] NATIONAL ACADEMIES OF SCIENCES & MEDICINE. 2018.
[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/.

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 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

[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).

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 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 quantum computing 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]

---

[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.

Interestingly, the idea of quantum computing 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 quantum computer 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 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

[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).
[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).

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 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

---

[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: 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.

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. The method is comparative: this part highlights the legally-consequential differences between classical and quantum technologies. Since the implications are so large, this part elucidates the landscape rather than attempt to solve the tensions that arise. To set the stage, this part begins with a discussion of quantum's strategic implications for nation-state conflict, and then explains how nations will attempt to interfere with others' use of quantum. It then turns to the highest-level policy issues surrounding quantum: how nation states should shape development of quantum through industrial policy and openness norms, whether quantum technologies can be lawfully used in space, quantum's effects on cybersecurity and countermeasures, and the implications of quantum-enhanced machine learning.

Quantum strategic implications

This essay 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 above introduced these technologies, along with some of their implications. This section makes the most consequential implications of quantum metrology, sensing, and computing more explicit and the next section surfaces possible policy responses.

The strategic landscape

Quantum metrology and sensing will enable dramatic improvements in intelligence, surveillance, and reconnaissance, and these improvements will have both strategic and tactical value. Take interferometry, for instance. Interferometry can detect gravimetric abnormalities from space.[66] Countries with space and quantum programs thus could use satellites to detect other nations' underground natural resources, but also matériel. Quantum detection power exceeds classical abilities, because camouflage (tin-rooved airline hangers, concrete domes, or inflatable structures) can obscure heavy matériel, but it will still bend the light in an interferometer. Commercial uses of the same technology will focus on detection and evaluation of natural resources, which of course can become the topic of competition between nation states.

Turning to quantum illumination, enhanced radar and sonar erode assumptions in conflict: that our stealth aircraft are (almost)[67] undetectable and our that our submarines operate in near secrecy. The speed and stealth of aircraft, and the stealth and survivability of submarines guarantees nations' ability to make a "second strike" in a nuclear conflict; submarine-based systems are also part of the US' tenuous

[66] See e.g. National Aeronautic and Space Administration, *Laser Interferometer Space Antenna*, *available at* https://lisa.nasa.gov/index.html.
[67] See Yugoslavia's successful 1999 attack on a F-117A.

strategy to intercept first strikes. Upsetting these assumptions with quantum radar and sonar endangers key aspects of nuclear deterrence strategy.

Two other military innovations point to quantum sensing as a consequential technology. First, increasingly conflict can be waged at great distances and at hypersonic speed. Nations have developed hypersonic missiles and even railguns capable of firing over a hundred miles. These weapons create a different strategic landscape, both because of their speed and because their use will occur with even fewer warning signs than ballistic missiles. Quantum-enhanced sensing may provide earlier warning signs when these weapons are used. Second, developments in electronic warfare will change how conflict is waged. Consider that in recent conflicts, the Russian Armed Forces have been able to test out their electronic and cyber warfare capabilities, showing them to be clever and capable. Both speed of conflict and the presence of electronic warfare will drive the need for miniaturized quantum devices to supplement jamming-prone GPS navigation.

Part XXXX above detailed the affordances of quantum communications. While quantum metrology and sensing will increase MASINT capabilities, quantum communications will complicate our current, golden age of SIGINT. That is, our current, classical internet is easy to wiretap, giving nation-states unprecedented ability to monitor people. A quantum internet would provide encryption that is unhackable and, importantly, would indicate the presence of surveillance to the users.

Not only might communications be more difficult to surveil, the legal rationales for doing so may also weaken. The US government might justify broad electronic interceptions at the border relying on the border search exception to the Fourth Amendment,[68] or by intercepting them outside the US from fiber optic paths.[69] Sovereign nations have the right to control who and what passes into a country, and there are reasonable rationales for governments to inspect and prohibit some international data transfers. The problems with the border search rationale include that data are rarely as dangerous as physical objects, and that users cannot control the paths of their communications, thus the internet's route-choosing protocol can cause entirely domestic communications to leave a country, or even circle the globe.[70] As these communications leave national borders, many other countries can take a peek at them.

Quantum could upset governments' search rationale in two ways. First, if quantum repeaters are invented, the network could provide teleportation between endpoints, thus eroding both nation-states' legal authorities and ability to intercept data based on border crossing. Quantum teleportation would provide point-to-point communication between two people, but without a physical connection between them. Once teleportation is established, the endpoints could communicate through "spooky action," with no information traversing a border, and thus no "place" to intercept it except at the endpoints.

---

[68] Orin Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285 (2015).
[69] Susan Landau, *Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations*, 11 IEEE SECURITY & PRIVACY 54 (2013).
[70] Kerr, STAN. L. REV. (2015).

Second, as with metrology and sensing, quantum communication can be satellite-based. Until quantum repeaters are invented, one could foresee a satellite network that routed international communications in space, only beaming data back to earth to a specific country. Because the medium is photonic, data can be received even underwater,[71] opening opportunities for other kinds of stealthy relaying.

A wealth of strategic implications would flow from the development of a general purpose, fault tolerant quantum computing. Popular reporting invoke quantum computing's potential to render encryption useless. But these claims have to be evaluated in context to understand their likely effect. Understood properly, some encryption is indeed vulnerable, some is merely degraded, and some unaffected by quantum computing. Most vulnerable is the encryption used to secure credit card transactions, to secure internet sessions, and to sign software packages and documents.

Of course, the entities with the know-how and resources to build a quantum computer won't be interested in your credit card number. Nation-states are much more likely to use quantum computing to falsely sign software updates and to forge documents. This is because with a single software update, a sophisticated attacker can "own" a device and capture all information from it instead of laboriously decrypting individual files and communications.[72] A malicious update allows the attacker to "own" the device as a regular user, and thus avoid the time intensive requirements of investigating a suspect through their communication logs or through interviewing people who conversed with the suspect.[73]

Turning to forged documents, imagine a future where nation states go "digital first" with documents of record. Estonia has done so, meaning that the nation's official document of record is computerized rather than on paper.[74] As nations implement similar e-government rules, they become susceptible to integrity attacks where an adversary could create chaos by subtly altering these records. Just as quantum computing can be used to falsely sign software updates, the same integrity protocols are used for signing documents. Thus, imagine if an adversary changed property lines, ownership records or taxes, or even revised another nation's laws by forging the certificates that guaranteed the authenticity of information. We have long lived in a world with fake news,[75] but what if we also lost bearings on the fundamental integrity of legal processes with "fake law"?

---

[71] Photonic transmissions could carry more data, be encrypted, and make is possible to communicate with submarines. This may change the "lone wolf" strategy of submarine operation. Marco Lanzagorta, Envisioning the Future of Quantum Sensing and Communications (Quantum Sensing and Communications, NASEM Intelligence Community Studies Board August 23, 2018). Elsa B. Kania & John K. Costello, Quantum Hegemony: China's Ambitions and the Challenge to U.S. Innovation Leadership (Center for a New American Security 2018).

[72] T. Li, et al., Security attack analysis using attack patterns (2016).

[73] Timothy Vidas, et al., All Your Droid Are Belong to Us: A Survey of Current Android Attacks (2011).

[74] Nathan Heller, *Estonia, The Digital Republic*, NEW YORKER December 18, 2017.

[75] PLUTARCH, THE PARALLEL LIVES § 10 (Loeb Classical Library edition ed 1921). (Plutarch describes the mob massacre of 2nd century reform politician Tiberius Gracchus and supporters by patricians who were enraged by false accounts that Tiberius sought a crown.)

Aside from threating encryption, quantum computing will have a host of other consequential uses. Competitors investing in quantum computing are focused on simulation of quantum mechanical events, in order to develop drugs, new synthetic materials, and engage in high-energy physics experiments. Some see quantum computing as a tool in discovery of the basis of superconduction at normal temperatures and even nuclear fusion. Others are focused on quantum computing's parallelism as a mechanism to build machine learning tools that can make sense of an unfathomable number of variables.

Quantum disruption, denial, degradation, destruction, and deception

Combined these technologies will have real consequence for nation-state conflict, such that they may affect strategy at the high level. Indeed, military scientists refer to quantum sensing and communications as the "atomic bomb" of information theory, and urge us to contemplate a quantum "strategic surprise."[76]

If the implications of quantum are so great, adversaries will turn to quantum disruption, denial, degradation, destruction, or deception ("D5") tactics.[77] Experimental work suggests effective D5 tactics. For instance, the Chinese scientists who achieved satellite-based quantum entanglement and communication had to generate millions of photons in order to overcome channel loss. The scientists had to manage beam diffraction, pointing error, and absorption and turbulence caused by clouds and the atmosphere generally. This raises two vital points: first, interference similar to ordinary atmospheric events—even sunlight—can degrade quantum technologies based on photonics. Thus natural events might be simulated to stealthily interfere with the technology. We could imagine weather control as a key technology development not just for agriculture but also for D5 tactics. Second, there is very little photonic loss in space, thus, the researchers would place their satellite in high orbit—much higher than the low earth path used in the experiment, and perhaps out of reach of even a superpower. One could imagine escalation and even a desire to develop space-based weapons in response.

Yet, each application of quantum is differently vulnerable to D5. Several quantum technologies are uniquely resistant to existing D5 tactics and are being evaluated to operate in their presence. Quantum clocks and location devices are seen as supplements to jamming-vulnerable GPS, and to guard against DRFM jamming. The miniaturization of these technologies focuses on developing missile-sized components, giving us some hint of the military's intentions.

Quantum interferometry and communications can be satellite based, and thus the physical devices are out of reach of most nations' ability to physically destroy them. Interferometry, because it is detecting gravimetric waves, appears to be invulnerable to most D5 tactics. With powerful quantum intelligence, surveillance, and communications on satellite platforms, quantum technologies may increase pressure to

[76] Lanzagorta. August 23, 2018.

[77] CARLO KOPP, CLASSICAL DECEPTION TECHNIQUES AND PERCEPTION MANAGEMENT VS. THE FOUR STRATEGIES OF INFORMATION WARFARE (2005).

use military force in space.[78] Adversaries of the handful of countries that both have space programs and quantum achievements thus might invest in anti-satellite weapons. They might find it irresistible—or simply necessary—to destroy satellites in order to impair reconnaissance powers and communication routes.

Quantum illumination enhances radar at a very low energy level, suggesting it will not be as susceptible to traditional jamming efforts. Recall that quantum radar involves sending an entangled photon into the sky to detect missiles and jets. Thus like photonic communication, methods that interfere with the generation of entangled photons and that scatter them in the atmosphere may be effective to counter quantum illumination.

Quantum communications security is likely to be less consequential than metrology and sensing developments. This is because D5 tactics can be directed at other aspects of communications activities. Encryption itself is almost never the weakest link in communications. Classical encryption already affords great security, so much so that attacks focus on other aspects of communication to gain access. Computer scientists have developed extremely clever "side channel attacks," those that detect information based on the implementation of some presumably secure system. These might include detecting subtle power or frequency variations when a computer codes 0 or 1. Attackers also know that human deception is relatively easy and simple phishing attacks work

Far more interesting than communications confidentiality is the awareness of surveillance that quantum communication affords. Recall that because of the no-cloning theorem, Alice and Bob can know if Eve is attempting to understand their communication. It is too early to say how nation states will react to this signaling. One could imagine D5 strategies that attempt to poison the channel by engaging in constant attempts to intercept or block photons. Perhaps Alice and Bob can never generate a secure key if intelligence agencies create enough listening points that generate error in QKD. Another D5 scenario would be to simply allow Alice and Bob to communicate, and then attack their devices after the fact. On the other hand, if denial or degradation of terrestrial-based fiber networks becomes routine, nation states could make their communications harder to reach through using point-to-point satellite QKD.

Finally, it is not clear how D5 tactics will limit quantum computing. For the foreseeable future, quantum computers will be large, intricate and delicate devices. They will be terrestrially-based, in places where human expertise, a lot of electricity, and supercooling helium is available. While these limitations do not suggest D5 techniques, as the next sections will make clear, they do afford legal and policy interventions for quantum.

Quantum industrial policy

Quantum provides an opportunity for a reordering of technical might. The EU and China are desperately seeking such opportunities to overcome the asymmetric advantages that US has enjoyed from

[78] JEREMY A. RABKIN AND JOHN YOO, STRIKING POWER: HOW CYBER, ROBOTS, AND SPACE WEAPONS CHANGE THE RULES FOR WAR (Encounter Books 2017). [ALSO JOHN'S FORTHCOMING SPACE ARTICLE]

incubating Silicon Valley. Both the EU and China have established significant quantum initiatives that include basic research funding. The EU funded a $1 billion quantum initiative, with support for research groups and specific projects already granted in 2018. China appears to have invested about $3 billion in quantum technology, according to a report warning of the country's muscularity and devotion to surpassing American innovation in the space.[79] China, as detailed above, has implemented the longest fiber quantum network, distributed quantum keys by satellite intercontinentally, and has likely developed game-changing sonar technology that could be deployed in hotbeds of conflict, such as the South China Sea. These accomplishments are not heralded by state media, but rather by peer reviewed articles in *Science* and *Nature*. The U.S. government on the other hand, has spent in the hundreds of millions to support quantum[80] and its approach has been uncoordinated.

A 2017 survey of quantum technologies by the Economist reflected this national competition in the patent landscape of quantum.[81] Using data current through 2015, the author found that the US had by far the most applications for quantum computing. However, there was a surge of Chinese applications focusing on communications and cryptography in recent years, with China exceeding the US 367 to 233. Investment in sensing was on par between these superpowers. Other countries with fulsome quantum portfolios included Canada (quantum computing), Japan (quantum computing and cryptography), and Germany (sensing).

To respond to these developments Congress quickly introduced and enacted the National Quantum Initiative Act.[82] Signed by President Trump in December 2018, the NQIA authorizes $1.3bn in research and education, to be coordinated by the White House's Office of Science and Technology. As of this writing, the funds have not yet been appropriated.

Taken together, these developments show that quantum is becoming part of nations' industrial policy. Quantum makes a good case for industrial policy interventions under a framework provided by Vinod Aggarwal and Andrew W. Reddie. Writing in the cybersecurity context, one that shares many strategic characteristics common with quantum, the duo explain that governments pursue industrial policy to create markets (market substitution), to facilitate markets, to modify markets, and to set rules for technologies created by markets (market proscription).[83]

In all three categories of quantum technologies, market substitution appears to be necessary. While there are obvious commercial uses for quantum metrology and the most sophisticated and well-resourced companies (such as oil services firms), currently, there are no realistic short-to-medium term commercial uses for quantum communication and computing. Quantum communication is so complex and the

[79] Costello. 2018.
[80] H. Rept. 115-950, National Quantum Initiative Act, 115th U.S. Cong. 2nd Sess. (2018).
[81] Jason Palmer, *Here, there and everywhere: Quantum technology is beginning to come into its own*, THE ECONOMIST March 9, 2017.
[82] National Quantum Initiative Act. 115th U.S. Cong. H. R. 6227, 2nd Session. (2018).
[83] Andrew W. Reddie & Vinod K. Aggarwal, *Comparative industrial policy and cybersecurity: a framework for analysis*, 3 JOURNAL OF CYBER POLICY 291 (2018).

existing commercial justifications for it so thin, that its implementations have been mere publicity stunts, for instance, when the Swiss government allowed a domestic company to use quantum encryption to transmit election information to a central government repository.[84] (Transmission integrity is hardly the most important security aspect of voting, when attackers can interfere with ballots, voting rolls, and the like.) More broadly, the main affordance of quantum communication to detect and prevent nation-state spying is unlikely to motivate the array of companies that operate the internet backbone. In fact, almost all of the major telecommunications providers quietly assisted the NSA's efforts to monitor internet. Both a shift in priority and a willingness to invest is needed to incorporate quantum at the core of the internet. Turning to computing, the National Academies lamented in 2018 that no commercial uses were practical for quantum computing.

Until commercial and consumer applications take root, quantum technologies will need some kind of philanthropy to kickstart a market. In the US, major technology firms have been patrons for quantum. But these efforts are greatly outshined by the EU and China's government-patronage approach. The EU seems to have learned from the American development of the internet as a kind of model for quantum. Despite the libertarian narratives to the contrary, the internet,[85] its most successful connected consumer devices,[86] and indeed even much of the west coast itself,[87] owes its lineage to military and basic research funding from the federal government. At the dawn of internet commerce, it was not clear at all that the web would even succeed as a medium. Today's most profitable companies, such as Amazon.com, languished for years while trying to perfect a web platform for commerce. Some of today's most hyped technology companies—Uber, Tesla, Palantir, Twitter, WeWork—have never turned a profit or are billions in the red, propped up by the hopes and wallets of venture capitalists. Europe in particular has taken up the cause that governments can be market creators in technology,[88] and that these new fields need government incubation to eventually become successful, particularly because Europe lacks a venture market as generous as Silicon Valley's.

American literature tends to be skeptical of industrial policy[89] and indeed there is a feeling rising to the level of reaction formation against government involvement in new technology in Silicon Valley. On the other hand, Aggarwal and Reddie reflect there is a "puzzling gap in the [industrial policy] literature with regard to the role the state has played in driving investment in the high-tech industry."[90] Such patronage is

[84] Paul Marks, *Quantum cryptography to protect Swiss election*, NEW SCIENTIST, October 15, 2007.
[85] Barry M. Leiner, et al., *A brief history of the internet*, 39 J SIGCOMM COMPUT. COMMUN. REV 22 (2009).
[86] MARIANA MAZZUCATO, THE ENTREPRENEURIAL STATE : DEBUNKING PUBLIC VS. PRIVATE SECTOR MYTHS (2015).
[87] JOAN DIDION, WHERE I WAS FROM (2003); GERALD NASH, THE FEDERAL LANDSCAPE: AN ECONOMIC HISTORY OF THE TWENTIETH-CENTURY WEST (1999). ("The size and scale of the new federal [military] establishments were unprecedented. Congress poured more than $100 billion into western installations between 1945 and 1973 . . . The military-industrial complex was the West's biggest business in the cold war years.")
[88] Mariana Mazzucato, *The entrepreneurial state*, 49 SOUNDINGS (2011).
[89] Sonia N & Aggarwal Aggarwal, Vinod K, The Political Economy of Industrial Policy (BASC Working Paper 16-1 ed., 2016).
[90] Aggarwal, JOURNAL OF CYBER POLICY (2018).

an explicit goal in Europe and China's quantum initiatives. Other nations seem to be learning from what the US has done instead of what it has said about industrial policy.

Funding quantum research is unlikely to suffer from pathologies of capture or picking winners or losers. The fundamental technical challenges are so difficult that government support should focus on basic research, as it has in the EU. The principal picking problem comes from betting on a single technology (e.g. trapped ions versus photonics). However, as the National Academes report reveals, the government has a sophisticated, skeptical view of the landscape, and it opined that no technological approach currently demonstrated could scale to a fault-tolerant quantum computer.[91]

Or perhaps the deeper picking problem is choosing quantum itself, instead of classical machine learning or some other promising new technology. Will we have wasted the careers of those who we subsidize in their quantum education and research agenda? That is a possibility, particularly if quantum computing efforts simply cannot be realized with any near-term advances in materials sciences.

In addition to funding, an industrial policy could make technical mandates, and this is an area where the government could pick winners and losers. To achieve a fully quantum internet, communications must be both generated and relayed by fully quantum devices. This would seem to require that networks not only be quantum, but also fully optical, as the technology works most robustly with photons. Thus, laying fiber optic, a major priority in Europe and China, should also be a focus in the US. There will be long-term, unforeseen consequences of an all-fiber network, just as there have been for our copper telephonic network.

How open should quantum be? Export control, immigration policy, and innovation

Originally developed by the military, Global Positioning System (GPS) access is available to the public freely and its unencumbered use has contributed to unimaginable benefits and exciting innovations. The internet has had a similar founding although a more complex path to commercialization that nonetheless has transformed our economy. Should quantum technologies, to the extent it is possible, be open for similar public use and extension? The €1 billion European initiative to promote quantum technologies explicitly embraces openness, calling for "end-user-inspired applications" in quantum networks and inclusion of QRNG in even "cheap devices."[92] The European posture suggests a harmony with an eventual end-to-end quantum internet for the average person.

American quantum policy has yet to explicitly commit to open innovation norms. In fact, the first explicit moves appear to embrace a market proscription approach. In November 2018, the Department of Commerce's Bureau of Industry and Security released an advance notice of proposed rulemaking seeking comment on whether a broad series of technologies should be considered for export control under the

[91] NATIONAL ACADEMIES OF SCIENCES & MEDICINE. 2018.
[92] High Level Steering Committee, Quantum Technologies Flagship Final Report (2017).

Export Control Reform Act of 2018.[93] The ANPRM suggests that quantum sensing, computing and encryption are "foundational technologies," as they are "emerging technologies that are essential to U.S. national security, for example because they have potential conventional weapons, intelligence collection, weapons of mass destruction, or terrorist applications or could provide the United States with a qualitative military or intelligence advantage." The agency is at an early stage, here seeking how to define and thus bound the definition of quantum so that identifiable technologies could be included on an export control list.

Can the government proscribe the quantum marketplace? Imposing export controls will have different implications for our three categories of quantum technologies. Interferometry is already widely dispersed, indeed many of its applications were demonstrated by European investigators. Many sensing technologies can be miniaturized, thus making controls practically more difficult. Quantum computing and communications technologies, on the other hand, rely upon expensive, complex and sensitive hardware/software ensembles that are more readily controlled. Miniaturization is unlikely in quantum computing and the added requirement of supercooling makes the technology more trackable.

Also adding to the market proscription complexity is that private companies play lead roles in quantum communication and quantum computing development. These companies, most of which are located in liberal, western democracies, are both dependent on military investment but sometimes seem to abhor it. For instance, in 2018, Google employees objected to "Project Maven," an effort to improve the object recognition capabilities of the Department of Defense.[94] Google is widely agreed to be the leading company in the quantum research space. Will its employees forgo military markets for quantum technologies, many of which have no other obvious buyer than governments?

The US can stay ahead on quantum by investing in research, by preventing other, hostile countries from getting the technology through theft, sale, or rental (as in commercial cloud or satellite offerings), and by attracting the brightest minds from the world to work on quantum. In 2015, the European Commission estimated that only 7,000 people were working on quantum research *worldwide*.[95] Thus, countries cannot rely on their population and riches alone to build a vigorous quantum industry. As part of a market substitution strategy, the US could optimize immigration policy that liberally allows experts from other countries to emigrate to the US. International diversity is as necessary to quantum as is multidisciplinary, in that quantum computing simply is not possible with expertise in several high-tech fields. The need for

[93] Bureau of Industry and Security Department of Commerce, Review of Controls for Certain Emerging Technologies § 15 CFR Part 744 (2018).
[94] Project Maven had clear implications for the drone program and for weaponry that needs to make target distinction decisions in situations where humans cannot. But a deeper problem with the employee objections is that all of Google's computer vision and artificial intelligence research can contribute to military objectives; the technologies are inherently dual use. It is unclear how Google will ever comply with these employees' demand to never "build warfare technology" when the root of so much of Google's discoveries are easily deployed for ISR or offensive purposes. Unnamed Google Employees, Project Maven Letter (Sundar ed.).
[95] Yasser Omar, Workshop on Quantum Technologies and Industry (DG Connect ed., 2015).

international diversity is reflected in the top academic authors in quantum, as well as when one visits the staff webpages of the companies most advanced in quantum and sees a spectrum of experts from around the world.

How should we normatively evaluate a strongly government-controlled quantum landscape? A scenario planning exercise by Berkeley Center for Long Term Cybersecurity (CLTC) envisions a world where the Department of Defense develops a general-purpose quantum computer and keeps the technology highly classified.[96] In so doing, the scenario highlights likely fault lines and contours of a highly-secretive, nuclear-like approach that seeks marketplace restriction. In the scenario, the plan works at first. Government funding for a field that has few commercial prospects keeps the quantum industry alive and even healthy. Meanwhile, the U.S. government and "five eyes" allies make stunning advances in anti-terrorism and anti-drug efforts.

Under the CLTC's scenario, a marketplace restriction approach ultimately harms commercial interests and the quantum industry itself. Being secret, quantum systems develop slowly, and dependent systems, such as software packages, are uniform and sclerotic. Eventually competing nations develop the technology and this causes a collapse of the U.S. strategy, with American firms worse off in the long run because of lost opportunities to gain quantum expertise during the period of secrecy. The scenario also borrows from the nuclear metaphor, suggesting that the early militarization of the technology creates a quantum "taint" or "taboo." Military-first uses make public perception of quantum negative, even dangerous. Between the secrecy and quantum taboo, humanitarian uses of quantum computing are impeded, darkening our future.

Quantum and space law

The seminal Outer Space Treaty of 1967[97] declares that the use of space will be carried out "for the benefit and in the interests of all countries…" and "exclusively for peaceful purposes." It further prohibits stationing any weapon of mass destruction in space. But between that proscription and affirmative obligation for peaceful purposes, nation-states have many options for using the military in space. As Professors Jeremy Rabkin and John Yoo explain in their book about next-generation weaponry and conflict, the treaty does not prohibit ICBMs, as they are not installed in space but rather pass through it.[98] Nor does the treaty explicitly ban intelligence and surveillance activities,[99] even those that support or enhance force in conflict. Furthermore, quantum metrology, sensing and communications devices are dual-use technologies. Even in a force-supporting role, these quantum technologies in no way trigger the traditional

[96] Center for Long Term Cybersecurity, Cybersecurity Scenarios 2025 (2019).
[97] Brian Krebs, *Inside the Gozi Bulletproof Hosting Facility*, KREBSONSECURITY, 2013.
Done at Washington, London, & Moscow Jan. 27, 1967;, T.I.A.S. No. 6347 (Oct. 10, 1967)
[98] YOO. 2017.
[99] The affirmative command of "peaceful" uses creates ambiguity. A subsequently enacted UN statement broadly allows remote sensing in space, but does not mention surveillance and defines remote sensing as observation performed for environmental purposes. Principles relating to remote sensing of the Earth from space § A/RES/41/65 (United Nations ed., 1986).

concerns of weapons regulation—of indiscriminate or superfluous injury, or of widespread, permanent environmental damage.[100] In fact, these technologies might support more discriminate applications of force.

Quantum technologies may be lawful in space, but they still could be destabilizing. Nations may find it compelling, even necessary, to make first strikes at space-based vessels routing quantum communications or using quantum sensing to silence or blind the handful of superpowers that have both a space program and quantum technology. If jus ad bellum requirements are met, it would seem that jus in bello considerations might mitigate in favor of striking at spacefaring platforms, as it could be justified as a discriminate attack that does not directly attack people, thus minimizing human suffering.

Quantum sensing could be so powerful that nations might find it expedient to voluntarily limit where and when it is deployed. In other domains, superpowers have refrained from developing technologies and in militarizing spaces because of the inherent destabilizing or weapons-race effects they can have. For instance, at times, superpowers have refrained from creating anti-ICBM defenses, for fear that their very presence could change the game theory of nuclear strikes and be escalatory. Turning to territorial forbearance, the Antarctic Treaty System prohibits militarization (both offensive and defensive uses) in Antarctica, making it more strictly regulated than space.

Quantum cybersecurity

Quantum networks may change the game theory of surveillance. Currently, one never knows whether internet intermediaries are trustworthy, whether they relay information faithfully, or whether they copy or alter data for their own purposes. Furthermore, intermediaries can infer the meaning of messages from monitoring metadata. One might address this by routing information differently, but the classical internet makes this difficult. Turning to quantum networks, the technology will afford stronger encryption, and one will know when an eavesdropper is present. How might governments react to that?

One could imagine that governments will double-down on interception. Having an eavesdropper present could deny communicants the ability to establish a secure session. Eavesdropping might also have a signaling function that has utility in a "defend forward" security posture, one characterized by the presence of constant conflict with adversaries. Such eavesdropping is easy because internet traffic routes circuitously, sometimes leaving national boundaries. Nation-states will have many opportunities to physically access fiber optic cables and "listen," even if they cannot understand what is being sent.

But quantum could also make the very design of the internet change. One could also imagine a factionalization of networks, with nation-state controlled, central trunks, much like China's Beijing to Shanghai fiber network. For regions such as the EU and counties like Russia and China, the promise of an interception-resistant channel might make it worthwhile to rearchitect the internet so that it is more private and so that one can choose the paths that data take to avoid likely interception points.

[100] Bill Boothby, *Space Weapons and the Law*, 93 INT'L L. STUD. 179 (2017).

Another, likely approach to the hardening of communications privacy is to erode endpoint security. That is, to discover ways to degrade the security of end users' devices. Even if communications links are perfected and users adopt quantum encryption for their local data, data has to be unscrambled for people to use it. Intelligence and law enforcement agencies that gain control of endpoints will be able to see all data stored on them.

Passwords are key to device security, and unfortunately for users, quantum computers will degrade password hashing security dramatically. Password hashing is the process where services use a one-way encryption function to store a user's password. For instance, the hash value of the common password "password" is: lyNZHNHP7LDv17An6pOxADNLKYYqXYoQHxtmjjacTDQ=. Encrypting passwords protects users because if a server is compromised, the attacker only gains scrambled passwords.[101] Hashing is vulnerable in part because users tend to choose weak passwords and because a quantum computer could be set loose to decrypt simple ones in systematic fashion. For instance, the National Academies warns that a quantum computer user could systematically reverse all the password hashes for 10 character or less passwords relatively quickly.[102]

Quantum computing proof privacy

In addition to decryption of communications data, quantum computing will degrade the most widely used encryption for files. This section is devoted to techniques to counter a privacy apocalypse of stored data.

Quantum resistant encryption

Several, classical computing techniques could frustrate mass decryption by a hypothetical quantum computer.[103] A simple way of countering Grover algorithm attacks, which in effect cuts symmetric key sizes in half, is to lengthen key sizes, thus re-imposing fantastic levels of computational costs. With respect to RSA, "forward secrecy" is an option. In forward secrecy, each session key is unique, thus a compromise of one does not degrade the confidentiality of all messages. Forward secrecy is available in the free Signal voice, text, and file encryption app. Shor's, Grover's, and yet to be discovered quantum algorithms have caused the updating of security standards,[104] and even experiments to determine whether new technologies are readily deployable.

Those working on "post-quantum" cryptography seek to enhance existing encryption or create new systems that will withstand a hypothetical, general purpose, powerful quantum computer. Certain problems are uniquely tractable by a quantum computer; post-quantum researchers test measures that are intractable for quantum computers. For instance, PQ Solutions developed a technique that involves

[101] Although the advent of "rainbow tables" that connect hashes to their underlying password, and the problem of servers accepting hashes as passwords (where the hacker just enters a user's password hash instead of the password to gain access) have eroded this protection.
[102] NATIONAL ACADEMIES OF SCIENCES & MEDICINE. 2018.
[103] Bernstein & Lange, NATURE NATURE (2017).
[104] National Security Agency, CNSA Suite and Quantum Computing FAQ (National Security Agency ed., 2016).

injecting random noise in to each message. In 2016, the Open Quantum Safe (OQS) project was formed to create open source versions of quantum-resilient encryption. Already, commercial companies, such as ID Quantique SA offer quantum encryption featuring QKD and QRNG.

Getting rid of data

Until recently, the modus operandi of technology companies was to collect as much information as possible and to keep it forever. But now even Google, the standard-bearer for information hoarding, started efforts to randomize identifiers associated with searches. This came in response to both FTC guidance and European regulation that encourage or require companies to limit how long identifiable information is maintained to "reasonable" business necessity.

Establishing ceilings for how long data is kept, even in pseudonymous form (because of the advent of machine learning-enabled reidentification techniques) would seem to be a worthwhile intervention in the face of quantum computing. But once regulators limit data retention to reasonable business necessity time periods, one must consider *how* to delete information. Of course, data are encoded on disks and other physical media, however when erased, most businesses destroy the data logically rather than physically. A physical layer deletion approach requires data collectors to actually destroy media with equipment such as disintegrators, which grind hard drives into a mash of metal bits. When one's business is "in the cloud" physical destruction is impossible because the data reside on another company's physical media. Thus, logical approaches, including formatting and simple encryption of the data, are common practice. Weak encryption used for deletion purposes will fail in the presence of quantum computing.

Regulation of decryption

On first blush, it might sound preposterous, but policymakers could weigh a simple prohibition on decryption of others' data. Such a prohibition would not be futile because of the affordances of quantum. To start with, practically speaking, because quantum computers are so expensive to build and maintain, the technology will not be democratically distributed. This gives regulators the opportunity to police a few big players, some of which will want to avoid the negative reputational taint of being linked to mass decryption efforts. Companies will want to capture profits from the devices, and there will be more money to be made in drug discovery and similar efforts than cybercrime or descrambling decades-old prescription records. Of course, this argument will not be true with respect to all government agencies and their contractors. Public sector quantum users will have to be policed in other ways—through constitutional tort and political oversight.

Several quantum innovators have created cloud-based devices for the public to use. This is an ingenious strategy because it allows the company to study how programmers use the device and to identify the most talented programmers. The cloud strategy is likely to be a winning one because few companies

will be able to afford their own quantum computers. Providers can monitor their cloud for signs of decryption, just as one can look for signs of child pornography trading or spam transmission today.[105]

Finally, regulating decryption may seem futile, but U.S. law already regulates many forms of information manipulation that are technologically easy to perform. For instance, U.S. copyright law prohibits the circumvention of digital rights management technologies (often a form of encryption) that protect copyrighted works. More broadly, the Fourth Amendment and the wiretapping laws prohibit warrantless interception of communications content, even though such activity is technologically simple for law enforcement and the intelligence community. As technologies have made private areas subject to sensing at a distance, for instance when law enforcement used infrared cameras to infer that marijuana was being grown in a home,[106] courts could treat government use of the technology as a search. As the Supreme Court has eroded the third-party doctrine,[107] there may come a time where people will enjoy a reasonable expectation of privacy in personal information databases held by third parties. Quantum decryption in such scenarios could be subject to the warrant preference.

Quantum machine learning and artificial intelligence

Companies in quantum identify a number of commercial goals with the technology. Some are seeking shorter term goals, but Google is aiming for the moonshot of achieving artificial intelligence using quantum computers. Quantum parallelism should enable the consideration of all possible decisions in microseconds, perhaps enabling computers to be as generative as people. Quantum computing is thought to both speed existing machine learning processes but also create the infrastructure for entirely new techniques.[108]

Machine learning may receive a significant advance with quantum because if current limitations on encoding quantum information can be overcome, a quantum machine learning process could consider more information than classical approaches. In classical approaches, data scientists deal with so much data that in order to make problems tractable, they either simplify or discard data. Simply put, high-dimensional datasets include too many independent variables to consider. Collapsing them makes computing faster or in some cases, simply possible. For instance, in natural language processing, in order to make computation of a corpus possible, a data scientist may systematically eliminate all words considered to be "low value" in meaning ("stop words"). Similarly, to reduce the problem space, data scientists uses stemming and lemmas to collapse words with similar roots into a single concept. Presumably a quantum machine learning approach, with its form of parallelism, would have no need for throwing out so much data.

Among the most intriguing proposals comes from combining machine learning with quantum simulation of physical objects. Aspuru-Guzik et al. puts it nicely: "Imagine that you want to find a

[105] This strategy fails if blind quantum computing is achieved, because its functions will be encrypted end-to-end and obscured even from the cloud quantum computer operator.
[106] Kyllo v. U.S., 533 US 27, (2001).
[107] Carpenter v. U.S., 585 US ___, (2018).
[108] Aspuru-Guzik, et al. 2015.

potential candidate for a cancer therapy. The user would begin by compiling a list of known compounds that are effective or ineffective for fighting a particular form of cancer. The user then decides a class of molecular features that they believe will be useful for deciding the effectiveness of a drug. Quantum simulation algorithms could then be used to calculate these features for use in a supervised data for a quantum machine learning algorithm. A quantum computer could subsequently use Grover's search to rapidly scan over a database of potential candidate molecules in search of one that the trained model believes will have therapeutic properties."[109] These same authors point out that paired ML-simulation systems could be used in myriad other contexts, including optimization of materials and even in attempts to reach nuclear fusion.

Quantum procedural fairness

AI/ML has raised deep concerns about how data inputs, algorithms, and commercial practices might result in machines that engage in unlawful discrimination or other kinds of unfairness. Because the answers produced by AI/ML systems will be thought to be "smart," users might inadvertently engage in invidious discrimination while laying the moral responsibility with the computer. A rich field known as FAT* (fairness, accountability, and transparency in machine learning, artificial intelligence, and other systems) seeks to create procedural and substantive standards to detect discrimination and other forms of perverse outcomes. A key problem in this space is that there appears to be an inverse relationship between learning power and explainability in ML. That is, the most powerful learning systems, because of their complexity, find subtle and unpredictable relationships. Yet this power comes with a price—users may not be able to explain why these relationships occur, and they may correlate with race or other factors that could result in perverse policy outcomes.

Quantum computers' affordances may help erode the explainability problem because the devices are reversible, unlike classical computers. A 2018 NAS report explains this affordance nicely: "…operations must be 'lossless'—that is, they must not dissipate any energy, since energy dissipation means that the system is connected to the environment to allow heat to flow out, which would result in unacceptable decoherence. Since losing information dissipates energy, quantum gates must be reversible, which means that not only can you compute the gate's outputs from its inputs, you can also compute the gate's inputs from its outputs (the gate's computation can be run backward, or reversed)." Presumably, reversibility should provide AI/ML engineers with the ability to debug in reverse, step-by-step, and perhaps diagnose the exact moment where unpredictable associations are made, or when unfairness inures in a system.

Quantum substantive fairness

Turning to substantive aspects of fairness, we might see quantum-enhanced learning as inherently disproportionate and powerful when applied to people in many domains. We would not consider it fair for

[109] Aspuru-Guzik, et al. 2015.

person to play Chess or Go against a supercomputer. But what if we are called to play consumer or investor against opponents with quantum optimization?

In the consumer context, the immense volume of internet traffic and tracking simply cannot be computed on classical machines. Thus, marketers use abstractions to make sense of consumers, such as profiles that bin consumers into general categories like age, sex, presence of children, and so on. These abstractions are coarse representations of reality, but good enough to target ads. Turning to a quantum marketing machine, individual consumers could come into full focus. The fine grained, second-by-second ways in which we pay attention might be sensed and understood. We should anticipate such systems to know about our history but also our personality. In a quantum world, sellers might understand our reserve prices, our strongest preferences, the kinds of evidence that causes us to change our minds.

Turning to investing, exchanges have already created affordances to address super investors. Automated traders can generate wealth simply through timing, thus some exchanges have used physical measures in order to slow computer trading such that it cannot outperform the exchange itself. The same high-dimensionality used to profile consumers could also make predictions about subtle marketplace inputs, leading to unforeseeable advantages.

Recall that quantum computing is most likely to be achieved by nation states or dominant technology companies. Google reportedly refrained from using user search terms to predict stock movements,[110] apparently because it realized that searches may include material non-public information. Google may similarly conclude that quantum trading approaches implicate insider-trading laws. But nation-states will not concern themselves with such limitations. In fact, quantum ML might be a seductive tool for the destabilization of other economies. Imagine using quantum optimization in order to identify subtle, inscrutable market effects disadvantageous for Vladimir Putin's oligarchs? Or imagine identifying the kinds of conditions that could poison the chances of a Chinese marketplace competitor, Huawei, for instance, from gaining a foothold in telecommunications markets. The intelligence community has already found offensive cyber to be a useful, asymmetric, secret tool to undermine adversaries. Won't quantum be just as tempting a tool?

The law already remedies many situations where automation or information asymmetry creates imbalances of power. Quantum ML might be a field where such imbalances need transparency forcing, or other remedies, including bans on certain applications.

Conclusion

Many technologies are deployed by companies and governments on people with no policy framework or plan to address their implications. We have an opportunity to begin a policy conversation on a consequential technology that will reshape how companies and government measure and observe,

[110] Jon Fortt, *Top 5 moments from Eric Schmidt's talk in Abu Dhabi*, FORTUNE, March 11, 2010.

communicate, and make sense of the world through simulations and problem solving. Quantum technologies are quickly arriving, and even if the most dramatic developments in quantum computer never take place, quantum sensing and communications could shift relationships irrevocably. This article has painted the landscape of quantum's legal implications—from nation-state concerns of strategic conflict, intelligence gathering, and military operational and tactical levels; to the concerns of companies that may be subject to industrial policy priorities and restrictions; to the level of the individual who may face a government and private sector with greater sensing and sense-making abilities. We ought to start deciding now how these technologies are used before others make the choice for us.

Bibliography

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).
ANIL ANANTHASWAMY, THROUGH TWO DOORS AT ONCE: THE ELEGANT EXPERIMENT THAT CAPTURES THE ENIGMA OF OUR QUANTUM REALITY (Dutton 2018).
Johannes Kalliauer, An illustration of the 'Double-slit experiment' in physics § 512x215 (Wikipedia 2017).
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).
W. Pfaff, et al., *Unconditional quantum teleportation between distant solid-state quantum bits*, 345 SCIENCE 532 (2014).
J. Yin, et al., *Satellite-based entanglement distribution over 1200 kilometers*, 356 SCIENCE 1180 (2017).
E. Gibney, *New definitions of scientific units are on the horizon*, 550 NATURE 312 (2017).
A. Cho, *Plot to redefine the kilogram nears climax*, 356 SCIENCE 670 (2017).
Abi Berger, *Magnetic resonance imaging*, 324 BMJ (CLINICAL RESEARCH ED.) (2002).
Michael A. Taylor & Warwick P. Bowen, *Quantum metrology and its application in biology*, 615 PHYSICS REPORTS (2016).
K. Svoboda & R. Yasuda, *Principles of two-photon excitation microscopy and its applications to neuroscience*, 50 NEURON 823 (2006).
Anthony Holtmaat, et al., *Long-term, high-resolution imaging in the mouse neocortex through a chronic cranial window*, 4 NATURE PROTOCOLS 1128 (2009).
Dmitry Strekalov & Jonathan Dowling, *Two-photon interferometry for high-resolution imaging*, 49 JOURNAL OF MODERN OPTICS 519 (2002).
Roger N. McDermott, Russia's Electronic Warfare Capabilities to 2025 (International Centre for Defence 2017).
Geoff Brumfiel, *U.S. Navy Brings Back Navigation By The Stars For Officers*, NPR, February 22, 2016.
USAF Scientific Advisory Board, Utility of Quantum Systems for the Air Force Study Abstract (USAF ed., 2015).
John Preskill, Q2B: Quantum Computing for Business (Keynote Address, Quantum Computing for Business 2018).
Marco Lanzagorta, *Quantum Radar*, 3 SYNTHESIS LECTURES ON QUANTUM COMPUTING (2011).
David Hambling, *China's quantum submarine detector could seal South China Sea*, NEW SCIENTIST, August 22, 2017.
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).

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.
Bruce Schneier, *Did NSA Put a Secret Backdoor in New Encryption Standard?*, WIRED November 15, 2007.
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).
ID Quantique, *Quantis Random Number Generator* (2019), *available at* https://www.idquantique.com/random-number-generation/products/quantis-random-number-generator/.
Centre for Quantum Computing and Communication Technology, *Welcome to the ANU Quantum Random Numbers Server*(2019), *available at* https://qrng.anu.edu.au/#.
C. H. Bennett & G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, 560 THEORETICAL COMPUTER SCIENCE 7 (2014).
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.
L. Oesterling, et al., Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information (2012).
Valerio Scarani, et al., *The security of practical quantum key distribution*, 81 REVIEWS OF MODERN PHYSICS (2009).
Stephanie Wehner, et al., *Quantum internet: A vision for the road ahead*, 362 NATURE eaam9288 (2018).
High Level Steering Committee, Quantum Technologies Flagship Intermediate Report (2017).
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.
Zhen-Sheng Yuan, et al., *Experimental demonstration of a BDCZ quantum repeater node*, 454 NATURE (2008).
H. J. Briegel, et al., *Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication*, 81 PHYSICAL REVIEW LETTERS (1998).
B. Hensen, et al., *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres*, 526 NATURE (2015).
Sheng-Kai Liao, et al., *Satellite-Relayed Intercontinental Quantum Network*, 120 PHYSICAL REVIEW LETTERS (2018).
Doug Finke, *Qubit Count* Quantum Computing Report(2018), *available at* https://quantumcomputingreport.com/scorecards/qubit-count/.
ENGINEERING NATIONAL ACADEMIES OF SCIENCES & MEDICINE, QUANTUM COMPUTING: PROGRESS AND PROSPECTS (Emily Grumbling & Mark Horowitz eds., The National Academies Press 2018).
Ashley Montanaro, *Quantum algorithms*, 2 NPJ QUANTUM INFORMATION (2016).
S. Jordan, *The quantum algorithm zoo*, *available at* http://math.nist.gov/quantum/zoo/.
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).
Mikhail Dyakonov, *The Case Against Quantum Computing*, IEEE SPECTRUM Nov. 15, 2018. 2018.

IBM, *IBM Q Experience*, *available at* https://quantumexperience.ng.bluemix.net/qx/editor.
R. P. Feynman, *Simulating Physics with Computers*, 21 INTERNATIONAL JOURNAL OF THEORETICAL PHYSICS 467 (1982).
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).
Lov K. Grover, *Quantum computing*, 39 SCIENCES 24 (1999).
Trevor Lanting, Next Generation QA Hardware (2018).
P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, 26 SIAM JOURNAL ON COMPUTING 1484 (1997).
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: ED; Size: 59 p. (2015).
Lov K. Grover, A fast quantum mechanical algorithm for database search (ACM 1996).
Daniel J. Bernstein, Grover vs. McEliece (Springer Berlin Heidelberg 2010).
D. J. Bernstein & T. Lange, *Post-quantum cryptography*, 549 NATURE NATURE (2017).
National Aeronautic and Space Administration, *Laser Interferometer Space Antenna*, *available at* https://lisa.nasa.gov/index.html.
Orin Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285 (2015).
Susan Landau, *Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations*, 11 IEEE SECURITY & PRIVACY 54 (2013).
Marco Lanzagorta, Envisioning the Future of Quantum Sensing and Communications (Quantum Sensing and Communications, NASEM Intelligence Community Studies Board August 23, 2018).
Elsa B. Kania & John K. Costello, Quantum Hegemony: China's Ambitions and the Challenge to U.S. Innovation Leadership (Center for a New American Security 2018).
T. Li, et al., Security attack analysis using attack patterns (2016).
Timothy Vidas, et al., All Your Droid Are Belong to Us: A Survey of Current Android Attacks (2011).
Nathan Heller, *Estonia, The Digital Republic*, NEW YORKER December 18, 2017.
PLUTARCH, THE PARALLEL LIVES § 10(Loeb Classical Library edition ed 1921).
CARLO KOPP, CLASSICAL DECEPTION TECHNIQUES AND PERCEPTION MANAGEMENT VS. THE FOUR STRATEGIES OF INFORMATION WARFARE (2005).
JEREMY A. RABKIN AND JOHN YOO, STRIKING POWER: HOW CYBER, ROBOTS, AND SPACE WEAPONS CHANGE THE RULES FOR WAR (Encounter Books 2017).
H. Rept. 115-950, National Quantum Initiative Act, 115th U.S. Cong. 2nd Sess. (2018).
Jason Palmer, *Here, there and everywhere: Quantum technology is beginning to come into its own*, THE ECONOMIST March 9, 2017.
National Quantum Initiative Act. 115th U.S. Cong. H. R. 6227, 2nd Session. (2018).
Andrew W. Reddie & Vinod K. Aggarwal, *Comparative industrial policy and cybersecurity: a framework for analysis*, 3 JOURNAL OF CYBER POLICY 291 (2018).
Paul Marks, *Quantum cryptography to protect Swiss election*, NEW SCIENTIST, October 15, 2007.
Barry M. Leiner, et al., *A brief history of the internet*, 39 J SIGCOMM COMPUT. COMMUN. REV 22 (2009).
MARIANA MAZZUCATO, THE ENTREPRENEURIAL STATE : DEBUNKING PUBLIC VS. PRIVATE SECTOR MYTHS (2015).

JOAN DIDION, WHERE I WAS FROM (2003).
GERALD NASH, THE FEDERAL LANDSCAPE: AN ECONOMIC HISTORY OF THE TWENTIETH-CENTURY WEST (1999).
Mariana Mazzucato, *The entrepreneurial state*, 49 SOUNDINGS (2011).
Sonia N & Aggarwal Aggarwal, Vinod K, The Political Economy of Industrial Policy (BASC Working Paper 16-1 ed., 2016).
High Level Steering Committee, Quantum Technologies Flagship Final Report (2017).
Bureau of Industry and Security Department of Commerce, Review of Controls for Certain Emerging Technologies § 15 CFR Part 744 (2018).
Unnamed Google Employees, Project Maven Letter (Sundar ed.).
Yasser Omar, Workshop on Quantum Technologies and Industry (DG Connect ed., 2015).
Center for Long Term Cybersecurity, Cybersecurity Scenarios 2025 (2019).
Brian Krebs, *Inside the Gozi Bulletproof Hosting Facility*, KREBSONSECURITY, 2013.
Principles relating to remote sensing of the Earth from space § A/RES/41/65 (United Nations ed., 1986).
Bill Boothby, *Space Weapons and the Law*, 93 INT'L L. STUD. 179 (2017).
National Security Agency, CNSA Suite and Quantum Computing FAQ (National Security Agency ed., 2016).
Kyllo v. U.S., 533 US 27, (2001).
Carpenter v. U.S., 585 US ___, (2018).
Jon Fortt, *Top 5 moments from Eric Schmidt's talk in Abu Dhabi*, FORTUNE, March 11, 2010.